Revision	Approved by	Number of Pages
002		483
Approval Date	24/12/2021	

CGN EDF
General Nuclear System

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	**HPR/GDA/PCSR/0012**

Title:

Pre-Construction Safety Report

Chapter 12

Design Basis Condition Analysis

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

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

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

DISTRIBUTION LIST

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

TABLE OF CONTENTS

12.1 List of Abbreviations and Acronyms

AAD	Startup and Shutdown Feedwater system [SSFS]
ADMS	Atmospheric Dispersion Modelling System
ALARP	As Low As Reasonably Practicable
APG	Steam Generator Blowdown System [SGBS]
ARE	Main Feedwater System [MFFCS]
ASG	Emergency Feedwater System [EFWS]
BOC	Beginning of Cycle
CRDM	Control Rod Drive Mechanism
DBA	Design Basis Analysis
DBC	Design Basis Condition
DEC-A	Design Extension Condition A
DN	Nominal Diameter
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
DWK	Fuel Building Ventilation System [FBVS]
DWL	Safeguard Building Controlled Area Ventilation System [SBCAVS]
EBA	Containment Sweeping and Blowndown Ventilation System [CSBVS]
ECCS	Emergency Core Cooling System
EDE	Annulus Ventilation System [AVS]
EDG	Emergency Diesel Generator
EOC	End of Cycle
FC1	Safety Category 1 Function
FC2	Safety Category 2 Function
FCG3	Fangchenggang Nuclear Power Plant Unit 3
FMEA	Failure Modes and Effects Analysis
FP	Full Power

GCT	Turbine Bypass System [TBS]
GDA	Generic Design Assessment
HP	High Pressure
HPR1000	Hua-long Pressurized Reactor
HPR1000 (FCG3)	Hua-long Pressurized Reactor under construction at Fangchenggang nuclear power plant unit 3
I&C	Instrumentation and Control
IRWST	In-containment Refuelling Water Storage Tank
KRT	Plant Radiation Monitoring System [PRMS]
LB-LOCA	Large Break - Loss of Coolant Accident
LCO	Limiting Condition of Operation
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident
LOOP	Loss of Off-Site Power
MCS	Maintenance Cold Shutdown
MHSI	Medium Head Safety Injection
MSIV	Main Steam Isolation Valve
MSLB	Main Steam Line Break
MSQA	Management of Safety and Quality Assurance
MSSV	Main Steam Safety Valve
NC	Non-Classified
NR	Narrow Range
NRPB	National Radiological Protection Board
NS/RIS-RHR	Normal Shutdown with RIS-RHR
NSSS	Nuclear Steam Supply System
NS/SG	Normal Shutdown with Steam Generators
OTS	Operating Technical Specification
PCSR	Pre-Construction Safety Report

PIE	Postulated Initiating Events
PSA	Probabilistic Safety Assessment
PSV	Pressuriser Safety Valve
PTR	Fuel Pool Cooling and Treatment System [FPCTS]
PZR	Pressuriser
RBS	Emergency Boration System [EBS]
RCCA	Rod Cluster Control Assembly
RCD	Reactor Completely Discharge
RCP	Reactor Coolant Pump
RCP	Reactor Coolant System [RCS]
RCPB	Reactor Coolant Pressure Boundary
RCS	Refuelling Cold Shutdown
RCV	Chemical and Volume Control System [CVCS]
REA	Reactor Boron and Water Makeup System [RBWMS]
REN	Nuclear Sampling System [NSS]
RGL	Rod Position Indication and Rod Control System
RHR	Residual Heat Removal
RIS	Safety Injection System [SIS]
RP	Reactor in Power
RPT	Radiation Protection Target
RRI	Component Cooling Water System [CCWS]
SADV	Severe Accident Dedicated Valve
SF	Safety functions
SFC	Single Failure Criterion
SFP	Spent Fuel Pool
SG	Steam Generator
SGa	Affected Steam Generator
SGTR	Steam Generator Tube Rupture

SSCs	Structures, Systems and Components
SWI	Seal Water Injection
UK HPR1000	The UK version of the Hua-long Pressurized Reactor
VDA	Atmospheric Steam Dump System [ASDS]
V&V	Verification and Validation

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

12.2 Introduction

The purpose of this chapter is to demonstrate that the UK version of the Hua-long Pressurised Reactor (UK HPR1000) is tolerant to design basis faults. This means that the safety functions provided in the design, and the related Structures, Systems and Components (SSCs), can protect the workers and the public, and that the nuclear safety risks are As Low As Reasonably Practicable (ALARP).

The Design Basis Condition (DBC) analysis presented in this issue of Chapter 12 is based on Design Reference (DR) 3.0, as described in UK HPR1000 Design Reference Report [1]. The safety assessment results are documented in this chapter and corresponding reports.

12.2.1 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 (Level 1 claims) and a number of Level 2 claims are developed and presented in Chapter 1. This chapter supports the ***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 and hazard analysis has been used to specify the requirements on the safety measures and inform emergency arrangements;*

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

The plant with its design basis safety systems can respond to any fault with an initiating event frequency > 1E-5/year and achieve a controlled and safe state with a tolerable radiation exposure or release of radioactive material.

All postulated initiating events or fault sequences of the UK HPR1000 are classified into four design basis conditions (DBC-1 to DBC-4) and two Design Extension Conditions (DEC-A and DEC-B). The analysis of design basis conditions is presented in this chapter, and that of design extension conditions in Chapter 13.

The purpose of this chapter is to demonstrate the high-level claim using the following sub-claims and arguments:

a) ***Sub-Claim 3.2.1.SC12.1****: All initiating events with the potential to lead to significant radiation exposure or release of radioactive material, including the*

effects of internal and external hazards have been identified.

1) ***Argument 3.2.1SC12.1-A1****: A systematic process has been defined to identify all Postulated Initiating Event (PIE) that could lead to a release of radioactive material.*

   - ***Evidence 3.2.1SC12.1-A1-E1:*** The identification of Postulated Initiating Event (PIEs) for UK HPR1000 is a combination of several methods including master logic diagram analysis and Failure Mode and Effect Analysis (FMEA) (see Sub-chapter 12.4).

   - ***Evidence 3.2.1SC12.1-A1-E2:*** The internal and external hazards schedules provide linkage between the effects of hazards and fault analysis (see Reference [2] and Reference [3]).

2) ***Argument 3.2.1SC12.1-A2****: The systematic PIE identification methodology has been applied to produce the PIE list which is a common input for both Design Basis Accident (DBA) and Probabilistic Safety Assessment (PSA) grouping process.*

   - ***Evidence 3.2.1SC12.1-A2-E1:*** The PIEs are identified based on established methodologies, and the DBC list used for DBA is identified based on the grouping and bounding analysis (see Sub-chapter 12.4).

3) ***Argument 3.2.1SC12.1-A3****: All operating states have been considered in the identification of PIE.*

   - ***Evidence 3.2.1SC12.1-A3-E1:*** Reactor in Power (RP), Normal Shutdown with Steam Generators (SG) (NS/SG), Normal Shutdown with RIS-RHR (NS/RIS-RHR), Maintenance Cold Shutdown (MCS), Refuelling Cold Shutdown (RCS) and Reactor Completely Discharge (RCD) are considered in the identification of PIE (see Sub-chapter 12.4).

4) ***Argument 3.2.1SC12.1-A4****: All potential sources of radioactivity have been assessed in the derivation of the PIEs.*

   - ***Evidence 3.2.1SC12.1-A4-E1:*** The identification of PIE considers all potential sources of activity and all risks to the public and the environment including the internal event, loss of supporting system, and the spurious actuation of Instrumentation and Control (I&C) (see Sub-chapter 12.4).

5) ***Argument 3.2.1SC12.1-A5****: The frequency of each PIE has been derived in a systematic manner.*

   - ***Evidence 3.2.1SC12.1-A5-E1:*** A categorisation system groups PIE into four categories according to their anticipated frequency of occurrence and potential radiological consequences to the public (see Sub-chapter

12.4).

6) ***Argument 3.2.1SC12.1-A6***: *The PIEs have been grouped to produce initiating events for detailed assessment.*

- ***Evidence 3.2.1SC12.1-A6-E1:*** The DBC list used for DBA is identified based on the grouping and bounding analysis (see Sub-chapter 12.4).

b) ***Sub-Claim 3.2.2.SC12.2***: *The appropriate analysis approach has been applied for each fault.*

1) ***Argument 3.2.2.SC12.2-A1****: Appropriate acceptance criteria have been identified that, if met, ensure the delivery of the three essential safety functions following any initiating event.*

- ***Evidence 3.2.2.SC12.2-A1-E1:*** Acceptance criteria have been defined that demonstrate the continuing delivery of the reactivity control essential safety function (see Sub-chapter 5.5 and Sub-chapter 12.5);

- ***Evidence 3.2.2.SC12.2-A1-E2:*** Acceptance criteria have been defined that demonstrate the continuing delivery of the heat removal essential safety function (see Sub-chapter 5.6 and Sub-chapter 12.5);

- ***Evidence 3.2.2.SC12.2-A1-E3:*** Acceptance criteria have been defined that demonstrate the continuing delivery of the confinement essential safety function (see Sub-chapter 6.6, Sub-chapter 7.2.4, Sub-chapter 12.5 and Sub-chapter 16.3).

- ***Evidence 3.2.2.SC12.2-A1-E4:*** The conditions arising from the identified initiating events will not result in the consequential failure of other safety related equipment (see Sub-chapter 19.4).

2) ***Argument 3.2.2.SC12.2-A2:*** *Appropriate analysis methods have been identified, verified and validated to assess the consequences of the design basis initiating events identified in the fault schedule.*

- ***Evidence 3.2.2.SC12.2-A2-E1:*** A review of potential analysis codes has identified a set of suitable analysis codes to perform the fault analysis for the UK HPR1000 (see Appendix A.);

- ***Evidence 3.2.2.SC12.2-A2-E2:*** Each of the codes identified for use in the fault analysis has been verified to confirm the correctness of the coding (see Appendix A);

- ***Evidence 3.2.2.SC12.2-A2-E3:*** For each fault analysis code, a detailed validation matrix has been produced showing all the validation cases and the related validated models or phenomena (see Appendix A);

- ***Evidence 3.2.2.SC12.2-A2-E4:*** Appropriate validation results have been

provided against the requirements of the validation matrix to justify the use of the fault analysis codes and related analysis methods (see Appendix A);

- ***Evidence 3.2.2.SC12.2-A2-E5:*** Appropriate guidance has been provided to the analysts who are applying the fault analysis codes (see Appendix A).

3) ***Argument 3.2.2.SC12.2-A3:*** *Appropriate analysis rules have been applied, addressing conservative initial conditions, plant operation parameters, operator actions and the worst single failure, in the analysis of design basis faults.*

- ***Evidence 3.2.2.SC12.2-A3-E1:*** Conservative plant initial conditions have been defined for the DBA (see Sub-chapter 12.7 – 12.9, 12.11 and reference report for each DBC event analysis);

- ***Evidence 3.2.2.SC12.2-A3-E2:*** Performance requirements for safety systems are defined for use in the fault analysis and in the design of the safety systems (see Sub-chapter 12.7 – 12.9, 12.11 and reference report for each DBC event analysis);

- ***Evidence 3.2.2.SC12.2-A3-E3:*** A detailed assessment of the progression of each fault is performed to identify the worst single failure (see Sub-chapter 12.7 – 12.9, 12.11 and reference report for each DBC event analysis).

c) ***Sub-claim 3.4.3.SC12.3:*** *Depending on the frequency of the initiating fault, an appropriate level of diversity, redundancy, and reliability of the individual SSCs is provided to achieve safety measures for a robust fault-tolerant plant, and identified in a comprehensive fault schedule.*

1) ***Argument 3.4.3.SC12.3-A1:*** *An appropriate methodology has been developed to produce the fault schedule*

- ***Evidence 3.4.3.SC12.3-A1-E1:*** Fault schedule production follows a defined process. PIE identification, determination of safety functions, and transient analysis are the the key parts to producing the fault schedule (see Sub-chapter 12.12).

2) ***Argument 3.4.3.SC12.3-A2:*** *The fault schedule methodology has defined the process for identifying SSCs of the required classification for each of the safety measures.*

- ***Evidence 3.4.3.SC12.3-A2-E1:*** The categorisation and classification of the safety systems required for main protection line and diverse protection line have been identified and have been presented in the fault

schedule (see Sub-chapter 12.12).

3) ***Argument 3.4.3.SC12.3-A3:*** *The safety measures required to protect against the fault following each initiating event have been identified.*

- ***Evidence 3.4.3.SC12.3-A3-E1:*** The safety measures required for each fault have been presented in the fault schedule (See Sub-chapter 12.12).

d) ***Sub-claim 3.4.5.SC12.4:*** *Analysis results demonstrated that the UK HPR1000 is able to achieve the controlled state and the safe state after any identified initial events without leading to an off-site release that would require significant off-site counter-measures (such as evacuation) or to an excessive dose to workers.*

1) ***Argument 3.4.5.SC12.4-A1:*** *The plant can be led to the controlled state and the safe state using the safety systems identified in the fault schedule without violation of the identified acceptance criteria. The achievement of safe state may require operator actions to achieve it.*

- ***Evidence 3.4.5.SC12.4-A1-E1:*** The fault analysis shows that the plant can be transferred to the controlled state under all faults in the fault schedule using only Class 1 or Class 2 safety systems without violating the defined acceptance criteria (see Sub-chapter 12.7-12.9);

- ***Evidence 3.4.5.SC12.4-A1-E2:*** The operator actions required to support the transition of the plant from the controlled state to the safe state have been identified (see Sub-chapter 12.7-12.9);

- ***Evidence 3.4.5.SC12.4-A1-E3:*** The systems required to support the transition from the controlled state to the long term safe state have been identified (see Sub-chapter 12.7-12.10);

- ***Evidence 3.4.5.SC12.4-A1-E4:*** The operator actions required to support the transition of the plant from the controlled state to the safe state have been appropriately justified (see Sub-chapter 12.7-12.10).

2) ***Argument 3.4.5.SC12.4-A2:*** *The radiological release and exposure or direct radiation exposure following design basis events meets the acceptance criteria.*

- ***Evidence 3.4.5.SC12.4-A2-E1:*** The consequences for the public under design basis faults have been evaluated and show that the required success criteria have been met (see Sub-chapter 12.11);

- ***Evidence 3.4.5.SC12.4-A2-E2:*** The consequences for workers under design basis faults have been evaluated and show that the required acceptance criteria have been met (see Sub-chapter 12.11).

12.2.2 Chapter Structure

As claimed in the Chapter Route Map, DBA is undertaken to demonstrate that UK HPR1000 is tolerant to design basis faults, which means that the safety functions provided in the design, and the related SSCs, can protect the workers and the public, and that the nuclear safety risks are ALARP.

The following evidence is provided to support claims and arguments in this chapter:

a) Fault identification and fault grouping;

b) Determination of analysis rules;

c) DBC analysis and identification of safety functions requirements;

d) Radiological consequences analysis;

e) Fault Schedule and demonstration of diverse protection lines;

f) Determination of Limits and Conditions for Operation (LCOs); and

g) ALARP demonstration.

Taking into account the above activities, this chapter is arranged as follows:

a) Sub-chapter 12.1 gives a list of abbreviations and acronyms;

b) Sub-chapter 12.2 gives the introduction including overall information for Chapter 12 and interfaces with other chapters;

c) Sub-chapter 12.3 presents the applicable codes and standards;

d) Sub-chapter 12.4 contains the methodologies and results of fault identification and fault grouping;

e) Sub-chapter 12.5 addresses the analysis rules applied in DBA;

f) Sub-chapter 12.6 addresses the plant characteristics taken into account during analysis;

g) Sub-chapter 12.7 contains the analysis of DBC-2 events;

h) Sub-chapter 12.8 contains the analysis of DBC-3 events;

i) Sub-chapter 12.9 contains the analysis of DBC-4 events;

j) Sub-chapter 12.10 provides a summary of Demonstration of Diverse Protection Lines;

k) Sub-chapter 12.11 contains the radiological consequences of the DBA;

l) Sub-chapter 12.12 describes the analysis of specific studies;

m) Sub-chapter 12.13 describes the design methodology of the Fault Schedule;

n) Sub-chapter 12.14 describes the limits and conditions of operation derived from DBA;

o) Sub-chapter 12.15 addresses the role of DBC analysis in the overall ALARP evaluation for UK HPR1000 design;

p) Sub-chapter 12.16 presents the concluding remarks;

q) The last sub-chapter provides the references;

r) Appendix 12A is the introduction of computer codes used in the fault studies and radiological release analysis.

12.2.3 Plant Design and Operation Supported by Fault Analysis

This section describes the general description of relationship between fault analysis, plant design and operation.

12.2.3.1 Fuel and Core Design

The fuel and core design is a vital input for design basis analysis, providing core-related parameters and acceptance criteria related to core and fuel under accidents. The agreement with acceptance criteria for the design basis analysis demonstrates a satisfactory fuel and core design.

12.2.3.2 Safety Functions and SSCs

Safety functions provided by SSCs are designed to prevent or mitigate faults. Only categorised safety functions and classified SSCs are taken into account in design basis analysis. Safety functions to mitigate faults are claimed in individual fault analysis and are summarised in Fault Schedule. The agreement with acceptance criteria for the design basis analysis demonstrates the adequacy of the design of safety functions and SSCs. The safety systems providing safety functions are summarised in Chapter 7.

12.2.3.3 Plant Operation

The design basis analysis is based on initial conditions, mitigation measures and assumptions. The acceptance criteria are met as long as the relevant LCOs are not breached. In operation, if these LCOs are breached, then actions must be taken to bring the operating envelope back within the bounds of the safety case. Otherwise, the reactor is operating without a valid safety case.

12.2.4 Interfaces with Other Chapters

The interfaces to other parts of the PCSR are as given in the table below.

T-12.2-1 Interfaces between Chapter 12 and Other Chapters

PCSR Chapter	Interface

PCSR Chapter	Interface
Chapter 1 Introduction	Chapter 1 provides the fundamental objective, level 1 claims and level 2 claims. Chapter 12 provides claims and arguments to support relevant claims that are addressed in Chapter 1.
Chapter 4 General Safety and Design Principles	Chapter 4 addresses the methods adopted for the assessment and substantiation of the plant systems.
Chapter 5 Reactor Core	Chapter 5 provides the acceptance criteria related to core and fuel under accidents and core-related parameters as input for fault analysis.
Chapters 6\7\8\9\10\11 Reactor Coolant System\Safety Systems\Instrumentation and Control\Electric Power\Auxiliary Systems\Steam and Power Conversion System	Chapters 6\7\8\9\10\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 fault analysis.
Chapter 13 Design Extension Conditions and Severe Accident Analysis	Chapter 13 provide the Design Extension Condition A (DEC-A) analyses which support Fault Schedule and diverse protection lines.
Chapter 14 Probabilistic Safety Assessment	Chapter 14 provides PSA results related to the Fault Identification and Fault Grouping in Chapter 12.
Chapter 15 Human Factors	Chapter 12 provides human-related claims (implied and explicit) in fault studies, which require Human Factor analysis and/or review. Chapter 15 substantiate the claims on operator actions under DBC conditions.
Chapters 18\19 External Hazards\ Internal Hazards	Chapters 18\19 address whether any hazards need to be considered in the DBC Accident Analysis.
Chapter 20 MSQA (Management of Safety and Quality Assurance) and Safety Case Management	PCSR Chapter 20 presents Safety Case and Design Control Management including relevant requirements, process and coding system of the Requirement Management. Chapter 12 applies the arrangements of Requirement Management set out in Chapter 20.
Chapter 21 Reactor	Chapter 12 and its supporting documents contain the

PCSR Chapter	Interface
Chemistry	description of chemical effects that relate to Design Basis Condition (DBC) source term analysis, including fission product control and iodine retention and transport.
Chapter 22 Radiological Protection	Chapter 12 provides design basis accident source terms. Chapter 22 provides the primary coolant source term for radiological consequence analysis under Design Basis Condition (DBC) accidents.
Chapter 23 Radioactive Waste Management	Chapter 12 provides the Design Basis Condition (DBC) analysis related to radioactive waste management systems. Chapter 23 provides the specific design of radioactive waste management systems, which are considered in the fault analysis.
Chapter 28 Fuel Route and Storage	Chapter 28 demonstrates that fuel handling and storage system have been substantiated. Analysis related to Fuel Route and Storage faults in Chapter 12 support the ALARP assessment of fuel handling and storage related operations in Chapter 28.
Chapter 31 Operational Management	Chapter 31 provides the arrangement of operating limits and conditions consistent with the safety analysis.
Chapter 33 ALARP Evaluation	Chapter 33 provides the overview of ALARP assessment. Chapter 12 provides the input for risk assessment to support the ALARP evaluation.

12.3 Applicable Codes and Standards

The general principles relevant to the selection of appropriate standards are presented in PCSR Chapter 4 section 4.4.7. Moreover, the detailed principles are presented in Reference [4] and [5].

Wherever possible, the standards applied for design basis conditions analysis should be:

a) Internationally recognised in the nuclear industry;

b) The latest or currently applicable approved standards;

c) Consistent with the plant reliability goals necessary for safety.

Based on the above principles, the applicable codes and standards which are intended to be selected and used in design basis conditions analysis are identified in Reference [6]. According to Reference [6], the main applicable codes and standards for design basis condition analysis are presented as below.

a) IAEA, Format and Content of the Safety Analysis Report for Nuclear Power Plants Safety Guide, Series No. GS-G-4.1, May, 2004.

b) IAEA, Safety Assessment for Facilities and Activities General Safety Requirements Part 4, Series No. GSR Part 4, February, 2016.

c) IAEA, Design of Reactor Containment Systems for Nuclear Power Plants Safety Guide, Series No. NS-G-1.10, September, 2004.

d) IAEA, Design of the Reactor Core for Nuclear Power Plants Safety Guide, Series No. NS-G-1.12, April, 2005.

e) IAEA, Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety Guide, Series No. NS-G-1.9, September, 2004.

f) IAEA, Storage of Spent Nuclear Fuel, Series No. SSG-15, February, 2012.

g) IAEA, Deterministic Safety Analysis for Nuclear Power Plants Specific Safety Guide, Series No. SSG-2, December, 2009.

h) IAEA, Safety Classification of Structures, Systems and Components in Nuclear Power Plants, Series No. SSG-30, May, 2014.

i) IAEA, Safety of Nuclear Power Plants: Design Specific Safety Requirements, Series No. SSR-2/1, February, 2016.

12.4 Fault Identification and Fault Grouping

12.4.1 Introduction of Methodology

A Postulated Initiating Event (PIE) is an event that has the potential to lead to anticipated operational occurrences or accident conditions. Generally, the PIEs can be identified by the methods presented below:

a) Use of analytical methods such as hazard and operability studies, Failure Modes and Effects Analysis (FMEA), and master logic diagrams;

b) Comparison with the list of PIEs developed for safety analyses of similar plants (although this method should not be exclusively used since prior mistakes could also be transferred);

c) Analysis of operating experience data for similar plants.

Due to the limitation of each method mentioned above, the identification of PIEs for UK HPR1000 is a combination of several methods. The detailed methodology is addressed in Reference [7].

12.4.2 Scope of Fault Identification

The PIEs considered for the UK HPR1000 include all foreseeable failures of plant systems and components, as well as operating errors and possible failures arising from internal and external hazards. PIEs consider full power, low power or shutdown states, that occur in the reactor or the fuel pool, or be associated with any other activity or area containing sources of radioactivity.

12.4.2.1 Operation modes

There are six normal operating modes for UK HPR1000 which are:

a) Reactor in Power (RP)

b) Normal Shutdown with Steam Generators (NS/SG)

c) Normal Shutdown with RIS-RHR (NS/RIS-RHR)

d) Maintenance Cold Shutdown (MCS)

e) Refuelling Cold Shutdown (RCS)

f) Reactor Completely Discharge (RCD)

All the 6 operation modes are considered during PIE identification. Furthermore, to facilitate PIE identification, the six normal operating modes are further subdivided into 14 detailed operating states. The relationship between operation modes and detailed operation states is addressed in T-12.4-1.

Events postulated in the safety analysis are supposed to occur during normal plant

operating states. The initiating conditions assumed in the safety analyses cover all the possible standard conditions from full power operation to cold shutdown. The definitions of the safety analysis domains for the UK HPR1000 are provided below.

a) State A: Power states, hot and intermediate shutdown states.

In these states, all the necessary automatic reactor protection functions are available. Some protection functions might be deactivated at low power, but there are always enough automatic protection functions to meet the acceptance criteria in case of a transient condition.

b) State B: Intermediate shutdown with temperature above 140℃.

When the temperature is above 140℃, in normal operation, the Safety Injection System (RIS [SIS]) is not connected in residual heat removal (RHR) mode to the Reactor Coolant System (RCP [RCS]). In this state, some automatic reactor protection functions available in state A may be deactivated.

c) State C: Intermediate shutdown and cold shutdown conditions when RIS [SIS] is under RHR operation mode.

In this state, the RCP [RCS] is closed or can be closed quickly (e.g., when the ventilation pipe is open) so that the SGs can be used for core heat removal if needed.

d) State D: Cold shutdown with RCP [RCS] open.

Due to the open status of the RCP [RCS], the SGs cannot be used for core decay heat removal.

e) State E: Cold shutdown during refuelling.

f) State F: Cold shutdown with the fuel fully unloaded.

During this state, work is undertaken on RCP [RCS] components. This state does not have to be analysed with regard to core protection.

The complete safety analysis state breakdown is presented in T-12.4 1.

T-12.4-1 Definition of Safety Analysis Domains

Normal operating modes	Standard operating conditions	RCP [RCS] state	Reactor coolant inventory	RCP [RCS] pumps in operation	RCP [RCS] average temperature (°C)	RCP [RCS] pressure (bar abs)	RCP [RCS] boron concentration (ppm)	Rods	Detailed Operating States for PIE Identification	Safety Analysis States for DBC Analysis	
Reactor in power (RP)	Reactor in power	closed	PZR level is at setpoint	3	295≤T≤307	155	Critical boron concentration	Shutdown banks extracted Control banks auto or manual	1	A	
	Hot standby	closed	PZR level is at setpoint	3	295	155	Critical boron concentration	Shutdown banks extracted Control banks manual	2		
Normal shutdown with steam generators (NS/SG)	Hot shutdown	closed	PZR level is at setpoint	3	295	155	CB≥Boron concentration of hot shutdown	Shutdown banks extracted Other rods inserted	3		
	Intermediate shutdown with NS/SG connection Conditions (P≥130bar abs)	closed	PZR level is at setpoint	3	T<295	130≤P<155	CB≥Boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	4		
	Intermediate shutdown with NS/SG connection Conditions (P＜130bar abs)	closed	PZR level is at setpoint	3	[T＞135 and 32≤P<130] and [T＞140 and P≤32]		CB≥Boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	5	B1	B
	Intermediate shutdown with RIS-RHR connection conditions	closed	PZR level is at setpoint	3	135≤T≤140	24≤P≤32	CB≥Boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	6	B2	
Normal shutdown with RIS-RHR (NS/RIS-RHR)	Intermediate shutdown with RIS-RHR	closed	PZR level is at setpoint or full	≥1	100≤T≤140	24≤P≤32	CB≥Boron concentration of cold shutdown	Shutdown banks extracted Other rods inserted	7	C1	C
		closed		≥1	10≤T＜100	24≤P≤32	CB≥Boron concentration of cold shutdown		8	C2	
		closed		≥0	10≤T≤60	P≤32	CB≥Boron		9	C3a	

Normal operating modes	Standard operating conditions	RCP [RCS] state	Reactor coolant inventory	RCP [RCS] pumps in operation	RCP [RCS] average temperature (°C)	RCP [RCS] pressure (bar abs)	RCP [RCS] boron concentration (ppm)	Rods	Detailed Operating States for PIE Identification	Safety Analysis States for DBC Analysis
							concentration of refuelling	P＜5bar abs All rods inserted		
	Normal cold shutdown (RCP [RCS] pressurizable)	Non-closed and pressurizable	≥ ¾ loop level	0	10≤T≤60	P≤32	CB≥Boron concentration of refuelling	All rods inserted	10	
Maintenance cold shutdown (MCS)	Normal cold shutdown for maintenance (RCP[RCS] not pressurizable)	Non-closed and not pressurizable, Reactor cavity non fillable	≥ ¾ loop level	0	10≤T≤60	Atmospheric pressure	CB≥Boron concentration of refuelling	All rods inserted	11	C3b
		Non-closed and not pressurizable, Reactor cavity fillable							12	D
Refuelling cold shutdown (RCS)	Normal cold shutdown for refuelling		Reactor cavity flooded	0	10≤T≤60	Atmospheric pressure	CB≥Boron concentration of refuelling	All rods inserted	13	E
Reactor completely discharged (RCD)	Core totally unloaded	---	---	---	---	---	---	---	14	F

12.4.2.2 Sources of Fault

All PIEs having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement are analysed. According to the different sources of radioactive material and SSC sources, the scope of PIE identification includes:

a) Internal event

   1) Internal event (except for loss of support system and for spurious actuation of I&C systems);

   2) Loss of support system; and

   3) Spurious actuation of I&C.

b) Hazard analysis

12.4.3 Process of the Production of DBC List

Based on the methodology described in sub-chapter 12.4.1 and Reference [7], the PIEs are identified with different categories (according to the list in sub-chapter 12.4.2) in parallel.

A number of PIEs are identified but it is not necessary to analyse all PIEs. The PIEs are grouped according to the similarity of the plant (including operator) response, accident mitigation measures, and fault frequency. A bounding case is selected for each PIE group. The DBC list is then established with all the bounding cases. The related process and documents are described and listed in Reference [8]. The identified PIEs are also an input for the PSA IE analysis.

The DBC list can be subdivided into four categories based on the frequency of PIEs and on good practice from other projects or from standards. Acceptance criteria are defined for each category. The four categories are as follows:

a) DBC-1: Normal operation

Operation within specified operational limits and conditions.

b) DBC-2: Anticipated operational occurrences

An operational process deviating from normal operation which is likely to occur at least once during the operating lifetime of a single unit facility but which, because of appropriate design provisions, does not cause any significant damage to items important to safety or lead to accident conditions.

c) DBC-3: Design Basis Condition category 3

Conditions that may occur once during the lifetime of a fleet of operating plants and

may result in the failure of a small fraction of the fuel rods but do not generate a Design Basis Category 4 Condition or result in the consequential loss of function of the Reactor Coolant System (RCP [RCS]) or Containment System.

d) DBC-4: Design Basis Condition category 4

Conditions which are not expected to occur but are postulated because their consequences could include the potential release of significant amounts of radioactive material; they are the most extreme conditions which must be considered in the design and they represent limiting cases.

For comparison with UK context, the DBCs can also be categorised into frequent and infrequent faults, as shown in T-12.4-3. For frequent faults, diverse design needs to be considered.

T-12.4-2 Category for DBCs

UK HPR1000 Design Condition	Frequency (/ry)	UK Context Terminology
DBC-1	≥1	Normal operation
DBC-2	Frequency $\geq 10^{-2}$	
		Frequent faults
DBC-3	10^{-2}> Frequency $\geq 10^{-3}$	
	10^{-3}> Frequency $\geq 10^{-4}$	Infrequent faults
DBC-4	10^{-4}> Frequency $\geq 10^{-5}$	

The fault identification from internal events, loss of support systems and spurious I&C actuation, which includes faults concerning fuel handling and storage, has been completed [8].

12.4.4 Fault List

The list of DBC events for the UK HPR1000 is provided in the sub-chapters below.

12.4.4.1 DBC-1: Normal Operation

The DBC-1 list for the UK HPR1000 is as follows:

a) All steady-state operation, startup and shutdown processes permitted by the nuclear power plant technical specifications during:

1) Power operation;

2) Hot standby;

3) Hot shutdown;

4) Cold shutdown;

5) Reactor refuelling;

6) Reactor start-up and load increase; and

7) Reactor power-reducing and shutdown processes.

b) Permitted operation with temporary deviation in plant parameters or equipment unavailability (or defects) permitted by the power plant technical specifications:

1) Within shutdown equipment or systems;

2) Fuel clad defect;

3) SG tube leakage;

4) Reactor coolant radioactive substance (fission products, corrosion products and tritium) concentration increases; and

5) Tests permitted by the technical specifications.

c) Operating transient:

1) Change in reactor coolant temperature within the rate specified by the technical specifications (excluding normal startup and shutdown);

2) Load ramp within the rates specified by the Technical Specifications;

3) Step change of load within the magnitude specified by the Technical Specifications; and

4) Load shedding (including full load shed to auxiliary power load).

12.4.4.2 DBC-2: Anticipated Operating Occurrences

The DBC-2 list (see Reference [8]) for UK HPR1000 is provided in T-12.4-3.

12.4.4.3 DBC-3: Design Basis Condition category 3

The DBC-3 list (see Reference [8]) for UK HPR1000 is provided in T-12.4-4.

12.4.4.4 DBC-4: Design Basis Condition category 4

The DBC-4 list (see Reference [8]) for UK HPR1000 is provided in T-12.4-5.

T-12.4-3 DBC-2 Conditions Considered in the UK HPR1000

No.	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
1	Decrease in Boron Concentration in Reactor Coolant due to Malfunction of RCV [CVCS], REA [RBWMS] and TEP[CSTS]	A\B\C	FF
2	RCCA Misalignment up to Rod Drop	A\B\C	FF
3	Uncontrolled RCCA Bank Withdrawal at Power	A	FF
4	Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition	A\B\C	FF
5	Spurious Reactor Trip	A\B\C	FF
6	Turbine Trip	A\B	FF
7	Loss of Normal Feedwater Flow	A\B	FF
8	Excessive Increase in Secondary Steam Flow	A\B	FF
9	Inadvertent Opening of One Pressuriser Safety Valve	A	FF
10	Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction	A\B	FF
11	Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction	A\B\C\D\E	FF
12	Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump	A\B\C	FF
13	Spurious Pressuriser Heater Operation	A\B\C	FF
14	Spurious Pressuriser Spray Operation	A\B\C	FF
15	Loss of One PTR [FPCTS] Train	A\B\C\D	FF
16	Increase in Feedwater Flow due to Feedwater System Malfunctions	A\B	FF
17	Startup of One Inactive Reactor Coolant Pump at an Improper Temperature	C\D\E	FF
18	Short Term LOOP of 2 Hours Duration	A\B\C\D\E\F	FF
19	Inadvertent Opening of One SG Relief Train or of One Safety Valve	A\B	FF

No.	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
20	Loss of One RIS [SIS] Train in RHR Mode	C\D\E	FF
21	Loss of RRI [CCWS] or SEC [ESWS] Train A[1]	A\B	FF

[1] New fault identified from loss of support system. The analyses for faults identified from loss of support system are presented in *Analysis for Loss of Support System Events*, Reference [100].

T-12.4-4 DBC-3 Conditions Considered in the UK HPR1000

No.	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
1	Rupture of a Line Carrying Primary Coolant outside Containment	A\B\C\D\E	IFF
2	Inadvertent Core Loading of Fuel Assemblies	A\B\C\D\E	IFF
3	Uncontrolled Single RCCA Withdrawal	A\B\C	FF
4	Inadvertent Closure of One or All Main Steam Isolation Valves	A\B	FF
5	Feedwater System Piping Small Break Including Breaks in Connecting Lines to SG	A\B	FF
6	Reduction in Feedwater Temperature due to Feedwater System Malfunctions	A\B	IFF
7	Steam System Piping Small Break Including Breaks in Connecting Lines	A\B	FF
8	Uncontrolled RCP [RCS] Level Drop	C\D\E	FF
9	SG Tube Rupture (One Tube)	A\B\C	FF
10	Small Break - Loss of Coolant Accident	A	FF
11	Forced Reduction in Reactor Coolant Flow (3 Pumps)	A\B\C	FF
12	Loss of One PTR [FPCTS] Train	E\F	FF
13	Isolatable Piping Failure on a System Connected to Spent Fuel Pool	A\B\C\D\E\F	IFF
14	Medium Term LOOP of 24 Hours Duration	A\B\C\D\E\F	FF
15	LOOP (>2 hours) Affecting Fuel Pool Cooling	A\B\C\D\E\F	FF
16	Inadvertent Opening of One Pressuriser Safety Valve	B\C	IFF
17	Volume Control Tank break[2]	A\B\C\D\E\F	IFF
18	Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinets Rooms of Safeguard Building Division B[3]	A\B	FF
19	Loss of RRI [CCWS] or SEC [ESWS] Train A[4]	C\D\E	FF

[2] New fault identified from loss of support system.
[3] New fault identified from loss of support system.
[4] New fault identified from loss of support system.

T-12.4-5 DBC-4 Conditions Considered in the UK HPR1000

No.	Event Description	Safety Analysis States	Frequent Fault (FF) or Infrequent Fault (IFF)
1	Dropping of Spent Fuel Cask	A\B\C\D\E\F	IFF
2	Spectrum of RCCA Ejection Accident	A\B	IFF
3	Steam System Piping Large Break	A\B	IFF
4	Intermediate Break and up to Surge Line Break - Loss of Coolant Accident	A\B	IFF
5	Small Break - Loss of Coolant Accident	B	IFF
6	Small Break - Loss of Coolant Accident	C\D\E	IFF
7	SG Tube Rupture (Two Tubes in One SG)	A\B\C	IFF
8	RHR System Piping Break inside or outside Containment	C\D\E	IFF
9	Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break	A\B\C	IFF
10	Long Term LOOP of 168 Hours Duration	A\B\C\D\E\F	IFF
11	Dropping of Fuel Assembly	A\B\C\D\E\F	IFF
12	Non Isolable Small Break or Isolable RIS [SIS] Break Affecting Fuel Pool Cooling	E	IFF
13	Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG	A\B	IFF
14	Inadvertent Opening of Severe Accident Dedicated Valves (One Train)	A\B\C	IFF
15	Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinets Rooms of Safeguard Building Division B[5]	C	IFF

[5] New fault identified from loss of support system.

12.4.5 Relationship with Diverse Protection Line

Under UK context, Common Cause Failures should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability for frequent faults (with frequency exceeding 10E-3 /ry).

Considering that the fault sequence frequency of 1E-07 /ry is the cut-off when applying design basis techniques, the safety systems claimed for frequent faults require a combined failure per demand of less than 10E-4. This means that the safety systems need to be diversified. This requires the implementation of a diverse protection line for frequent faults identified in fault schedule.

DBCs and diverse protection lines are defined as the design basis in UK which are subjects of PCSR Chapter 12. DEC-A and diverse protection line are both concept for risk reduction. DEC-A concept is inherited from FCG3 while diverse protection line is a concept from UK practice. Some sequences are the same in these two practices.

Previous studies on DEC-A and diverse protection show that part of the DEC-A analysis (frequent fault combined with CCF of the first line of protection) can be used to support the diverse protection line demonstration for UK HPR1000. The detailed analysis for DEC-A is shown in Sub-chapter 13.4.5. Other demonstrations of diverse protection line are described in Sub-chapter 12.10.

12.4.6 Specific Studies

Specific studies are the events that are excluded from DBC but needed to carry out additional analysis on the terms of defence in depth. They are studied to justify the safety margins of some systems and components and to ensure that there is no cliff edge effect.

Specific studies are identified for those PIEs that cannot be bounded by the presented DBC and DEC-A list. The specific studies (see Reference [8]) are listed in T-12.4-6.

T-12.4-6 List of Specific Studies

---	No.	PIEs with Specific Studies	Safety Analysis States	Remark
Spurious I&C Actuation	1	Spurious actuation of one or more ASG [EFWS] trains	A/B	With RPS [PS] and Safety Automation System (SAS) unavailable
	2	Spurious actuation of one or more ASP [SPHRS] trains	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	3	Spurious actuation of the GCT [TBS] MCD function and RIS	A/B	With RPS [PS] and SAS

---	No.	PIEs with Specific Studies	Safety Analysis States	Remark
		[SIS] injection function with large miniflow line closed		unavailable
	4	Spurious opening of one or more VDA [ASDS] trains	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	5	Spurious isolation of all main feedwater	A/B	With RPS [PS] and SAS unavailable
	6	Spurious isolation of all RHR trains	C/D/E/F	With RPS [PS] and SAS unavailable
	7	Spurious isolation of one or more steam lines	A/B	With RPS [PS] and SAS unavailable
	8	Spurious shutdown of all the reactor coolant pumps	A/B/C	With RPS [PS] and SAS unavailable
	9	Spurious isolation of RCV [CVCS] letdown due to isolation of the containment at stage A	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	10	Spurious actuation of one or more MHSI trains with large miniflow line closed	B	With RPS [PS] and SAS unavailable
	11	Spurious actuation of one or more MHSI trains with large miniflow line open	C/D/E/F	With RPS [PS] and SAS unavailable
	12	Spurious opening of one PSV	C/D/E/F	With RPS [PS] and SAS unavailable
	13	Spurious opening of the letdown line or isolation of the charging line of RCV [CVCS]	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	14	Spurious start-up of all the pressuriser heaters	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	15	Spurious opening of the pressuriser auxiliary spray line	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	16	Spurious isolation of one or more PTR [FPCTS] cooling trains	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
	17	Total loss of RRI [CCWS] due to a certain spurious actuation	A/B/C/D/E/F	With RPS [PS] and SAS unavailable
Loss of	18	Loss of Two RRI [CCWS] or	A\B\C\D\E\F	This PIE contains two

---	No.	PIEs with Specific Studies	Safety Analysis States	Remark
Support Systems		SEC [ESWS] Trains		events: a) Loss of RRI [CCWS] or SEC [ESWS] train A and train C; b) Loss of RRI [CCWS] or SEC [ESWS] train A and train B, Reference [2].
	19	Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room (DVL [EDSBVS] 4510/4520CL- and DVL [EDSBVS] 5510/5520CL-)	C	---
Other	20	Double-ended Guillotine Failure of Largest RCS Pipe	A	---
	21	Main Steam Line Large Break (Pipe with HIC classification)	A\B	---

12.5 DBC Accident Analysis Rules

This sub-chapter describes the rules which are followed for the DBC accident analysis. Sub-Chapters 12.5.1 to 12.5.9 provide the general requirements for reactor faults. Sub-Chapter 12.5.10 presents the specific rules for events associated with the spent fuel pool. The analysis rules for diverse protection line are presented in Sub-Chapter 12.10.

12.5.1 Acceptance Criteria

Acceptance criteria are assigned to each DBC accident or incident (or family of accidents or incidents), Reference [8]. Compliance with these acceptance criteria ensures that the safety objectives relevant to the DBC accident or incident are met.

The acceptance criteria include safety criteria and decoupling criteria.

a) Safety criteria

Safety criteria are defined in terms of radiological limits. They have to be met in the safety analysis.

The radiological consequences will be evaluated against Radiation Protection Target 4 (RPT-4), see Sub-chapter 4.4.

Data and assumptions used for radiological calculations are described in the section related to radiological consequences, see Sub-chapter 12.11.

b) Decoupling criteria

In addition to safety criteria, it is convenient for practical purposes to introduce some decoupling criteria, which can be applied to the thermal hydraulic and neutronic calculations. In this way, the thermal hydraulic and neutronic calculations, and the radiological calculations, can be decoupled and carried out separately.

Decoupling criteria relate to integrity of barriers to releases of radioactivity. Sufficient conservatism is included to ensure that there are adequate safety margins to the loss of integrity of the barrier. Meeting the decoupling criteria guarantees an acceptable level with respect to the integrity of barriers under accidental conditions. For all DBC faults, decoupling criteria typically ensures at least one barrier remains intact, which significantly contributes to the respect of safety criteria.

Decoupling criteria should be met under application of all “DBC analysis rules”.

The following decoupling criteria are used in the DBC-2 analyses:

Fuel integrity shall be ensured (no Departure from Nucleate Boiling (DNB) and no fuel melting).

1) The Departure from Nucleate Boiling Ratio (DNBR) shall be greater than the design limit which is described in Sub-section 5.6.2.1;

2) The fuel temperature shall be lower than the fuel melting temperature of { }℃.

The following decoupling criteria are used in the DBC-3 and DBC-4 analyses:

1) For DBC-3 and DBC-4 events (Loss of Coolant Accident (LOCA) excluded), the amount of fuel rods experiencing DNB must remain lower than 10% (DBC-3 and DBC-4).

2) In the DBC-3 and DBC-4 analyses, the fuel pellet melting at the hot spot must not exceed 10% (DBC-3 and DBC-4 excluding LOCA) by volume, i.e. considering a cross section of the hottest fuel rod at the elevation of the power peak, less than 10% (DBC-3 and DBC-4) of this area is allowed to reach the melting temperature. However, for the analysis of some DBC-3 and DBC-4 faults, the criteria of no DNB and no fuel melting are still applied.

3) For cases not involving the rapid transient of oxidation of the cladding, the peak cladding temperature must remain lower than 1482℃.

4) For UK HPR1000, no fuel failure is considered as an additional criterion for frequent faults and is demonstrated [9] including no fuel melting, no Pellet-Cladding Interaction - Stress Corrosion Cracking (PCI-SCC) induced failure, no cladding bursting failure, no DNB occurrence and no Pellet-Cladding Mechanical Interaction (PCMI) induced failure.

5) Moreover, the decoupling criteria for a rod ejection accident are:

   - The enthalpy of fuel pellet must be less than the design limit (942 J/g for non-irradiated fuel and 837 J/g for irradiated fuel).

   - {

     }

6) The decoupling criteria for LOCA events:

   - The peak cladding temperature must remain lower than 1204℃.

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

   - The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding

had reacted.

- The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling.
- The long-term core cooling shall be ensured, i.e. the calculated core temperature shall be maintained at an acceptably low value and decay heat shall be removed.

7) Under the safe state, the plant shall be maintained in a sub-critical state.

In addition, protection against primary and secondary system overpressures is discussed in Sub-chapter 6.6 and containment integrity is discussed in sub-chapter 7.4.1.

12.5.2 Definition of States

The safety analysis must be performed up to a safe condition. Two states are defined: the controlled state and the safe state.

For each DBC-2/3/4 event, it shall be demonstrated that the controlled state can be reached. The analysis of the transition from controlled state to safe state can be performed by grouping similar transient causes and PIEs.

a) Controlled state

This is the plant state, following an anticipated operational occurrence or accident conditions, in which the fundamental safety functions can be ensured and which can be maintained for a time sufficient to effect provisions to reach a safe state. Under this state, the main characteristics are as follows:

1) The core remains sub-critical;
2) The residual heat removal can be ensured for a time sufficient to implement provisions to reach a safe state;
3) The core inventory remains stable;
4) Radioactive releases remain tolerable.

For the assumptions of most events, the reactor is at a sub-critical state when the emergency shutdown happens, and the core remains sub-critical after shutdown. Examples are provided below:

1) For DBC-2 events, the controlled state is:
   - During a controlled state, the core remains sub-critical by inserting the control rods under reactor trip signal;
   - Between the controlled state and the safe state, during the RCP [RCS] cooling process, the operators can maintain the sub-critical state.

2) For small break LOCA cases, the controlled state is:

- The break flow can be compensated;
- The heat in RCP [RCS] can be evacuated;
- The heat in the In-containment Refuelling Water Storage Tank (IRWST) can be evacuated;
- Under a controlled state and safe state, core sub-criticality needs to be ensured.

b) Safe state

This is the plant state, following an anticipated operational occurrence or accident conditions, in which the reactor is subcritical and the fundamental safety functions can be ensured and maintained as stable in the long term. Under this state:

1) The core remains sub-critical, even after Xenon burn-off;
2) The residual heat is evacuated;
3) Radioactive releases remain tolerable.

12.5.3 Methodology

The transient analysis uses calculation codes that are appropriate for the relevant physical phenomena, which are implemented to ensure conservative results.

The methodology for DBC analysis comprises the following steps:

1) Define initiating event;
2) Identify key physical phenomena and confirm selected computer codes are appropriate to perform the studies;
3) Identify analysis assumptions including dominant parameters, uncertainties and conservatisms, within the calculations.

Uncertainties are considered either:

1) In a deterministic manner for each dominant parameter considered as conservative value; or
2) In a statistical manner with the uncertainties in several parameters statistically combined.

The Rod Cluster Control Assembly (RCCA) having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip.

A DBC study must show that the safety criteria are met with a high confidence level,

of at least 95%.

12.5.4 Initial Conditions

The initial conditions for DBC analyses correspond to a steady state operation.

The safety analysis domains for DBC are described in Sub-chapter 12.4.

Within the given safety analysis domain, the most pessimistic operating condition is considered with regard to the fulfillment of the DBC acceptance criteria, e.g. full power operation for LOCA in state A, or the maximum RCP [RCS] pressure of { } for LOCA in state C (RIS [SIS] operation in RHR mode).

The physical parameters are within the limits provided by the plant controls. A conservative combination of parameters is considered including uncertainties, dead bands and response times. For each DBC event, the most conservative case is analysed.

The list of DBC events covers all plant operating conditions, including shutdown states, as potential initial conditions before the occurrence of initiating events.

12.5.5 Rules for Operator Actions

The transient can be divided into an automatic phase and a manual phase. The differences between these two phases are as follows:

a) Automatic phase means the transient between occurrence of an incident and the first manual action.

b) Manual phase means the transient between the first manual action and the safety shutdown.

   During the manual phase, operator actions need to be considered in addition to automatic actions. The assumption for operator actions is as follows:

   1) A manual action from the Main Control Room (MCR) is assumed to take place, no earlier than 30 minutes after the first significant information is transmitted to the operator;

   2) A local manual action, i.e. a manual action that must be performed outside the MCR, is assumed to take place no earlier than one hour after the first significant information is transmitted to the operator.

For most cases, the controlled state can be achieved with automatic actions. However, manual actions are also allowable when the grace period condition is met.

The operators must follow the rules for emergency operation. In the DBC analysis, operator errors are not considered. Feedback from human factors will be taken into account if appropriate.

12.5.6 Safety Classification of Mechanical, Electrical and I&C Systems

The safety classification concept and related wording are defined in PCSR Chapter 4 section 4.4.

In DBC analysis, the safety classification of systems can be divided as follows:

a) Safety Category 1 Function (F-SC1) systems and Safety Category 2 Function (F-SC2) systems;

b) Safety Category 3 Function (F-SC3) systems and Non-Classified (NC) systems.

12.5.6.1 F-SC1, F-SC2 Systems and Functions

Conservative performance of the F-SC1 and F-SC2 systems are considered in DBC analyses, i.e., the most pessimistic system efficiencies of the F-SC1 and F-SC2 systems are considered including the following aspects:

a) Conservative uncertainties on equipment characteristics;

b) Conservative uncertainties on actuation of signals;

c) The most pessimistic environmental conditions.

It shall be shown in the DBC analyses that:

a) The controlled state can be reached relying only on F-SC1 systems;

b) The transition from the controlled state to the safe state can be done relying only on F-SC1 and/or F-SC2 systems.

12.5.6.2 F-SC3 and NC Systems

The following principles apply to F-SC3 and NC systems used in the DBC analysis:

a) If the transient leads to the actuation of an F-SC3 or NC system, and if the operation of this system would have a beneficial effect with regard to a safety criterion, the DBC analysis shall be performed without considering this system;

b) If the transient leads to the actuation of an F-SC3 or NC system, and if this system worsens the consequences of the transient with regard to a safety criterion, the DBC analysis shall be performed assuming the system is operating normally;

   For example: Following loss of main feedwater, the pressuriser main spray should be considered to operate normally when calculating the minimum DNBR.

c) If the transient has no impact on F-SC3 or NC system performance (no change of status, no change of operating and environmental conditions), and if the system were operating prior to the initiating event, the system is assumed to continue in normal operation.

   For example: Chemical and Volume Control System (RCV [CVCS]) charging is

F-SC3 safety classified. If RCV [CVCS] charging is supposed to be in operation before Steam Generator Tube Rupture (SGTR) happens, it is assumed to continue in operation during the transient until it is isolated.

d) More generally, an F-SC3 or NC system is assumed either to work correctly or not to work at all. Spurious operation is not considered in the DBC analyses.

   For example, when considering the RCV [CVCS], the charging pumps are supposed to function as intended, or not at all.

e) Turbine isolation valves are not F-SC1 or F-SC2 classified, but they are considered to close normally after a reactor trip. This is justified because they are redundant in series. The situation described above is its design condition, and they are designed as “fail safe”. After the turbine trip, the disconnection of the main power generator is also assumed to be effective.

12.5.7 Application of the Single Failure Criterion (SFC) in the Safety Analysis

For the DBC analyses, the term single failure is considered as any active or passive failure, independent of the postulated initiating event, which affects all or part of equipment used in the analysed transient.

In system design, this concept is considered under the same conditions as described in the universal design safety criterion (see Sub-chapter 4.4.5), and the following aspects are considered:

a) If FC1 and FC2 functions can be fulfilled by more than one safety system, including equipment or auxiliary systems, the single failure must be applied to these systems only once;

b) For passive single failure, it must be verified in the DBC analysis that a single failure in the form of a leak at any location in the pressure boundary and its consequential failure do not prevent the performance of the required safety function.

In DBC analyses, the following additional rules are applied:

a) The most pessimistic single failure must be assumed to occur anywhere in the systems needed to perform the safety function.

b) Consequential failures resulting from the assumed failure must be considered in single failure criteria.

c) If necessary, a sensitivity analysis must be performed for a given initial event with the application of the SFC to different components. The purpose is to determine the worst-case single failure with regard to safety criteria.

d) The active single failure must be considered from the beginning of the analysis. For UK HPR1000, a single failure of passive components within systems that

deliver FC1 or FC2 safety functions is assessed at the start of a transient. Additional analysis to consider passive single failure from the beginning of accident is carried out and described in Reference [10].

e) Any exception with respect to the single failure must be stated and justified.

f) The spurious opening of a safety valve is considered as an initial event.

g) The non-closure of a safety valve after actuation is considered as an application of the SFC.

12.5.8 Loss of Off-Site Power (LOOP)

LOOP due to turbine trip shall be considered for DBC-2, DBC-3 and DBC-4 accidents at power where it is conservative to do so. After LOOP, the Emergency Diesel Generators (EDGs) are actuated automatically and the related safety systems will be powered by EDG to ensure the accidents could be mitigated successfully.

12.5.9 Preventive Maintenance

For DBCs, the preventive maintenance activity can be carried out only when the safety function's availability and redundancy requirements are satisfied. Examination, Maintenance, Inspection and Testing (EMIT) window is arranged compliant with requirements from safety analysis. Particularly, conflict between EMIT strategy and safety requirements on EDG and PTR [FPCTS] is found in the review process. Through rearrangement of EMIT strategy and improvement on safety measures, the consolidated EIMT strategy is consistent with safety requirements [11].

12.5.10 Analysis Rules Specific to DBC Events Associated with the Fuel Storage Pool

This section provides acceptance criteria, definitions, initial conditions and the analysis rules of accidents associated with the fuel storage pool. Due to the specific characteristics of the fuel storage pool, such as operating at low pressure, the physical parameter changes in the accidental transient are very low when compared to those affecting the core in the reactor building. The acceptance criteria and analysis rules are consequently adapted and are described in the sub-sections below.

12.5.10.1 Acceptance Criteria

The acceptance criteria for the DBC-2/3/4 transients related to the fuel storage pool are as follows:

a) Permanent maintenance of sub-criticality;

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

12.5.10.2 Definition of States

a) Controlled State

The controlled state is a state in which the decay heat removal is ensured in the short term. For the fuel storage pool without draining events, because of the long grace period before fuel exposure, the controlled state can be considered as being reached from the start. For the fuel storage pool with draining events, the controlled state is reached when the fuel pool water inventory is stabilised, after the draining has been stopped and no fuel assemblies have been exposed.

b) Safe state

The safe state is a state where the decay heat of the fuel assemblies in the fuel storage pool is reliably removed in the long term and water inventory of SFP is stabilised to assure that the fuel assemblies are covered with water.

For each DBC-2/3/4 fuel storage pool related transient, it must be demonstrated that the safe state can be reached and maintained.

12.5.10.3 Initial Conditions

The initial conditions for DBC analyses correspond to a steady state operation. Three initial conditions are considered in the spent fuel pool DBC events.

a) Refuelling

After the total unloading of the core, the pool is filled with the following fuel assemblies: fuel assemblies just unloaded; new fuel assemblies (for the following cycle); and fuel assemblies unloaded from cycles previous to the most recent.

b) Beginning of cycle (BOC)

The fuel assemblies in the fuel storage pool are as per the ‘refuelling’ state, minus those that have just been loaded in the core for the cycle to come.

c) End of cycle (EOC)

Fuel assemblies are the same as those for BOC, but preventive maintenance performed at this stage when the decay heat is at its lowest is considered.

To maximise the pool temperature reached at the end of the transient, the transient analyses consider uncertainties in the decay heat value.

12.5.10.4 Analysis Rules

12.5.10.4.1 Rules for Operator Actions

In the DBC analysis associated with the fuel storage pool, the rules for operator action are consistent with the rules specified for DBC accident analysis in Sub-section 12.5.5.

12.5.10.4.2 Mechanical, Electrical and I&C Systems used in DBCs Analysis

It is shown in the DBC analyses associated with the fuel storage pool that:

a) The controlled state can be reached relying only on F-SC1 systems;

b) The transition from the controlled state to the safe state can be done relying only on F-SC1 and/or F-SC2 systems.

12.5.10.4.3 Application of the Single Failure Criterion (SFC) in the Safety Analysis

For the DBC analysis associated with the spent fuel storage pool, the term single failure will be understood as any active failure, independent of the postulated initiating event, which affects all or part of the equipment used in the analysed transient. It applies to equipment that needs a change of state to fulfil its function and that has beneficial effects on the transient.

Passive single failures are not considered for the PTR [FPCS] as part of the DBC analysis associated with fuel storage pool because of the specific characteristics of the fuel storage pool cooling system, such as operating at low pressure, and use of an in-service inspection program.

12.5.10.4.4 Preventive Maintenance

PTR [FPCS] preventive maintenance is programmed at a state when the grace period for SFP boiling in the fuel storage pool is sufficiently long for maintenance. The time taken for SFP boiling to start depends on both the decay heat and the cooling water temperature.

In the DBC analysis, preventive maintenance for the PTR [FPCS] train is assumed to be performed under EOC conditions, when the decay heat in the fuel storage pool is at its lowest.

During the refuelling stage, PTR [FPCS] preventive maintenance is not performed. However, maintenance of the supporting systems may be carried out during these periods. To keep different trains separate and independent, suitable measures must be implemented on the support systems.

12.5.10.4.5 Loss of Offsite Power (LOOP)

Loss of offsite power is not considered in the DBC safety analysis associated with fuel storage pool. The occurrence of initiating events associated with the fuel storage pool does not affect the core in the reactor building and does not cause the turbine trip. LOOP as an initiating event has been included in the fault list associated with the fuel storage pool.

12.6 Plant Characteristics taken into account in Accident Analyses

12.6.1 Plant Level Parameters

12.6.1.1 Plant Geometry Data

T-12.6-1 lists the main geometry data of the RCP [RCS] (see Reference [12]).

12.6.1.2 Plant Initial Conditions

Initial conditions of the fault analysis are obtained by considering maximum steady state uncertainties in a pessimistic way: adding or subtracting maximum steady state uncertainties to or from nominal values. The steady state uncertainties include the measurement uncertainties, the steady state fluctuations, and the control dead band (if applicable).

The main technical parameters are summarised in Reference [12] including the nominal values for the following relevant parameters:

a) Core power

b) PZR pressure

c) RCP [RCS] average temperature

d) PZR level

e) SG level

f) Flowrate

The maximum steady state uncertainties for initial conditions adopted in the accident analyses are summarised in Reference [13].

The transient response of the RCP [RCS] is related to the initial power distribution. The nuclear design of the reactor core minimises adverse power distribution through adequate positioning of the control rods and adherence to operating instructions.

The most unfavourable power distributions that can occur during normal operation are considered as initial conditions for the transient studies.

T-12.6-1 Main Geometry Data of RCP [RCS]

Number of fuel assemblies in reactor core	177 (17×17 type)
Number of fuel rods per assembly	264
Core active height	3.6576 m
Volume of PZR	67 m^3
Total volume of RCP [RCS]	357.5 m^3
Inner diameter of surge line	0.284 m
Inner diameter of main coolant line	0.760 m

Note: The above data is based on the cold condition of the RCP [RCS].

12.6.2 Core related Parameters

Generic core related parameters used in transient analysis are introduced in this section. Specific neutronic parameters are used when using generic core related parameters is not appropriate or too conservative. Specific neutronic parameters are introduced in detailed fault analysis section when adopted.

12.6.2.1 Reactivity Coefficients

The transient response of the reactor is related to reactivity feedback effects, in particular the moderator density coefficient and the Doppler power coefficient. These reactivity coefficients and their values are discussed in Sub-chapter 5.5.

In the analysis of some events, conservatism requires the use of maximum reactivity coefficient values, whereas for others, conservatism requires the use of minimum reactivity coefficient values. The values used are given in T-12.6-2.

RCP [RCS] boron concentration for the initial state (nominal operating conditions), and required boron concentration for the RIS [SIS] in RHR mode are provided in T-12.6-3.

T-12.6-2 Reactivity Coefficients (conservative values set for point kinetic model for UO_2 fuel management)

	Minimum	Maximum
Prompt neutron generation time	13.5 μs	31 μs
Fraction of delayed neutrons	440 pcm	750 pcm
Moderator density coefficient	0 (Δk/k)/(g/cm^3)	0.58 (Δk/k)/(g/cm^3)
Doppler temperature coefficient	-4.65pcm/℃	-1.8pcm/℃
Doppler power coefficient	-12.4 pcm/%FP at 100%FP	-5.2 pcm/%FP at 100%FP
	-12.9 pcm/%FP at 80%FP	-5.5 pcm/%FP at 80%FP
	-15.0 pcm/%FP at 60%FP	-5.7 pcm/%FP at 60%FP
	-18.6 pcm/%FP at 40%FP	-6.1 pcm/%FP at 40%FP
	-23.5 pcm/%FP at 20%FP	-6.5 pcm/%FP at 20%FP
	-29.8 pcm/%FP at 0%FP	-6.9 pcm/%FP at 0%FP

T-12.6-3 RCP [RCS] Boron Concentrations

Plant conditions	EOC	BOC
Nominal operating conditions (full power)	~ 6 ppm (35% concentrated ^{10}B)	575 ppm (first cycle) / 1021 ppm (equilibrium cycle) (35% concentrated ^{10}B)
RIS [SIS] in RHR mode	1300ppm (35% concentrated ^{10}B)	1300ppm (35% concentrated ^{10}B)

12.6.2.2 Design Hot Channel Factor

The design hot channel factor used in the safety analysis depends on a transient study (related to uncertainties). The power distribution may be characterised by the enthalpy rise hot channel factor $F_{\Delta H}$ and the heat flux hot channel factor F_Q. The values are given below:

a) Enthalpy rise hot channel factor $F_{\Delta H}$=1.65

b) Heat flux hot channel factor F_Q=2.45

12.6.2.3 Power Distribution

The transient response of the reactor system is related to the initial power distribution. The nuclear design of the reactor core minimises adverse power distribution by adequate positioning of control rods and adherence to operating instructions. The power distribution may be characterised by the total enthalpy rise factor $F_{\Delta H}$ and the total peaking factor F_Q. Peak factor limits are defined in Sub-chapter 5.5.

For transients which may be DNB limited, $F_{\Delta H}$ is of high importance. The $F_{\Delta H}$ value increases with decreasing power levels due to control rod insertion. All transients that may be DNB limited are assumed to begin with an $F_{\Delta H}$ value to be taken into account into Technical Specifications.

The axial power shape used in the DNB calculation is discussed in Sub-chapter 5.5.

For transients, which may be overpower limited, the F_Q is of importance. These transients are assumed to begin with plant conditions, including power distributions, which are consistent with reactor operation as defined in the Technical Specifications.

For overpower transients which are slow with respect to the fuel rod thermal response, fuel rod thermal evaluations are determined as discussed in Sub-chapter 5.4.

For overpower transients which are fast with respect to the fuel rod thermal response (for example, the uncontrolled rod cluster control assembly bank withdrawal during subcritical conditions, and rod cluster control assembly ejection incidents which result in a large power rise over a few seconds), a detailed fuel heat transfer calculation is performed.

12.6.2.4 Fission Power and Decay Heat after Reactor Trip

This sub-chapter describes the method for fission power and decay heat calculation after reactor trip, Reference [14].

The residual heat in a subcritical core can be split into three terms:

a) The residual thermal power generated by residual fissions (A term)

b) The heat came from the decay of capture products U-239 and Np-239 (B term)

c) The heat produced from the decay of fission products and actinides excluding U-239 and Np-239 (C term)

The residual thermal power of A term is defined by the number of neutrons, whose sources are classified as follows:

a) The decay of delayed neutron precursors

b) The spontaneous fissions of actinides

c) The (α, n) reactions

The residual thermal power due to the decay of fission products and actinides (B+C term) depends on the amount of these products at the moment of RT. The main parameters that have an influence on the nuclide composition in the core are linked to the fuel type and to the fuel management. They are:

a) The initial fuel enrichment

b) The number of fuel assemblies in the core

c) The enrichment and the burnup of the different fuel assemblies

d) The burnup history (irradiation sequences) of each fuel assembly (cycle length, specific irradiation power)

Uncertainties are considered in the calculation of the residual heat of B+C terms:

1) +1.645σ uncertainty

2) +2σ uncertainty

A time-dependent rod reactivity worth curve is defined based on the decoupling dropping characteristics shown in T-12.6-4.

T-12.6-5 RCCA Dropping Characteristics

Total dropping time (maximum)	4.20s (with earthquake) 3.00s (without earthquake)

12.6.3 I&C Signals

I&C signals considered in the DBC accident analysis include reactor trip signals (FC1) and safety systems actuation signals (FC1/FC2). Some non-FC1\FC2 signals may be accounted for if in accordance with the accident analyses rules.

The signals and thresholds for reactor trip considered in the DBC accident analyses are listed in Table T-12.6-5.

The FC1 and FC2 signals related to the Primary and Secondary (P/S) systems used in the DBC accident analyses are listed in Table T-12.6-6, with mention of the setpoints and their associated uncertainties. Some F-SC1 systems that are not actuated by the I&C signals, such as the PZR safety valves and main steam safety valves (MSSVs), are also listed.

The manual FC2 actions are not listed in this sub-chapter. These actions are mentioned in the relevant sub-chapters on accident analysis.

The most conservative time delay is considered for the actuation of a signal and completion of the resulting action. The safeguard actions delays considered in the DBC accident analyses are listed in T-12.6-7.

T-12.6-6 Reactor Trip Protection Thresholds

Signal	Threshold	Delay, s	Uncertainties
High neutron flux (intermediate range)	25 %FP	0.7	10 %FP
High neutron flux (power range, low setpoint)	25 %FP	0.7	10 %FP
High neutron flux (power range, high setpoint)	109 %FP	0.7	9 %FP
High positive neutron flux rate	5 %FP	0.7	1.00 %FP
High negative neutron flux rate	-5 %FP	0.7	-1.00 %FP
Overtemperature ΔT and Overpower ΔT	See reference [15]	1.0	See reference [15]
Low flow rate in two primary loops	88.80% nominal flowrate	1	3% nominal flowrate
Low flow rate in one primary loop	88.80% nominal flowrate	1	3% nominal flowrate
Low-low RCP speed	91.90% nominal speed	0.7	-0.70% nominal speed
PZR pressure low 2	13.5 MPa	1.3	normal conditions: 0.1 MPa degraded conditions: 0.5 MPa
PZR pressure high 2	16.62 MPa	1.3	normal conditions: 0.1 MPa degraded conditions: 0.5 MPa
PZR level high 1	80.00%	1.9	normal conditions: 2.5% degraded conditions:11%
SG pressure drop high 1	-0.5 MPa/min, initial pressure -0.7 MPa	1.3	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
SG pressure low 1	5.0 MPa	1.3	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
SG pressure high 1	8.6 MPa	1.3	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
Containment pressure high 1	0.123 MPa	1.3	normal conditions: 0.02 MPa degraded conditions: 0.02 MPa

T-12.6-7 FC1 and FC2 Signals (P/S related)

PZR pressure		
Action	Threshold	Uncertainties
3rd Pressuriser Safety Valve (PSV) opening (closing)	17.7 MPa (90% opening threshold)	± 0.15 MPa
2nd PSV opening (closing)	17.4 MPa (90% opening threshold)	± 0.15 MPa
1st PSV opening (closing)	17.1 MPa (90% opening threshold)	± 0.15 MPa

SG pressure			
	Action	Threshold	Uncertainties
High 1	Reactor trip, Turbine trip	8.6 MPa	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
Low 1	Reactor trip, Turbine trip	5 MPa	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
Low 2	Main Feedwater System (ARE [MFFCS]) isolation	4 MPa	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
Low 3	Atmospheric Steam Dump System (VDA [ASDS]) isolation	4 MPa	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa
Low 4	Charging line isolation	3.5 MPa	normal conditions: 0.15 MPa degraded conditions: 0.5 MPa

T-12.6-8 Safeguard Actions Delay

Safeguard action	Delay (maximum)	Note
Medium Head Safety Injection (MHSI) & Low Head Safety Injection (LHSI)	17 s	Delay in Safety Injection (SI) pump start-up to full flowrate after SI signal (without LOOP)
MHSI	38 s	Delay in SI pump start-up to full flowrate after SI signal (with LOOP)
LHSI	33 s	Delay in SI pump start-up to full flowrate after SI signal (with LOOP)
Emergency Feedwater System (ASG [EFWS]) actuation	15 s	Delay in pump start-up to full flowrate after ASG signal (without LOOP)
	55 s	Delay in pump start-up to full flowrate after ASG signal (with LOOP)
ARE [MFFCS] full load isolation	5.0 s	Valves closing delay
ARE [MFFCS] low load isolation	20 s	Valves closing delay
ASG [EFWS] isolation	60 s	Valves closing delay
RCV [CVCS] letdown line isolation	35 s	Valves closing delay
RCV [CVCS] charging line isolation	40 s	Valves closing delay
MSIV closure	5.0 s	Valves closing delay
VDA [ASDS] opening	1.8 s	VDA IV opening delay
VDA [ASDS] isolation	20 s	VDA IV closing delay
RCP [RCS] pumps cut-off	0.15 s	Breaker opening delay
Turbine trip	2.2s (minimum) 4.2s (maximum)	Delay between reactor trip signal and turbine trip signal

12.6.4 Safety Systems Functions and Characteristics

This sub-chapter lists the characteristics of the safety systems used to mitigate the consequences of a DBC accident.

The FC1 and FC2 mechanical and fluid systems accounted for in the DBC accident analyses include:

a) The core control and shutdown rods, performing RTs

b) The RCP [RCS] and SG isolation valves

c) The RCP [RCS] and SG fluid systems performing injection

d) The RCP [RCS] and SG fluid systems performing pressure relief

e) The RCV [CVCS] control tank isolation valves

These systems are designed according to the conservative DBC analyses rules defined in Sub-chapter 12.5:

a) Minimum guaranteed efficiency

b) Consideration of the worst-case single failure

The FC1 systems/functions involved in accident analyses are:

a) RT

b) RGL[RPICS] Bank R position low 3 monitor

c) RIS [SIS] (MHSI, LHSI, accumulators, In-containment Refuelling Water Storage Tank (IRWST))

d) PSV

e) VDA [ASDS]

f) MSSV

g) MSIV

h) ASG [EFWS] actuation

i) ASG [EFWS] isolation

j) Containment/RCP [RCS] isolation

k) ARE [MFFCS] full load isolation

l) ARE [MFFCS] low load isolation

m) SG blowdown isolation

n) RCP trip

o) EDG start-up

The FC2 systems/functions involved in accident analyses (other than FC1 instances previously listed) are:

a) Emergency Boration System (RBS [EBS]) startup

b) LHSI in hot leg SI mode (switchover to hot leg injection)

c) LHSI in RHR mode

d) RCP [RCS] pump manual cut-off

e) MHSI manual cut-off

f) Accumulators manual isolation

g) VDA [ASDS] manual operation

h) MSIV bypass

i) SG blowdown between two SGs

In the analysis of DBC accidents, the safety systems that provide the safety functions are assumed to comply with the design given in Chapter 7.

Additional, in UK HPR1000, High Integrity Components (HIC) techniques are used to prevent gross failure of the pipes of RCP [RCS] and large break loss of coolant accident (LB-LOCA) is excluded from DBC list. However, the LB-LOCA event is still considered in system design, especially for safety injection system and containment.

In addition to the above FC1 and FC2 systems, non-FC1\FC2 systems may be considered in the DBC accident analyses according to the DBC analyses rules (either negative impact, or positive impact but not experiencing any discontinuity in their operation).

12.7 Analyses of DBC-2 Events

12.7.1 Increase in Heat Removal by the Secondary System

12.7.1.1 Increase in Feedwater Flow due to Feedwater System Malfunctions

12.7.1.1.1 Description

This event leads to an increase in heat removal from the secondary circuit. During power operation, this increase in heat removal leads to an increase in the core power due to the moderator feedback or by the RCP [RCS] average coolant temperature control. In the hot shutdown state, the heat removal increase leads to a return to power due to the moderator feedback. Therefore, feedwater system malfunction causing an increase in feedwater flow may lead to DNB. This fault may occur in State A or B.

Feedwater system malfunctions causing an increase in feedwater flow may be caused by:

a) ARE [MFFCS] failure;

b) Spurious actuation of ASG [EFWS];

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

d) Motor Driven Feedwater Pump System (APA [MFPS]) malfunction.

The coolant temperature and core power at full power level are higher than those conditions at other power levels in State A. Therefore, the full power case can cover any cases of other power levels. The coolant temperature in hot shutdown state is higher than other shutdown states in State A and State B, so the DNB risk is more onerous. The increase of feedwater flow may lead to a decrease of feedwater temperature, so the core may return criticality. Thus the cases at full power level and at hot shuntdown state are analysed.

12.7.1.1.2 Acceptance Criteria

The event is classified as a DBC-2 event. The acceptance criteria to be considered are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.1.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Full power operation

   1) Reactor trip is triggered on “SG level (narrow range) high 1” signal;

2) Turbine trip is actuated on receipt of reactor trip signal;

3) The ARE [MFFCS] full load isolation is actuated by “SG level (narrow range) high 1” or reactor trip signal;

4) The ARE [MFFCS] low load isolation is actuated by “SG level (narrow range) high 0” and reactor trip signal.

b) Hot shutdown state

1) The ARE [MFFCS] full load isolation is actuated by “SG level (narrow range) high 1” or reactor trip signal;

2) The ARE [MFFCS] low load isolation is actuated by “SG level (narrow range) high 0” and reactor trip signal;

3) The main steam isolation valves are closed by “pressure drop of SG high 1” signal;

4) The RIS [SIS] is actuated on “Pressuriser pressure low 3” signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.1.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

During power operation, an increase in feedwater flow causes a reduction of the primary average coolant temperature and pressure. Due to the effects of negative moderator feedback, the core power increases. This event can lead to reactor trip triggered by “SG level (narrow range) high 1” signal. The ARE [MFFCS] full load isolation is actuated by “SG level (narrow range) high 1” or reactor trip signal. If the SG level remains above the threshold of “SG level (narrow range) high 0” after a period of time delay, the low load main feedwater lines are isolated.

In hot shutdown state, an increase in feedwater flow causes a reduction of the primary average coolant temperature and pressure. Due to the effects of negative moderator feedback, core cooling leads to a decrease of the core shutdown margin, and then the

core may return to criticality. The ARE [MFFCS] full load isolation is actuated by "SG level (narrow range) high 1" or reactor trip signal. The main feedwater low load control and isolation valves are closed on reactor trip signal and "SG level (narrow range) high 0" signal. The MSIVs are closed by "pressure drop of SG high 1" signal, which reduces the main steam flowrate to zero.

Later on, the controlled state is reached. Under this state, the residual heat is removed via the VDA [ASDS] of all SGs. And the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.1.1.5 Analysis Assumptions

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

a) The initial event is considered to occur under full power condition and in hot shutdown condition respectively.

b) A conservative increase in main feedwater flowrate and a conservative decrease in feedwater temperature are considered. Symmetrical and asymmetrical feedwater flow increase is respectively taken into account.

c) The Doppler power coefficient is considered to be at its minimum absolute value, the moderator density coefficient is considered to be at its maximum absolute value.

d) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

e) In power operation condition, reactor trip is the only protection action before

minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one "SG level (narrow range) high 1" channel. In hot shutdown condition, the single failure is applied on one train of MHSI, so as to reduce the injection of boron and increase the core power.

f) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreases greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. So LOOP is not considered in this fault analysis in power operation condition. In the hot shutdown condition, the turbine is out of operation. Thus, LOOP is not considered.

12.7.1.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

In power operation conditions, the detailed analysis of this fault (see Reference [16]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

In hot shutdown state, the reactor returns to criticality. However, the peak nuclear power is low. Thus there is no DNB or fuel melting risk.

b) The acceptance criteria for this event are met. From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and Coolant Storage and Treatment System (TEP [CSTS])" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the “Turbine Trip” fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.7.1.2 Excessive Increase in Secondary Steam Flow

12.7.1.2.1 Description

This event is defined as a rapid increase in steam flow that causes a power mismatch between reactor power and steam flow demand. An excessive increase in steam flow may thus lead to an inadequate cooling of the fuel cladding by DNB. This fault may occur in State A or B.

An excessive increase in secondary steam flow may be caused by:

a) Spurious opening of the turbine inlet valve;

b) Spurious opening of one GCT [TBS] control valve.

c) Spurious actuation of Secondary Passive Heat Removal System (ASP [SPHRS]).

For shutdown conditions in State A and State B, the consequence of GCT [TBS] failure and spurious actuation of ASP [SPHRS] can be bounded by that of Steam Line Break (SLB). Thus the bounding case for this fault is at power operation.

12.7.1.2.2 Acceptance Criteria

The excessive increase in secondary steam flow is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.1.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is actuated on “Pressure drop of SG high 0” signal；

b) Turbine trip and isolation of the full load main feedwater lines on all SGs are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by “SG pressure high 1” signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.1.2.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

An excessive increase in secondary steam flow induces an overcooling of the primary circuit. This overcooling leads to a core power increase due to moderator feedback or the RCP [RCS] average coolant temperature control. In this event, the reactor can be protected by the “Pressure drop of SG high 0” protection signal.

After reactor trip, turbine trip and the ARE [MFFCS] full load isolation are initiated. The plant stabilises in the hot shutdown state.

If the increase in steam flow is limited, the event may not result in a reactor trip, and the reactor stabilises at a higher power level. The alarm for high core thermal power can alert the operator to the occurrence of such an accident. Once the source of the alarm is identified, the operator attempts to stop the excessive increase in steam flow, and the reactor returns to normal power operation. Otherwise the operator needs to transfer the reactor to the controlled state.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.1.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [17]. The main assumptions are as follows:

a) The initial power is assumed to be each 10% FP step from 10%FP to 100%FP;

b) The initiating event is that the secondary steam flow extracted from the SGs

increases to 110% of nominal value at power operation. This conservative step increase in steam flow envelops the following cases: spurious opening of one GCT [TBS], spurious opening of the turbine inlet valve and spurious actuation of ASP [SPHRS].

c) Plant behaviour is analysed using four cases:

1) BOC, manual reactor control;

2) EOC, manual reactor control;

3) BOC, automatic reactor control;

4) EOC, automatic reactor control.

d) The Doppler power coefficient is considered as its minimum absolute value so as to maximise the increase of core power. The moderator density coefficient is considered as its minimum absolute value at BOC and the maximum absolute value at EOC.

e) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “Pressure drop of SG high 0” channel.

f) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreased greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.1.2.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [17]) shows that the minimum DNBR is { } which is greater than the design limit { }. The nuclear power increases by a small amount from the initial moment, and a limited increase in the fuel temperature is induced. However, the fuel melting temperature limit is not challenged. Additionally, “no PCI-SCC” and “no PCMI” is demonstrated, Reference [9].

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the “Decrease in Boron

Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and Coolant Storage and Treatment System (TEP [CSTS])" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.1.3 Inadvertent Opening of One SG Relief Train or of One Safety Valve

12.7.1.3.1 Initiating Event

The inadvertent opening of one SG relief train, which is also called atmospheric steam dump train (VDA [ASDS]), or of one safety valve can be caused by the spurious opening of a VDA [ASDS] isolation valve, or spurious opening of a main steam safety valve (MSSV). This accident leads to an increase in the heat removal from the RCP [RCS] to the secondary side due to the increase of steam flow, which causes an overcooling effect on the core. The core power increases due to the negative moderator temperature coefficient. This could lead to the occurrence of departure from nucleate boiling (DNB) and subsequently to fuel damage.

The inadvertent opening of one atmospheric steam dump train (VDA [ASDS]) or of one safety valve is considered in state A and state B. The consequences of this fault in State B can be enveloped by analysis in State A since the initial sub-criticality margin and the initial boron concentration are higher in state B, which weakens the moderator effect. Therefore, the analysis for this fault is performed only in State A.

12.7.1.3.2 Acceptance Criteria

The inadvertent opening of one SG relief train or one safety valve in state A and state B is classified as a DBC-2 event. The acceptance criteria of no DNB and no fuel melting are applied for this fault:

a) The minimum DNBR shall be greater than { }

b) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.In terms of integrity of RCP [RCS], the analyses are performed in dedicated overpressure analysis synthesis report

12.7.1.3.3 Main Safety Functions

In order to reach the controlled sate, the following FC1 safety functions are required:

a) Reactor trip can be actuated on receipt of any of the following signals:

   1) High neutron flux (power range, high setpoint);

   2) Pressure Drop of SG high 0.

b) Affected VDA [ASDS] can be isolated by “SG pressure low 3” signal.

c) The safety injection system can be actuated by the “Pressuriser pressure low 3” signal.

d) Any of the following signals can lead to the quick closure of the MSIV to protect the RCP [RCS] against overcooling:

1) SG pressure low 1;

2) Pressure drop of SG high 1.

e) Any of the following signals can lead to ARE [MFFCS] isolation to protect the RCP [RCS] against overcooling:

1) ARE [MFFCS] full load lines isolated on the “RT” signal;

2) ARE [MFFCS] low load lines isolated on the “SG pressure low 2” signal;

3) ARE [MFFCS] low load lines isolated on the “Pressure drop of SG high 2” signal.

In order to reach the safe state, the following FC2 safety functions are required:

a) Affected VDA[ASDS] isolation

The affected VDA[ASDS] is isolated manually to prevent the core overcooling and to limit the mass and energy release.

b) Startup/Isolation of ASG [EFWS]

If the ASG [EFWS] for the unaffected SGs are not actuated automatically, the operator will start the ASG [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASG [EFWS].

c) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

d) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

e) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray, or by opening the PSV when the PZR normal spray is unavailable.

f) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

g) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.7.1.3.4 Typical Events Sequences

a) From initiating event to controlled state

1) The initial event occurs at full power

The inadvertent opening of an atmospheric steam dump train (VDA [ASDS]) or a safety valve at full power leads to a sudden increase of steam flow, and then the steam flow will reduce due to the decrease of steam pressure.

The increase in the capacity of heat removal from the RCP [RCS] to the secondary side during the accident causes coolant temperature and pressure to decrease. Due to the negative moderator temperature coefficient, a decrease of RCP [RCS] temperature can induce positive reactivity insertion, resulting in a core power increase.

The reactor trip might be actuated by “SG pressure low 1” signal or “Pressure drop of SG high 1” signal. ARE [MFFCS] full load lines are isolated and turbine trip is actuated both on the “RT” signal. Then, the sequence of events is similar with that in shutdown condition. In the case of inadvertent VDA [ASDS] opening, the affected VDA [ASDS] can be isolated by “SG pressure low 3” signal.

If the discharge size is not large enough, this accident might not cause a reactor trip, and the core power will remain at a higher level. The operator can identify this event via the “high core power” alarm signal. Once confirming the alarm, the operator will take actions to bring the reactor to controlled state (i.e. hot showdown state).

2) The initial event occurs at zero power

At zero power, the inadvertent opening of one VDA [ASDS] or one safety valve leads to a depressurisation in the secondary side. The “SG pressure low 1” signal or “Pressure drop of SG high 1” signal might be triggered and all the MSIVs are automatically isolated. After that, only the affected SG continues to depressurise. In the case of inadvertent VDA [ASDS] opening, the affected VDA [ASDS] can be isolated by “SG pressure low 3” signal.
The fault can result in an overcooling in the primary side, which induces positive reactivity in the core due to the negative moderator temperature coefficient, and the reactor might return to criticality. However, the Doppler Effect might limit the power excursion.
ARE [MFFCS] low load lines would be isolated on the “SG pressure low 2” signal or the “Pressure drop of SG high 2” signal. The “Pressuriser pressure low 3” signal would actuate the safety injection (RIS [SIS]). The plant can be taken to the controlled state.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.1.3.5 Results and Conclusions

a) From initiating event to controlled state

The break spectrum ranging from DN50 (corresponding to nominal diameter 50 mm) to double ended guillotine break of “Steam System Piping Large Break” is analysed in section 12.9.1.1, which results show that no DNB occurs and the fuel cladding and fuel pellet temperatures are not challenged, the acceptance criteria are met. Since the discharge size of VDA or MSSV is within this range, the acceptance criteria for inadvertent opening of one VDA [ASDS] or one safety valve can be met. Additionally, “no PCI-SCC” and “no PCMI” is demonstrated, Reference [9].

b) From controlled state to safe state

This transient to reach safe state is bounded by other faults from the following aspects:

1) In terms of sub-criticality, it is bounded by “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]” fault. From controlled state to safe state, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown, the sub-criticality margin of the bounding case is lowest due to the boron dilution, and more boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG” fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case, whereas at least two ASG [EFWS] trains are available in this fault.

c) Radiological Consequence

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.7.2 Decrease in Heat Removal from the Primary Circuit

12.7.2.1 Turbine Trip

12.7.2.1.1 Description

For a turbine trip event, the reactor could be tripped directly if power > 10%FP and some conditions regarding condenser unavailability are satisfied. The turbine stop valves close rapidly on loss of trip-fluid pressure actuated by one of a number of trip signals. The steam flow to the turbine decreases abruptly following the stop valve closure. Sensors on the stop valves detect the turbine trip and steam dump is initiated. The loss of steam flow results in a rapid rise in the secondary circuit temperature and pressure. Consequently, the pressure also increases in the primary circuit. Because of the rapid reduction in steam flow, the capacity of the secondary system to remove the core heat decreases, further potentially causing DNB and insufficient cooling of the fuel cladding. This fault may occur in State A and B.

The turbine trip may be caused by:

a) Spurious turbine trip;

b) Failure of Condensate Extraction System (CEX [CES]);

c) Failure of Circulating Water System (CRF [CWS]).

The failures on CRF [CWS] may affect the normal operation of CEX [CES] (may result in loss of vacuum in condenser) and can lead to turbine trip or loss of secondary steam load when the turbine is out of operation. The primary temperature and pressure increase in the primary circuit and may lead to DNB. The core power and the coolant temperature at full power in State A is higher than that in State B. Thus the bounding case for analysis is turbine trip at full power level.

If turbine trip results in the LOOP, the RCP [RCS] pumps coast down and the main feedwater pumps are tripped after LOOP. The capacity of the primary coolant to remove the core heat decreases. The case of LOOP after turbine trip needs to be analysed.

Therefore, the case with LOOP and the case without LOOP are analysed in the fault analysis.

12.7.2.1.2 Acceptance Criteria

The turbine trip accident is considered as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.2.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “Pressuriser pressure high 2” signal.

b) If turbine trip results in the LOOP, reactor trip is triggered on “Low RCP [RCS] pump speed” signal.

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

d) The VDA [ASDS] is actuated by the “SG pressure high 1” signal.

e) The PSVs are opened when the PZR pressure reaches the setpoint.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.2.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

After turbine trip, the loss of steam flow results in a rapid rise in secondary circuit temperature and pressure. Consequently, the temperature and pressure also increases in the primary circuit. The reactor trip is automatically triggered on “Pressuriser pressure high 2” signal.

If turbine trip results in LOOP, it leads to the decrease of the heat removal capacity of the fuel cladding. After the loss of power supply, the RCP [RCS] pump begin to coast down. The coast down of the reactor coolant pump speed takes several seconds due to the inertia of the flywheel. Furthermore, the main feedwater pumps are tripped after the LOOP. When the speed of the reactor coolant pump reaches the “Low RCP [RCS] pump speed” setpoint, reactor trip is actuated so as to protect the core. During the whole transient, the important instrumentation and control equipment and safety valves are supplied by uninterruptible power supply system uninterruptedly. The EDGs are initiated by the low-voltage signal of the emergency busbar.

After reactor trip, the RCCAs drop into the core and the core power decreases dramatically.

Since the secondary circuit pressure rises continuously after reactor trip, the VDA [ASDS] is automatically opened (triggered by "High steam generator pressure 1" signal), and the steam is discharged into the atmosphere. The GCT [TBS] is unavailable because of the loss of condensate pumps. During this period, the VDA [ASDS] may be unable to remove all the residual heat of the core. The PSVs may open to limit the increase in primary pressure, since the normal spray is unavailable. Then, the ASG [EFWS] is actuated by the "SG level (wide range) low 2" signal.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all SGs and the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.2.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [18]. The main assumptions are as follows:

a) The initiating event is that turbine is tripped at time zero under full power condition and it is assumed that the main feedwater flowrate is completely lost after the turbine trip.

b) Plant behaviour is analysed using the following cases:

1) Turbine trip without LOOP;

2) Turbine trip with LOOP.

c) The moderator density coefficient is considered as its minimum absolute value to limit the core power decrease by moderator effect due to the coolant temperature increase, and thus to worsen the consequences of the event regarding DNBR.

d) The Doppler power coefficient is considered as its maximum absolute value to

maximise the core power, and thus to worsen the consequences of the event regarding DNBR.

e) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

f) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one "Pressuriser pressure high 2" channel (without LOOP) or one "Low RCP [RCS] pump speed" channel (with LOOP).

12.7.2.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [18]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The quantitative analysis on radioactive substance confinement from the controlled state to the safe state is given in the Reference [19]. For sub-criticality and radioactive substance confinement, it is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and Coolant Storage and Treatment System (TEP [CSTS])" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.7.2.2 Short Term LOOP of 2 Hours Duration

12.7.2.2.1 Description

A loss of offsite power leads to the loss of power supply to all RCP [RCS] pumps, main feedwater pumps and condensate pumps. Because of the decrease of reactor coolant flow and the decrease of the heat removal capacity by the secondary circuit, the capacity of the primary coolant to remove the core heat decreases, potentially resulting in DNB and insufficient cooling of the fuel cladding.

The loss of offsite power may be caused by:

a) A complete loss of offsite grid;

b) An onsite power distribution system failure;

c) An external grid disturbance (dropped voltage or frequency).

Since the core power and coolant temperature at full power in State A is higher than that in State B\C\D\E\F, the consequence of loss of off-site power at full power in State A is the most severe. Thus the bounding case for analysis is a loss of off-site power at full power level.

12.7.2.2.2 Acceptance Criteria

The short term LOOP of 2 hours duration accident is considered as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.2.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “Low RCP [RCS] pump speed” signal;

b) Turbine trip is actuated on receipt of reactor trip signal;

c) EDG are actuated by “LOOP” signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) The VDA [ASDS] is actuated by “SG pressure high 1” signal.

f) The residual heat in RCP [RCS] is removed by the RIS [SIS] system in RHR mode

g) Automatic actuation of EDG supply electricity to RIS [SIS] pumps, thus ensuring the recovery of RIS [SIS] in RHR mode.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.2.2.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

After the loss of power supply in State A, the RCP [RCS] pumps begin to coast down. The coast down of the reactor coolant pump speed takes several seconds due to the inertia of the flywheel. Furthermore, the condensate pump and the main feedwater pumps are tripped after the loss of offsite power. The capacity of the primary coolant to remove the core heat decreases.

When the speed of reactor coolant pump reaches the “Low RCP [RCS] Pumps Speed” setpoint, the reactor trip is actuated so as to protect the core. After the reactor trip, the RCCAs drop into the core and the core power decreases dramatically.

During the whole transient process, the important instrumentation and control equipment and safety valves are supplied by un uninterruptible power supply system.

Since the secondary circuit pressure rises continuously after the reactor trip, the VDA [ASDS] is automatically opened (triggered by “SG pressure high 1” signal), and the steam is discharged into the atmosphere. The GCT [TBS] is unavailable because of the loss of condensate pumps. During this period, the VDA [ASDS] may be unable to remove all the residual heat from the core. The PSVs may open to limit the increase in primary pressure, since the normal spray is unavailable. Then, the ASG [EFWS] supplied by EDG is actuated by the “SG level (wide range) low 2” signal.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all SGs and the feedwater is supplied by the ASG [EFWS].

After the loss of off-site power supply in the State C, D, E and F, RIS [SIS] pumps coast down and the capacity of the primary coolant to remove the core residual heat decreases. After a period of time, EDGs are actuated by the “LOOP” signal and the power of RIS [SIS] pumps is restored. The RHR function continues to remove the residual heat. The controlled state is reached.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the PSVs.

12.7.2.2.5 Analysis Assumptions

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

a) The initial event is considered under full power condition.

b) The non-emergency power is lost at initial time, and then the RCP [RCS] pumps begin to coast down.

c) The Doppler power coefficient is considered as its maximum absolute value, the moderator density coefficient is considered as its minimum absolute value.

d) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

e) The single failure is applied on one EDG.

12.7.2.2.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [20]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.2.3 Loss of Normal Feedwater Flow

12.7.2.3.1 Description

Loss of normal feedwater flow is an overheating event, leading to the reduction in capability of the secondary circuit to remove the heat generated in the primary circuit, and inadequate cooling of fuel cladding due to DNB. This fault may occur in State A and B.

The loss of normal feedwater flow may be caused by:

a) Feedwater lines isolation or control valves malfunction;

b) Failures of main feedwater pumps, valves, or other signals;

c) Spurious shutdown of the APA [MFPS] pumps and the AAD [SSFS] pumps;

d) Break in High Pressure Feedwater Heater System (AHP [HPFHS]), Feedwater Deaerating Tank and Gas Stripper System (ADG [FDTGSS]), Low Pressure Feedwater Heater System (ABP [LPFHS]) or CEX [CES].

Compared to a break in AHP [HPFHS], ADG [FDTGSS], ABP [LPFHS] and CEX [CES], total loss of secondary feedwater due to feedwater lines isolation or control valves malfunction is more onerous because it leads to more significant heat removal from secondary side. Besides, the average coolant temperature at full power is higher than that at any other power levels. Thus the bounding case for analysis is loss of normal feedwater flow at full power level.

12.7.2.3.2 Acceptance Criteria

The loss of normal feedwater flow event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.2.3.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “SG level (narrow range) low 1” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

d) The VDA [ASDS] is actuated by the “SG pressure high 1” signal;

e) The PSVs are opened when the PZR pressure reaches the setpoint.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

12.7.2.3.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

After the loss of normal feedwater flow, the water inventory of SGs decreases while the core power remains unchanged, leading to an increase in the primary temperature and pressure.

Afterwards, the “SG level (narrow range) low 1” signal triggers reactor trip automatically, leading to turbine trip. The secondary pressure is limited by the GCT [TBS] if it is available. Otherwise, it is limited by the VDA [ASDS]. The SG levels continuously decrease until the “SG level (wide range) low 2” signal occurs, and the ASG [EFWS] starts to remove the core residual heat.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all SGs and the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.2.3.5 Analysis Assumptions

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

a) The initial event is considered under full power condition.

b) The main feedwater flowrate is completely lost at time zero.

c) The Doppler power coefficient is considered as its maximum absolute value so as to minimise the decrease of core power; the moderator density coefficient is considered as its minimum absolute value so as to maximise the core power.

d) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

e) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “SG level (narrow range) low 1” channel.

f) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreases greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.2.3.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [21]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The quantitative analysis on heat removal from the controlled state to the safe state is given in the Reference [22]. For sub-criticality and radioactive substance confinement, it is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

In terms of sub-criticality, it is bounded by the “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP

[CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.2.4 Spurious reactor trip

Spurious reactor trip can be initiated by either a manual shutdown due to the spurious actuation of an automatic reactor trip signal or an operator error. This is covered by other DBC-2 events resulting in reactor trip, in Sub-chapter 12.7.2.

12.7.2.5 Loss of One RIS [SIS] Train in RHR Mode

12.7.2.5.1 Description

In this event, one RIS [SIS] train in RHR mode is lost, and the primary average coolant temperature increase leads to a reduction of the capability of the heat removal. This fault may occur in State C, D and E.

The loss of one RIS [SIS] train in RHR mode may be caused by:

a) Failures in RIS [SIS];

b) Failures in Component Cooling Water System (RRI [CCWS]).

In State C1 and C2, the PZR level is at setpoint or full, and the primary pressure is higher than atmospheric pressure; the decay heat is higher in State C1 than State C2. Therefore, loss of one RIS [SIS] train in RHR mode in State C2 can be bounded by the event in State C1.

In State C3 and D, the RCP [RCS] level and the primary pressure are lower than that in State E, in which the reactor cavity is flooded and the primary pressure is at atmospheric pressure. A low RCP [RCS] level is disadvantageous to residual heat removal. And if the RCP [RCS] temperature attains saturation temperature, the RCP [RCS] water evaporates and RCP [RCS] level decreases, which leads to core uncovery probably.

Thus, the bounding case for analysis is loss of one RIS [SIS] train in RHR mode in State C1, C3 and D.

12.7.2.5.2 Acceptance Criteria

The loss of one RIS [SIS] train in RHR mode is classified as a DBC-2 event. The acceptance criteria to be considered for this event are:

a) Core water inventory is stable and no core uncovery occurs;

b) Heat removal is ensured on a long term basis.

12.7.2.5.3 Main Safety Functions

In this event, the following main safety functions (FC2) are required:

a) SI is actuated on “RCP [RCS] loop level low 1” signal;

b) The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.7.2.5.4 Typical Events Sequences

During normal condition, the cooling of the plant is performed by the RIS [SIS] in RHR mode. When the RCP [RCS] temperature is between 100℃ and 140℃ (State

C1), the RIS [SIS] train A and train B are used in RHR mode. When the RCP [RCS] temperature is lower than 100℃ (State C2), the RIS [SIS] train C is used additionally in RHR mode. Below 60℃, two RIS [SIS] trains in RHR mode are sufficient to maintain the current RCP [RCS] temperature, and the third train is in standby in SI mode. When the RCP [RCS] temperature is below 60℃, the RCP [RCS] loop level can be lowered to ¾ loop, which corresponds to State C3 (RCP [RCS] partially open, rapidly re-closable) or D (RCP [RCS] open). When the reactor cavity is flooded, the reactor operates on Refuelling Cold Shutdown mode (State E).

In this event, the RCP [RCS] temperature increases. If the RCP [RCS] temperature does not attain the saturation temperature, the reactor finally attains equilibrium. If the RCP [RCS] temperature attains saturation temperature, the RCP level drops following the vaporization of coolant primary, and the MHSI is actuated by the "RCP [RCS] loop level low 1" signal.

In the long term, heat removal is ensured by the unaffected RIS [SIS] train, the reactor reaches the safe state.

12.7.2.5.5 Analysis Assumptions

The detailed assumptions are presented in Reference [23]. In State C1, the sensibility analysis shows that there is a large margin of RCP [RCS] temperature from saturation temperature during the event. In State C3 and D, the main assumptions are listed as follows:

a) The plant operates in RCP [RCS] ¾ loop level condition;

b) The failure of one RIS [SIS] train in RHR mode is assumed;

c) The maximum decay heat is considered during the event, so as to increase the core power;

d) The actuation of MHSI pump is the only protection action before core uncovery, so the single failure is applied on one MHSI pump.

12.7.2.5.6 Results and Conclusions

The detailed analysis of this fault (see reference [23]) shows that one remaining RIS [SIS] train in RHR mode is able to remove the total RCP [RCS] primary power.

In State C3 and D, at shutdown condition, the analysis result shows that the RCP [RCS] temperature increases during the event and finally attains its maximum temperature { }, which is lower than the saturation temperature at { }. The core water inventory is stable and no core uncovery occurs.

In State C3 and D, at start-up condition, the RCP [RCS] temperature attains saturation temperature { }. The RCP [RCS] water is evaporated and RCP [RCS] loop level decrease. The SI is triggered by "RCP [RCS] loop level low 1" signal. After the injection of MHSI, the heat removal is ensured by the unaffected RIS [SIS] train.

In this accident, there is no radioactivity release to the environment and the RPT-4 BSO is met.

12.7.3 Decrease in Core Coolant System Flow

12.7.3.1 Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump

12.7.3.1.1 Description

Partial loss of core coolant flow due to loss of one reactor coolant pump leads to an increase in the primary coolant temperature. The decrease of core coolant flow causes a reduction of the capacity of the primary coolant to remove heat from the core. This can lead to an inadequate cooling of the fuel cladding through DNB. This fault may occur in State A, B and C.

The partial loss of core coolant flow due to loss of one reactor coolant pump can be caused by:

a) Mechanical or electrical failure in a reactor coolant pump;

b) Failure of the busbar supplying a reactor coolant pump.

Since the core power and coolant temperature at full power level in State A are higher than those in State B\C, the consequences of this fault in State B\C can be bounded by those at full power level in State A. Thus the bounding case for analysis is the loss of core coolant flow in one primary loop at full power level.

12.7.3.1.2 Acceptance Criteria

The partial loss of core coolant flow due to loss of one reactor coolant pump event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.3.1.3 Main Safety Functions

a) In order to reach the controlled state, the following main safety functions (FC1) are required: reactor trip is triggered on “Low flow rate in one primary loop” and P8 (nuclear power >30%FP) signals;

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by “SG pressure high 1” signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.3.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

At the start of the event, one reactor coolant pump is assumed to fail. The total core flow rate decreases gradually over time. reactor trip is caused by “Low flow rate in one primary loop” signal. After reactor trip, the RCCAs drop into the core and the core power decreases dramatically. Turbine trip and the ARE [MFFCS] full load isolation are initiated by the reactor trip signal. The secondary circuit pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all steam generators.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.3.1.5 Analysis Assumptions

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

a) The initiating event is the loss of the one pump at full power condition.

b) The Doppler power coefficient is considered as its maximum absolute value so as to minimise the decrease of core power; the moderator density coefficient is considered as its minimum absolute value so as to minimise the decrease of

nuclear power.

c) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

d) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one "Low flow rate in one primary loop" channel.

e) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreased greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.3.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [24]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the “Turbine Trip” fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.4 Reactivity & Power Distribution Anomalies

12.7.4.1 Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition

12.7.4.1.1 Description

Uncontrolled RCCA bank withdrawal event is defined as an uncontrolled addition of reactivity to the reactor core resulting in a power excursion. This fault may occur in State A, B and C.

Uncontrolled RCCA bank withdrawal at a subcritical or low power startup condition may be caused by:

a) Withdrawal of sub-bank of R\G\N bank;

b) Withdrawal of R\G\N bank.

The analysis on uncontrolled RCCA bank withdrawal at power in State A is given in Sub-chapter 12.7.4.2. At hot standby and hot shutdown in State A, the reactor can be protected by “high neutron flux (power range, low setpoint)” signal as well as “high neutron flux (intermediate range)” signal. When the initial nuclear power gets higher, the reactor trip costs less time and the peak nuclear power in the transient is lower. For the other shutdown conditions in State A\B\C, the reactor is protected by reactor trip signal of high neutron flux (source range). The setpoint of this signal is much lower than that of “high neutron flux (power range, low setpoint)” signal and that of “high neutron flux (intermediate range)” signal. The nuclear power will not increase significantly. Therefore, the enveloped case for the analysis is the withdrawal of two RCCA banks at hot shutdown in State A.

12.7.4.1.2 Acceptance Criteria

The “Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition” event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.4.1.3 Main Safety Functions

In order to reach the controlled state, the main safety function (FC1) required is that the reactor trip is triggered on “high neutron flux (power range, low setpoint)” signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.4.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

At the beginning of the transient, the two banks with the highest worth are fully inserted and assumed to be withdrawn simultaneously at the maximum speed. The core reactivity increases uncontrollably, causing an abnormal power distribution.

With the continuous reactivity insertion, the neutron flux rises rapidly until it is stopped by the Doppler negative feedback. This self-limitation of the power excursion is of primary importance because it limits the power during the delay time for protection actions. The reactor trip is triggered by “high neutron flux (power range, low setpoint)” signal.

After reactor trip, the RCCAs drop into the core and the core power decreases dramatically. The secondary circuit pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all steam generators.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.4.1.5 Analysis Assumptions

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

a) The two banks with the highest worth are fully inserted and assumed to be withdrawn at the maximum speed (72 steps/minute). Under the assumed condition, the uncontrolled withdrawal of RCCA banks induces a very conservative reactivity insertion rate.

b) The delayed neutron fraction and the prompt neutron lifetime used in the analysis are set to the maximum envelope values, i.e. 750pcm and 31μs respectively, to ensure the maximum energy stored in the fuel pellet.

c) The Doppler power coefficient is considered as its minimum enveloped absolute value of each cycle to maximize the peak nuclear power.

d) The axial power distribution greatly tilting towards the core bottom is selected, maximizing the differential worth of the withdrawn RCCAs as well as the axial peak power factor.

e) The cladding-pellet gap heat transfer coefficients are assumed to be the minimum value to maximize the fuel pellet temperature.

f) The most pessimistic position of the withdrawal banks between the full insertion and total withdrawal is used in the $F_{\Delta H}$ calculation. The $F_{\Delta H}$ is assumed to remain unchanged and to equal the maximum value during the RCCA bank withdrawal.

g) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “high neutron flux (power range, low setpoint)” channel.

h) LOOP is considered as a consequence of turbine trip. However, the turbine is out of operation at hot shutdown. Thus, LOOP is not considered in this fault analysis.

12.7.4.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [25]) shows that the minimum DNBR is 1.87. However, the quality of the minimum DNBR state point is -0.22, which is a little lower than -0.15, the low limit of W3 correlation validity domain. In order to increase the quality of the minimum DNBR state point, the inlet core temperature is raised from 298.8℃ to 306℃ as a conservative assumption for DNBR calculation. The minimum DNBR is 1.52 which is greater than the design limit 1.36

(W3 correlation, deterministic method). The maximum fuel temperature is 1412℃ which is lower than the fuel melting temperature { }℃.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.4.2 Uncontrolled RCCA Bank Withdrawal at Power

12.7.4.2.1 Description

This event is defined as a continuous uncontrolled RCCA bank withdrawal at power. The insertion of positive reactivity results in an increase in the core power; before the secondary circuit pressure reaches the setpoint of the relief valve or safety valve, the heat removed from the SGs lags behind the increase in core power. Therefore, there is a significant increase in the reactor coolant temperature and pressure. If the event is not controlled manually or automatically, the DNB may be initiated by the power mismatch between the primary and secondary circuits as well as the resulting increase in primary average coolant temperature. This fault may occur in State A.

Uncontrolled RCCA bank withdrawal at power may be caused by:

a) The withdrawal of the sub-bank of R\G\N bank;

b) The withdrawal of the R\N\G bank.

In State A, except for when the reactor is in power condition, the event is bounded by "Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition" fault.

At reactor in power condition, the initiating events are positive reactivity insertion caused by uncontrolled RCCA bank withdrawal. The maximum positive reactivity insertion rate analysed is greater than that for the simultaneous withdrawal at maximum speed (72 steps/min) of the two control banks having the maximum combined worth and the maximum overlap. Thus, the bounding case for analysis is the uncontrolled RCCA bank withdrawal at different power level.

12.7.4.2.2 Acceptance Criteria

The event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.4.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on "Overtemperature ΔT" signal or "High neutron flux (power range, high setpoint)" signal;

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by "SG pressure high 1" signal;

d) PSVs open when PZR pressure attains opening threshold.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

12.7.4.2.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

The induced reactivity insertion results in an increase in the core heat flux. The heat extraction from the SGs lags behind the core power generation. The pressure and temperature of the primary and secondary circuit increase until reactor trip. Before reactor trip, the PSVs may open to limit the RCP [RCS] pressure and the VDA [ASDS] may be opened to limit the secondary circuit pressure.

For high reactivity insertion rates, reactor trip is initiated by the “High neutron flux (power range, high setpoint)” signal. The neutron flux in the core rises rapidly for these insertion rates while core heat flux and primary coolant temperature lag behind due to the thermal capacity of the primary circuit. Thus, the reactor is tripped prior to significant increase in heat flux with resultant high minimum DNBR during the transient. As reactivity insertion rate decreases, core heat flux and coolant temperature can remain in closer equilibrium with the neutron flux; minimum DNBR during the transient thus decreases with decreasing insertion rate.

With further decrease in reactivity insertion rate, the “Overtemperature ΔT” and “High neutron flux (power range, high setpoint)” trips become equally effective in terminating the transient. For further reduction in reactivity insertion rates, the effectiveness of the “Overtemperature ΔT” trip increases (in terms of increased minimum DNBR) due to the fact that with lower insertion rates the power increase rate is slower than the rate of rise of average coolant temperature.

After reactor trip, the RCCA banks drop into the core and the core power decreases dramatically. Turbine trip and the ARE [MFFCS] full load isolation are initiated by the reactor trip signal. The secondary circuit pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable.

Finally, the controlled state is reached. The residual heat is removed by the VDA

[ASDS] of all steam generators.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.4.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [26]. The main assumptions are listed as follows:

a) The initial power is assumed to be each 10% step from 10%FP to 100%FP inclusive.

b) The reactivity insertion rates (0.1 pcm/s ~ 100 pcm/s) assumed in the analysis bound all possible conditions. The maximum positive reactivity insertion rate analysed is greater than that for the simultaneous withdrawal at maximum speed of the two control banks having the maximum combined worth and the maximum overlap.

c) Two sets of reactivity coefficients are considered for each reactivity insertion rate:

1) Minimum reactivity feedback: The Doppler power coefficient is considered as its minimum absolute value; the moderator density coefficient is considered as its minimum absolute value.

2) Maximum reactivity feedback: The Doppler power coefficient is considered as its maximum absolute value, the moderator density coefficient is considered as its maximum absolute value.

d) Pressuriser spray and PSVs which limit the RCP [RCS] pressure increase are available.

e) Reactor trip actuated by “Pressuriser pressure high 2”, “Pressuriser level high 1” and “Overpower ΔT” signals are not considered. These protection channels may

be triggered under low initial power level and small reactivity insertion rate.

f) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

g) The single failure is applied on one "High neutron flux (power range, high setpoint)" channel or one "Overtemperature ΔT" channel.

12.7.4.2.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [26]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before reactor trip, the nuclear power increases by a small amount, and a limited increase in the fuel temperature is caused. However, the fuel melting temperature limit is not challenged. Additionally, "no PCI-SCC" and "no PCMI" is demonstrated, Reference [9].

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents is not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.4.3 RCCA Misalignment up to Rod Drop

12.7.4.3.1 Description

One or more RCCAs in one sub-bank dropping into the core may cause a negative reactivity insertion, thus leading to a decrease in the primary average coolant temperature. If reactor trip is not triggered, the core power decrease and primary-secondary power mismatch result in a thermal-hydraulic transient governed by the reactivity feedback and by RCP [RCS] average coolant temperature control. The core power may return to the initial level and may exhibit an overshoot for a short period. The combination of the high power level and the distorted power distribution caused by the rod drop may lead to a DNB if the reactor core is not protected. This fault may occur in State A.

RCCA misalignment up to rod drop may be caused by:

a) One RCCA of R\G\N\S-bank drop;

b) One sub-bank of R\G\N\S-bank drop;

c) Insertion of one RCCA of R\G\N\S bank;

d) Insertion of the sub-bank of R\G\N\S bank.

In state of reactor in power, the core power and coolant temperature at full power level are higher than those at lower power level, so the mismatch will be aggravated at full power which penalises the DNB. Thus the bounding case for analysis is drop of one or more RCCAs at full power level.

12.7.4.3.2 Acceptance Criteria

The RCCA misalignment up to rod drop is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.4.3.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “high negative neutron flux rate” signal;

b) Turbine trip and isolation of the full load main feedwater line on all SG are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by “SG pressure high 1” signal.

In order to reach the safe state, the following manual safety functions (FC2) are

required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

12.7.4.3.4 Typical Events Sequences

a) From the Initiating Events to the Controlled State

At the beginning of the transient, the nuclear power drops rapidly. The RCP [RCS] pressures and the primary average coolant temperature decreases.

If the reactor trip is triggered on “high negative neutron flux rate” signal, turbine trip and ARE [MFFCS] full load isolation are initiated on the reactor trip signal. The secondary pressure is limited by VDA [ASDS] if GCT [TBS] is unavailable. The feedwater is supplied by the ARE [MFFCS].

For the transient without reactor trip, the nuclear power increases to a new primary-secondary equilibrium if the control banks are in automatic control mode. If the reactivity inserted by the temperature control banks is sufficient, the core power may return to the initial level and might exhibit an overshoot for a short period. If the rod control system is in the manual control mode, the core power might return monotonously to a new balance, and the primary coolant temperature remains lower than the initial value. The reactor can be tripped by the operator manually, and the reactor can be stabilised in the hot shutdown state after reactor trip.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all SGs.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via RBS [EBS] if RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS].

ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.4.3.5 Analysis Assumptions

The detailed assumptions are presented in Reference [27]. The main assumptions are listed as follows:

a) The initiating event is one or more RCCAs in one sub-bank begining to fall into the core in the full power condition;

b) For the Doppler power coefficients and the moderator density coefficients used in detection and transient analysis, the maximum absolute values are considered in detection phase and the minimum absolute values are considered in transient phase respectively;

c) LOOP is not considered in this event since the reactor is not tripped for the undetected rod drop cases;

d) Single failure is applied on one “high negative neutron flux rate” channel.

12.7.4.3.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [27]) shows that the minimum DNBR is { } which is greater than the design limit { }. The nuclear power increases slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met. Additionally, “no PCI-SCC” and “no PCMI” is demonstrated, Reference [9].

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]” fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.4.4 Startup of an Inactive Reactor Coolant Loop at an Improper Temperature

Spurious startup of a reactor coolant pump leads to an increase of primary flow rate. Meanwhile, the thermal power of the pump may cause an overpressure in the primary circuit, especially when the pressuriser is full. The core will not return criticality due to the reactivity insertion by RCP [RCS] pumps startup at low loop temperature. Therefore, this event would not have any consequence for safety.

12.7.4.5 Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]

12.7.4.5.1 Overview

This section describes the analysis for the uncontrolled boron dilution. The uncontrolled boron dilution may be caused by:

a) Operator error;

b) Failure in Reactor Boron and Water Makeup System (REA [RBWMS]) or Chemical and Volume Control System (RCV [CVCS]);

c) A water leak from the Component Cooling Water System (RRI [CCWS]) through a damaged condenser of Coolant Storage and Treatment System (TEP [CSTS]) to RCV [CVCS], and into the Reactor Coolant System (RCP [RCS]).

This fault is classified as a Design Basis Condition 2 (DBC-2) event and may occur in State A, B and C. The analysis is divided into three parts according to their different initial conditions:

Part 1: Uncontrolled boron dilution initiated in State A, as the reactor is at power operation condition in manual control mode;

Part 2: Uncontrolled boron dilution initiated in State A, as the reactor is at power operation condition in automatic control mode;

Part 3: Uncontrolled boron dilution initiated in State A, B and C, as the reactor is at shutdown condition.

12.7.4.5.2 Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS] (State A: power operation: manual control)

12.7.4.5.2.1 Description

Injection of water with no boron or lower boron concentration reduces the boron concentration of RCP [RCS] and causes a reactivity increase, which potentially results in DNB if it occurs during power operation.

For uncontrolled boron dilution at power operation condition in manual control mode, a reactivity insertion results in a slow increase of reactor power level and coolant average temperature.

12.7.4.5.2.2 Acceptance Criteria

The acceptance criteria to be considered for DBC-2 events are: Fuel integrity shall be ensured. For boron dilution at power operation condition in manual control mode the acceptance criteria are as follows:

a) After reactor trip, the operator has more than 30 minutes of grace period to perform dilution source isolation before the reactor returns to criticality;

b) At power operation, the Departure from Nucleate Boiling Ratio (DNBR) shall be greater than the design limit.

12.7.4.5.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on "Overtemperature ΔT" signal or "Overpower ΔT" signal. After reactor trip, the operator needs enough time to perform dilution source isolation before the reactor core returns to criticality.

b) Even if the operator fails to perform dilution source isolation in time, an automatic isolation can still be triggered by subsequent "High neutron flux (source range)" signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of Emergency Boration System (RBS [EBS])

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of Safety Injection System (RIS [SIS]) in Residual Heat Removal (RHR) mode

12.7.4.5.2.4 Typical Sequence of Events

For this event, the typical sequence of events includes the following two stages:

a) From Initiating Event to Controlled State

As positive reactivity being inserted, reactor power level and the average coolant temperature increase slowly. Following that, "Overtemperature ΔT" protection signal or "Overpower ΔT" protection signal is generated.

After reactor trip, the operator performs manual dilution source isolation (isolation of RCV [CVCS]) after 30 minutes and the controlled state is reached. Under this state, the residual heat is removed via the VDA [ASDS].

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to

the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurization according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurization via the normal or auxiliary pressurizer spray, and the PSV can be used when the pressurizer sprays are unavailable.

12.7.4.5.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [28]. The main assumptions are listed as follows:

a) Initial Conditions

The initial conditions assumed conservatively in reactivity control analysis for power operation condition in manual control mode (State A) are as follows:

1) G1, G2, N1, N2, R control rod banks are at limiting positions;

2) Critical core;

3) The unit is initially operated under Hot Zero Power (HZP);

4) The borated water inventory of RCP [RCS] (except for the pressurizer and the dead zone at the top of the reactor pressure vessel) is 178t;

5) The dilution flow rate is considered as maximum value of 87t/h;

6) For all fuel cycles analyzed, the maximum initial boron concentrations are considered in manual control mode. Uncertainty included in the initial boron concentration is 60 ppm (enriched boron concentration with boron-10 abundance of 35%).

b) Initial Event

Reactivity insertion rate is dependent on the boron concentration of reactor coolant and dilution flow rate. For power operation condition, the most conservative case for uncontrolled boron dilution is at the Beginning of Cycle (BOC) as the boron concentration is the highest. Therefore, only BOC case is analyzed.

c) Core-related Assumptions

1) All reactor coolant pumps keep functioning to ensure continuous mixing of

borated water in the reactor pressure vessel;

2) After reactor trip, the highest worth Rod Cluster Control Assembly (RCCA) is stuck out of the core;

3) The accumulation of xenon in the core is not considered in the calculation;

4) 10% of uncertainty is included in total worth of N-1 shutdown banks.

d) LOOP Assumption

The LOOP is considered as a consequence of turbine trip.

LOOP could lead to the loss of power supply to charging pumps (FC3) of RCV [CVCS]. Important instrumentations, control equipment and safety valves are supplied by UPS system. The protection and safety system are able to perform the safety functions since these systems can be supplied by EDG. Therefore, not considering LOOP in this fault analysis is conservative.

e) Single Failure

For uncontrolled boron dilution at power operation conditions in manual control mode, the reactor is protected by “Overtemperature ΔT” channel protection or “Overpower ΔT” channel protection with the logic of “2 out of 3”.

As an automatic isolation could be triggered by “High neutron flux (source range)” signal after the operator failed to isolate dilution source manually, the single failure is applied to “Overtemperature ΔT” signal (one sensor or channel) or “Overpower ΔT” signal (one sensor or channel).

f) Protection Signals

Reactor trip is triggered on “Overtemperature ΔT” signal or “Overpower ΔT” signal. The setpoint is assumed to be the rated value with uncertainties.

An automatic isolation could be triggered by “High neutron flux (source range)” signal if the operator failed to isolate dilution source manually.

g) Control Systems

The function of control systems is not considered in the analysis.

12.7.4.5.2.6 Results

For uncontrolled boron dilution of reactivity control case at power operation conditions in manual control mode, calculation results for all fuel cycles analyzed show that after reactor trip the operator has at least 60 minutes of grace period before the core reaches criticality.

If the operator failed to perform dilution source isolation in time, an automatic isolation and reactor trip could still be triggered by “High neutron flux (source range)”

signal, with a corresponding power level far below 0.1%FP.

For DNB analysis, the minimum DNBR is greater than the design limit of { }.

12.7.4.5.3 Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS] (State A: power operation: automatic control)

12.7.4.5.3.1 Description

This section is dedicated to the analysis for uncontrolled boron dilution at power operation condition in automatic control mode.

Injection of water or borated water with lower boron concentration reduces the boron concentration of RCP [RCS] and induces a reactivity insertion, which potentially results in DNB if it occurs during power operation.

For uncontrolled boron dilution at power operation condition in automatic control mode, the control system reacts in order to maintain the reactor in its initial state.

12.7.4.5.3.2 Acceptance Criteria

The acceptance criteria to be considered for DBC-2 events are: Fuel integrity shall be ensured. For boron dilution at power operation condition in automatic control mode the acceptance criteria are:

a) The maximum allowable delay time after the isolation signal shall be larger than the delay time used in the accident analysis;

b) At power operation, the DNBR shall be greater than the design limit.

12.7.4.5.3.3 Main Safety Functions

For power operation condition in automatic control mode, isolation of dilution source is triggered by “Bank R position low 3” signal (FC1) combining with the permissive signal P10 and controlled state is reached.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of Emergency Boration System (RBS [EBS])

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of Safety Injection System (RIS [SIS]) in Residual Heat Removal

(RHR) mode

12.7.4.5.3.4 Typical Sequence of Events

The typical sequence of events includes the following two stages:

a) From Initiating Event to Controlled State

In automatic control mode, bank R insertion gradually compensates for positive reactivity insertion and maintains the power level until “Bank R position low 3” signal is generated and dilution source isolation is triggered.

When the accident is identified to be the uncontrolled boron dilution according to the “Bank R position low 3” signal, the automatic fault diagnosis is activated and the emergency operating procedure is performed, including the manual power reduction and manual shutdown.

b) From Controlled State to Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurization according to specific rules as that descripted in Sub-section12.7.4.5.2.4.

12.7.4.5.3.5 Analysis Assumptions

a) Initial Conditions

The initial conditions assumed conservatively in reactivity control analysis for power operation condition in automatic control mode (state A) are as follows:

1) R control rod bank is at Bank R position low 3 position;
2) Critical core;
3) Negative reactivity insertion induced by xenon is excluded;
4) The borated water inventory of RCP [RCS] (except for the pressurizer and the dead zone at the top of the reactor pressure vessel) is 178t;
5) The dilution flow rate is considered as maximum value of 84.18t/h;
6) The water storage quantity of RCV [CVCS] pipeline is 1.44t;

b) Initial Event

As demonstrated in the Sub-section 12.7.4.5.2.5, only BOC case is analyzed.

c) Core-related Assumptions

1) All reactor coolant pumps keep functioning to ensure continuous mixing of borated water in the reactor pressure vessel;

2) Negative reactivity insertion induced by xenon is excluded;

3) 10% of uncertainty is included in the worth of R banks.

d) LOOP Assumption

The LOOP is considered as a consequence of turbine trip. As unintentional trip will not occur in this event, LOOP is not considered in this fault analysis.

e) Single Failure

For uncontrolled boron dilution at power operation conditions in automatic control mode, the isolation is triggered primarily on “Bank R position low 3” combining with the permissive signal P10. For the “Bank R position low 3” signal, redundant signals from independent channels of the Reactor Protection System (RPS [RPS]) and the majority voting logic (2 out of 4) are used.

The single failure can also be applied to automatic closure of redundant valves downstream of the Volume Control Tank (VCT) and hydrogen station.

f) Protection Signals

Dilution source isolation is triggered on the Bank R position low 3 signal combining with the permissive signal P10.

g) Control Systems

The function of control systems is not considered in the analysis.

12.7.4.5.3.6 Results

For uncontrolled boron dilution of reactivity control case at power operation conditions in automatic control mode, calculation results show that the R bank worth between “Bank R position low 3” and “Bank R position low 4” has time margin for all fuel cycles analysed, besides compensating the reactivity insertion by residual water from RCV [CVCS] and the reactivity insertion by dilution during the delay time.

For DNB case, the minimum DNBR is greater than the design limit of {
}.

12.7.4.5.4 Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS] (State A\B\C: Shutdown conditions)

12.7.4.5.4.1 Description

This section is dedicated to the analysis for uncontrolled boron dilution at shutdown condition.

Injection of water or borated water with lower boron concentration reduces the boron concentration of RCP [RCS] and induces a reactivity insertion, which potentially

results in unintentional criticality if it occurs during shutdown.

For shutdown condition, the G1, G2, N1, N2 and R banks are inserted and the shutdown banks are out of core. As an uncontrolled boron dilution occurs, it induces a neutron flux increase, which leads to RT. After reactor trip, positive reactivity insertion could still be induced by delay of dilution source isolation, dilution by water plug and RCP [RCS] cooling with negative isothermal temperature coefficient.

For SG maintenance (C3b) condition, coolant is provided by In-containment Refuelling Water Storage Tank (IRWST) (with enriched boron concentration of 1300-1400 ppm and boron-10 abundance of 35%) while administrative isolation is applied on REA [RBWMS] demineralized water makeup pipeline. Hence, the boron dilution is not considered under this condition.

12.7.4.5.4.2 Acceptance Criteria

The acceptance criteria to be considered for DBC-2 events are: Fuel integrity shall be ensured (no DNB and no fuel melting). For boron dilution at shutdown condition the acceptance criteria are:

a) The reactor remains subcritical after RT;

b) Isolation of dilution source is achieved.

12.7.4.5.4.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “High neutron flux (source range)” signal;

b) Closure of valves downstream of the VCT and hydrogen station is triggered on “High neutron flux (source range)” signal;

c) Automatic switchover of the intake of charging pump to IRWST with higher concentration (FC3) is triggered on “High neutron flux (source range)” signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of Emergency Boration System (RBS [EBS])

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of Safety Injection System (RIS [SIS]) in Residual Heat Removal

(RHR) mode

12.7.4.5.4.4 Typical Sequence of Events

The typical sequence of events includes the following two stages:

a) From Initiating Event to Controlled State

As positive reactivity is inserted, the neutron flux increases and triggers the “High neutron flux at shutdown” alarm (3Φ alarm) informing the operator of the dilution. The neutron flux increasing continues until “High neutron flux (source range)” signal triggers RT. Meanwhile, the “High neutron flux (source range)” signal will enable the charging pump of RCV [CVCS] linking to IRWST, initiating a fast and automatic isolation of the dilution source.

After reactor trip and dilution source isolation, the controlled state is reached. Under this state, the residual heat is removed by the VDA [ASDS] or RHR, and the feedwater is supplied by the ASG [EFWS]. Boric acid can be injected manually via RBS [EBS] following requirement of Operating Technical Specification (OTS).

b) From Controlled State to Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurization according to specific rules as that descripted in the Sub-section 12.7.4.5.2.4.

12.7.4.5.4.5 Analysis Assumptions

a) Initial Conditions

The initial conditions assumed conservatively in reactivity control analysis for shutdown condition (State A, B and C) are as follows:

1) For hot shutdown and cold shutdown conditions, all control rods are inserted in, except that SA, SB, SC and SD shutdown rod banks are out of the core;

2) Initial effective multiplication factor of the core is 0.99;

3) Negative reactivity insertion induced by xenon is excluded.

4) For cold shutdown condition, the borated water inventory in RCP [RCS] (except for the pressurizer and the dead zone at the top of the reactor pressure vessel) is 255t;

5) For hot shutdown condition, the borated water inventory in RCP [RCS] is 183t;

6) In RCV [CVCS], the water storage quantity in the pipeline from the isolation valve to reactor vessel is 2.775t;

7) The dilution flow rate is considered as maximum value of 87t/h;

8) The charging flow rate equals to the let-down flow rate;

9) A reactor coolant pump or a RHR pump keeps functioning to ensure continuous mixing of borated water in the reactor pressure vessel.

b) Initial Event

As demonstrated in the Sub-section12.7.4.5.2.5, only BOC case is analysed.

The shutdown conditions include cold shutdown, hot shutdown and transition from hot shutdown to cold shutdown.

c) Core-related Assumptions

The following positive reactivity introduction is considered in calculation of the final core sub-criticality:

1) Enveloping “high neutron flux (source range)” with supercritical reactivity of 300pcm;

2) Positive reactivity inserted in the delay time of dilution source isolation;

3) Positive reactivity inserted by water from the RCV [CVCS] pipeline (water plug);

4) A control rod cluster with the maximum reactivity worth stuck out of the core;

5) 10% of uncertainty on total worth of N-1 shutdown banks.

For initial event in transition from hot shutdown to cold shutdown some more conservative assumptions are included:

1) Bounding uncertainty of isothermal temperature coefficient;

2) Maximum cooling rate of { }.

d) LOOP Assumption

The LOOP is considered as a consequence of turbine trip. However, the turbine is out of operation at shutdown condition. Thus, LOOP is not considered in this fault analysis.

e) Single Failure

For shutdown conditions, reactor trip and dilution source isolation is triggered by “High neutron flux (source range)” signal.

As boration via RBS could be started by the operator after the controlled state achieved mitigating the failure of isolation, single failure is applied to the “High neutron flux (source range)” signal.

For the “High neutron flux (source range)” signal, redundant signals from independent channels of the RPS [RPS] and the majority voting logic (2 out of 3) are used.

f) Protection Signals

For shutdown condition, reactor trip and dilution source isolation is triggered on the “High neutron flux (source range)” signal. The setpoints are assumed to be rated values plus uncertainties.

g) Control Systems

The function of control systems is not considered in the analysis.

12.7.4.5.4.6 Results

For each condition, the core remains subcritical after reactor trip and dilution source isolation. The minimum sub-criticality of the reactor for all fuel cycles analysed is 733pcm, which occurs during transition from hot shutdown to cold shutdown.

12.7.4.5.5 Conclusions

The analysis shows that for power operation condition in manual control mode, the operator has enough time for intervention considering actions of protection system. For the most conservative condition, operator has at least 60 minutes for intervention in return to criticality. In automatic control mode, the maximum allowable delay time after the isolation signal is larger than the delay of this isolation. The reactivity introduced by the residual non-borated water in the RCV [CVCS] pipe and the non-borated water injected during the delay time after the isolation can be compensated by the R banks worth from rod position of “Bank R position low 3” to “Bank R position low 4”. During power operation, the DNBR is always greater than the design limit. For shutdown condition, the reactor can always maintain subcritical in order to ensure the safety of core.

Additionally, “no PCI-SCC” and “no PCMI” is demonstrated, Reference [9].

As the acceptance criteria are met, fuel and core integrity are ensured.

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in chapter 12.11.4.1.

12.7.5 Increase in Reactor Coolant System Inventory

12.7.5.1 Increase in RCP [RCS] Inventory RCV [CVCS] Malfunction

12.7.5.1.1 Description

An RCV [CVCS] malfunction causing an increase in RCP [RCS] inventory may result in the increase in pressuriser pressure and level. The cooling down of the RCP [RCS] causes a core power increase due to moderator feedback. This fault may occur in State A.

The RCV [CVCS] malfunction causing an increase in reactor coolant inventory may be caused by:

a) Abnormality of seal injection function of RCV [CVCS];

b) Abnormality of high pressure letdown function of RCV [CVCS];

c) Abnormality of charging function of RCV [CVCS];

d) RBS [EBS] malfunction;

e) Abnormality of low pressure letdown function of RCV [CVCS].

Compared to State B\C\D\E\F, the coolant temperature and nuclear power is the highest at full power in State A, Thus the bounding case for analysis is a RCV [CVCS] malfunction at full power level.

12.7.5.1.2 Acceptance Criteria

The increase in RCP [RCS] inventory due to RCV [CVCS] malfunction accident is considered as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.5.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “Pressuriser level high 1” signal；

b) Turbine trip and the ARE [MFFCS] full load isolation are actuated on receipt of reactor trip signal；

c) The RCV [CVCS] charging line is isolated following the “Pressuriser level high 1” signal；

d) The Seal Water Injection (SWI) for RCP [RCS] pumps is isolated on “Pressuriser level high 2” signal；

e) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

f) The VDA [ASDS] is actuated by “SG pressure high 1” signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.5.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

In this event, the PZR level increases. If the PZR level control fails to maintain the water level, reactor trip is triggered on “Pressuriser level high 1” signal or “Pressuriser pressure high 2” signal.

Turbine trip and the ARE [MFFCS] full load isolation are initiated on receipt of the reactor trip signal. The secondary pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. The RCV [CVCS] charging line is isolated following the “Pressuriser level high 1” signal. The SWI for RCPs is isolated on “Pressuriser level high 2” signal. The PSVs may open if the normal spray is unable to limit the increase in primary pressure.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all SGs and the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is

exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.5.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [29]. The main assumptions are listed as follows:

a) The initial event is considered to occur under full power condition.

b) The Doppler power coefficient is considered as its minimum absolute value, the moderator density coefficient is considered as its maximum absolute value.

c) The PZR pressure control is considered, because it limits the increase in primary pressure. The maximum spray capacity is considered.

d) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

e) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “Pressuriser level high 1” channel.

f) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreased greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.5.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [29]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.6 Decrease in Reactor Coolant System Inventory

12.7.6.1 Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction

12.7.6.1.1 Description

The RCV [CVCS] malfunction causes the reactor coolant inventory to decrease, which induces a RCP [RCS] pressure decrease and may therefore result in inadequate cooling of the fuel cladding through DNB. This fault may occur in State A and B.

Decrease in RCP [RCS] inventory due to RCV [CVCS] malfunction can be caused by:

a) An abnormality of seal injection function of RCV [CVCS];

b) An abnormality of high pressure letdown function of RCV [CVCS];

c) An abnormality of charging function of RCV [CVCS].

Since The coolant temperature and nuclear power at full power in State A is higher than that at any other power levels and State B, Thus the bounding case for analysis is a decrease in reactor coolant inventory at full power level.

12.7.6.1.2 Acceptance Criteria

The decrease in RCP [RCS] inventory due to RCV [CVCS] malfunction event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.6.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions are required:

a) reactor trip is triggered on “Pressuriser pressure low 2” signal;

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by “SG pressure high 1” signal;

d) RCV [CVCS] letdown line is isolated by “Pressuriser level low 1” and reactor trip signals;

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.6.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

In this event, the reactor coolant inventory and pressure decrease. If the pressure decrease cannot be stopped by the PZR pressure control system, the reactor trip is triggered to protect the core when the “Pressuriser pressure low 2” setpoint is reached.

After reactor trip, the RCCAs drop into the core and the core power decreases dramatically. Turbine trip and the ARE [MFFCS] full load isolation are initiated by the reactor trip signal. The secondary circuit pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. When the “Pressuriser level low 1” and reactor trip signals occur, the RCV [CVCS] letdown line is isolated.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all steam generators.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.6.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [30]. The main assumptions are listed as follows:

a) The initiating event is a faulty opening of both HP reducing stations while two

charging pumps are in operation at full power condition.

b) The Doppler power coefficient is considered as its maximum absolute value so as to minimise the decrease of core power, the moderator density coefficient is considered as its minimum absolute value so as to minimise the decrease of nuclear power.

c) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

d) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “Pressuriser pressure low 2” channel.

e) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreased greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.6.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [30]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]” fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the “Loss of Normal Feedwater

Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.6.2 Inadvertent Opening of a Pressuriser Safety Valve (State A)

12.7.6.2.1 Description

Inadvertent opening of a pressuriser safety valve is defined as the spurious opening of a PSV which can reseat in time when pressure drops to close setpoint during plant operation. Decrease in RCP [RCS] pressure may lead to inadequate cooling of the fuel cladding by DNB. This fault may occur in State A, B and C.

This event may be caused by spurious activation of PSV when PZR is under operation.

Since the core power and coolant temperature at full power level in State A are higher than that in State B\C, the consequence of inadvertent opening of a pressuriser safety valve in State A is the most severe. Thus the bounding case for analysis is inadvertent opening of a pressuriser safety valve at full power level.

12.7.6.2.2 Acceptance Criteria

Inadvertent opening of a pressuriser safety valve is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.6.2.3 Main Safety Functions

The reactor attains a new balance during the transient. Safety function is not required.

12.7.6.2.4 Typical Events Sequences

The inadvertent opening of a PSV causes the PZR pressure drops sharply and primary coolant temperature decreases. The core power is increased a little due to positive moderator density feedback. The opening PSV will reseat when the pressure drops to the setpoint. The reactor finally reaches a new equilibrium.

12.7.6.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [31]. The main assumptions are listed as follows:

a) The initiating event is that a PSV with lowest closure setpoint pressure is inadvertent opening.

b) The Doppler power coefficient is considered as its minimum absolute value so as to minimise the negative reactivity insertion caused by power increase. The moderator density coefficient is considered as its minimum value to minimise the negative reactivity insertion caused by coolant density decrease.

c) The RCCA having the highest worth is assumed to be stuck out of the core to

minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

d) The single failure is not considered in this event because no protection signal is actuated.

e) The impact of LOOP after turbine trip is not considered in this event because no reactor protection signal is actuated.

12.7.6.2.6 Results and Conclusions

The detailed analysis of this fault (see Reference [31]) shows that the minimum DNBR is { } which is greater than the design limit { }. The nuclear power changes slightly from the initial moment, and the fuel temperature changes slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

In this accident, there is no radioactivity release to the environment and the RPT-4 BSO is met.

12.7.7 Increase/Decrease in Reactor Coolant System Pressure

12.7.7.1 Spurious Pressuriser Heater Operation

12.7.7.1.1 Description

The unit controls the pressure of RCP [RCS] by controlling the pressuriser pressure. Proportional heaters and ON-OFF heaters are applied to increase the RCP [RCS] pressure. Two normal sprays that originate from the cold legs of two RCP [RCS] loops, and one auxiliary spray that originates from the RCV [CVCS] are used to reduce the RCP [RCS] pressure. A spurious pressuriser heating event leads to a pressure increase in the RCP [RCS]. This fault may occur in State A, B and C.

A spurious pressuriser heating event can be caused by:

a) Spurious pressuriser heater operation;

b) Failure of continuous spray.

Since the core power and coolant temperature at full power level in State A are higher than those in State B\C, the consequences of this fault in State B\C can be enveloped by those at full power level in State A. Thus the bounding case for analysis is the spurious pressuriser heater operation at full power level.

12.7.7.1.2 Acceptance Criteria

The spurious pressuriser heating operation event is considered as a DBC-2 event. The acceptance criteria to be considered for this event are:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.7.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “Pressuriser pressure high 2” signal;

b) Turbine trip and isolation of the full load main feedwater lines on all SG are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by “SG pressure high 1” signal;

d) The PSVs open when the PZR pressure reaches the setpoint;

e) The RHR safety valves open to mitigate the pressure increase when RHR pressure reaches the setpoint in State C.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurization;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.7.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

If a spurious pressuriser heating event occurs, the PZR pressure control system automatically switches off the heaters, and opens the normal spraying valves. The pressuriser pressure can be stabilised around its nominal vaule. No protection signal is actuated and the pressuriser safety valves do not open.

If the PZR heaters are not switched off automatically, reactor trip is actuated on the “Pressuriser pressure high 2” signal.

After reactor trip, the RCCAs drop into the core and the core power decreases dramatically. Turbine trip and the ARE [MFFCS] full load isolation are initiated by reactor trip signal. The secondary circuit pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. Then, the ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal. The PSVs may open if the normal spray is unable to limit the increase in primary pressure.

Finally, the reactor is in the hot shutdown state. The controlled state is reached. The residual heat is removed by the VDA [ASDS] of all steam generators.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable. In addition, the PZR heaters can be switched off by the operator manually 30 minutes later after RT

12.7.7.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [32]. The main assumptions are listed as follows:

a) The initiating event is a spurious pressuriser heater operation at full power level.

b) The Doppler power coefficient is considered as its minimum absolute value so as to maximise the increase of core power. The moderator density coefficient is considered as its maximum absolute value so as to maximise the increase of core power.

c) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

d) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “Pressuriser pressure high 2” channel.

e) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreased greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.7.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [32]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.7.2 Spurious Pressuriser Spray Operation

12.7.7.2.1 Description

A spurious pressuriser spraying event induces a pressure decrease on the primary circuit and may lead to inadequate cooling of the fuel cladding by DNB. This fault may occur in State A, B and C.

A spurious pressuriser spraying event can be caused by:

a) Spurious actuation of normal spray or auxiliary spray;

b) Failure of pressuriser heater.

Since the core power and coolant temperature at full power level in State A are higher than those in State B\C, the consequences of this fault in State B\C can be enveloped by those at full power level in State A. Thus the bounding case for analysis is the spurious actuation of normal spray or auxiliary spray at full power level.

12.7.7.2.2 Acceptance Criteria

The spurious pressuriser spraying event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.7.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is triggered on “Pressuriser pressure low 2” signal;

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) The VDA [ASDS] is actuated by “SG pressure high 1” signal.

d) The SI is actuated by “Pressuriser pressure low 3” signal.

e) The Medium Pressure Rapid Cooldown (MCD) is actuated on receipt of the SI signal.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.7.7.2.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

In this event, the RCP [RCS] pressure decreases. The pressure control system automatically switches off both normal and auxiliary spraying valves, and switches on the heaters.

If the pressure decrease cannot be stopped by the PZR pressure control system, reactor trip is triggered by “Pressuriser pressure low 2” signal.

After reactor trip, the RCCAs drop into the core and the core power decreases dramatically. Turbine trip and the ARE [MFFCS] full load isolation are initiated by the reactor trip signal. The pressure of secondary circuit is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. The pressure of primary circuit keeps decreasing so that the SI signal is triggered by the “Pressuriser pressure low 3” signal. Then the MCD is actuated following the SI signal, cooling down the RCP [RCS]. The RIS [SIS] starts injecting when the RCP [RCS] pressure is below the pump injection head. Then the pressure of primary circuit stabilises at a low level.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all steam generators.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.7.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [33]. The main assumptions are listed as follows:

a) The initiating event is spurious actuation of normal spray or auxiliary spray at full power condition.

b) The doppler power coefficient is considered as its maximum absolute value so as to minimise the decrease of core power. The moderator density coefficient is considered as its minimum absolute value so as to maximise the core power. .

c) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

d) Reactor trip is the only protection action before minimum DNBR appears, so the single failure can be chosen between one sensor or channel failure of reactor trip signal and the highest worth RCCA stuck out of the core. However, the highest worth RCCA stuck out of the core is considered as the conservative assumption. So the single failure is applied on one “Pressuriser pressure low 2” channel.

e) The main effect of LOOP is to cause the RCP [RCS] pumps to coast down. Since the reactor power decreased greatly before the RCP [RCS] pumps begin to coast down, LOOP caused by turbine trip has no effect on the minimum DNBR results. Thus LOOP is not considered in this fault analysis.

12.7.7.2.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [33]) shows that the minimum DNBR is { } which is greater than the design limit { }. Before the reactor trip, the nuclear power changes slightly from the initial moment, and the fuel temperature changes slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

b) From the Controlled State to the Safe State

The transient from the controlled state to the safe state is not explicitly analysed as it is bounded or represented by other faults in the following aspects:

1) In terms of sub-criticality, it is bounded by the “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]” fault. From the controlled state to the safe state, RCP [RCS] is borated by RBS [EBS] to compensate the reactivity resulting from RCP [RCS] cooldown. The sub-criticality margin of the bounding case

is the lowest due to the boron dilution. More boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by the "Loss of Normal Feedwater Flow" fault. From the controlled state to the safe state, ASG [EFWS] is used to cooldown RCP [RCS]. The bounding case is more onerous, as the consumption of water in ASG [EFWS] tank is the highest for DBC-2 event.

c) Radiological Consequence

The radiological consequence can be represented by the "Turbine Trip" fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.7.8 Fuel Pool Accidents

12.7.8.1 Loss of One PTR [FPCTS] (State A\B\C\D)

12.7.8.1.1 Description

Loss of One PTR [FPCTS] (State A\B\C\D) may cause inadequate cooling of the fuel assemblies in the Spent Fuel Pool (SFP). There are three independent PTR [FPCTS] trains (A/B/C). They have the same capacity, powered by individual electrical switchboard.

This fault may be caused by:

a) PTR [FPCTS] system failure;

b) Loss of cooling chains;

c) Loss of water intake.

12.7.8.1.2 Acceptance Criteria

Loss of one PTR [FPCTS] train (State A\B\C\D) is a DBC-2 event. The safety criteria for the DBC accidents associated with spent fuel storage pool are as follows:

a) Permanent maintenance of sub-criticality;

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

12.7.8.1.3 Main Safety Functions

When the RRI [CCWS] is available, all three PTR [FPCTS] cooling trains are provided by RRI [CCWS]. After loss of one operating train of the PTR [FPCTS], the last train is able to remove the decay heat from the SFP.

Except for the RRI [CCWS], the Extra Cooling System (ECS [ECS]) is available to remove heat from the Train A and Train B.

12.7.8.1.4 Typical Events Sequences

The transients of the loss of one PTR [FPCTS] train are shown as follows:

a) If one PTR [FPCTS] train is in normal operation, the other two are available. After loss of one operating train of the PTR [FPCTS], the last train is able to remove the decay heat from the SFP.

b) In the condition with preventive maintenance, the SFP is cooled down by a main cooling train, and the third one is started preventively while the second main train is in preventive maintenance. Once one PTR [FPCTS] train is lost, the third PTR [FPCTS] train, which is already in service, remains available for SFP cooling.

For this analysis, the controlled state can be considered to be reached from the initial time because of the long grace time before fuel uncovering.

12.7.8.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [34]. The following conservative assumptions are considered in the analysis:

a) 10% penalty factor is considered in the PTR [FPCTS] heat exchanger performance curve.

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

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

d) Before the accident, RRI [CCWS] inlet temperature is 38℃.

Once the SFP cooling system is recovered, the mean SFP water temperature is calculated in steady state, using the following assumptions:

a) The SFP is cooled by one PTR [FPCTS] cooling train.

b) A maximal RRI [CCWS] inlet temperature is 45℃.

Assumptions on Loss of offsite power (LOOP), single failure and preventive maintenance are as follows:

a) LOOP: LOOP is not considered in the DBC-2 safety analysis associated with fuel storage pool. The occurrence of initiating events associated with the fuel storage pool does not affect the core in the reactor building and does not cause the turbine trip.

b) Single Failure: Generally, one PTR [FPCTS] train is in operation and the other two are back up. After loss of the operating train of the PTR [FPCTS], the other PTR [FPCTS] trains are started up by the operator. However, one back up train is not considered because of the single failure assumption. The third train can remove the decay heat from the SFP.

c) Preventive Maintenance: when the second PTR [FPCTS] train is in preventive maintenance, the third PTR [FPCTS] train is started preventively. Once one PTR [FPCTS] train is lost, the backup train is working to remove the decay heat from the SFP.

12.7.8.1.6 Results and Conclusions

The analysis results are resumed as follows:

a) Temperature

The SFP cool down is ensured by the PTR [FPCTS] train C on the long term. The corresponding stabilized temperature is { }.

b) Grace Period

After the total loss of the cooling system and without accidental SFP draining, the average SFP temperature will reach 80℃ in about { } and 95℃ in { } respectively.

The analysis result shows that the temperature of the SFP will not reach 80℃ during the entire transient, and all the fuel assemblies are covered with water during the transient. Thus the acceptance criteria for this event are met.

In terms of radiological consequence, since no boiling occurs in the accident and fuel assemblies are always covered in the SFP, there is no radioactivity release.

12.7.9 Loss of Support Systems

12.7.9.1 Loss of RRI [CCWS] or SEC [ESWS] Train A (State A\B)

12.7.9.1.1 Description

This event is the representative of the following events which cause similar transient impact on the reactor core (Reference [100]):

a) Loss of DXS [ESWVS] train A;

b) SAR [ICADS] failure of providing compressed air for ARE [MFFCS] and RRI [CCWS] in Safeguard Building;

c) Loss of NI 690V SBO Power Distribution System (LJA/LJU [SBOPDS(NI-690V)]).

This event leads to loss of main feedwater superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]). Besides, the additional impact on other key safety functions is loss of MHSI train A, loss of LHSI train A and loss of RIS-RHR train A. This event may occur in State A and B.

The loss of main feedwater results in decrease in heat removal by the secondary system and increase in primary coolant temperature, which may lead to the risk of DNB.

The increase in charging flow or decrease in letdown flow due to control failure of RCV [CVCS] results in increase in primary coolant inventory, pressuriser pressure and level.

The decrease in charging flow or increase in letdown flow due to control failure of RCV [CVCS] results in decrease in primary coolant inventory and inadequate core cooling, which may lead to the risk of DNB.

The bounding case for analysis of this event is at full power level.

The following DBC-2 events cause similar transient impact on the reactor core:

a) Loss of Normal Feedwater Flow (Sup-chapter 12.7.2.3);

b) Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sup-chapter 12.7.5.1);

c) Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sup-chapter 12.7.6.1).

12.7.9.1.2 Acceptance Criteria

The loss of RRI [CCWS] or SEC [ESWS] train A (State A\B) event is classified as a DBC-2 event. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.7.9.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is actuated by the “SG level (narrow range) low 1” signal, “Pressuriser level high 1” signal or “Pressuriser level low 2” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

d) The VDA [ASDS] is actuated by the “SG pressure high 1” signal;

e) The PSVs are opened when the pressuriser pressure reaches the setpoint;

f) The RCV [CVCS] charging line is isolated following the “Pressuriser level high 1” signal;

g) The seal water injection for RCP [RCS] pumps is isolated on “Pressuriser level high 2” signal;

h) The RCV [CVCS] letdown line is isolated by “Pressuriser level low 1” and reactor trip signals.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

12.7.9.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

Although this event leads to multiple transient impact, it is estimated that the impact of loss of main feedwater is quicker than that of increase/decrease in RCV [CVCS] flow. Therefore, it is anticipated that reactor trip is automatically triggered by the earlier signal of “SG level (narrow range) low 1”, and thus leading to turbine trip.

After reactor trip, the PSVs may open if the normal spray is unable to limit the increase of primary pressure. The secondary pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. The ASG [EFWS] is automatically actuated by "SG level (wide range) low 2" signal to compensate for the secondary side inventory.

The RCV [CVCS] charging line, seal injection line and letdown line are automatically isolated if the corresponding signals are actuated.

Finally, the controlled state is reached. The core residual heat is removed by the VDA [ASDS] and the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.7.9.1.5 Results and Conclusions

Compared with loss of normal feedwater flow event (Sup-chapter 12.7.2.3), the reactor trip time of increase/decrease in RCV [CVCS] flow event (Sup-chapter 12.7.5.1 and 12.7.6.1) is later and the primary coolant temperature increase is less significant. Hence, there are reasons to believe that the transient evolution of loss of RRI [CCWS] or SEC [ESWS] train A (State A\B) event is similar to that of loss of normal feedwater flow event (Sup-chapter 12.7.2.3). Considering the DNBR margins shown in Sup-chapter 12.7.2.3, 12.7.5.1 and 12.7.6.1, it is justified that the DNBR limit will not be exceeded for loss of RRI [CCWS] or SEC [ESWS] train A (State A\B) event. The limit of fuel pellet temperature is not challenged since the core power is limited and no DNB occurs. Therefore, all the acceptance criteria are met.

Because the main safety functions required in Sup-chapter 12.7.2.3, 12.7.5.1 and 12.7.6.1 are very similar to and still available for loss of RRI [CCWS] or SEC [ESWS] train A (State A\B) event, it is justified that the controlled state and safe state can be reached.

The radiological consequence can be represented by the “Turbine Trip” fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.8 Analyses of DBC-3 Events

12.8.1 Increase in Heat Removal by the Secondary System

12.8.1.1 Reduction in Feedwater Temperature due to Feedwater System Malfunctions

12.8.1.1.1 Description

This event results in a sudden reduction in the feedwater temperature of the SGs. The reduction in feedwater temperature increases the heat transfer from the primary circuit to the secondary circuit, which results in a decrease of the primary coolant temperature and an insertion of positive reactivity. The core power increases, which potentially causes DNB. This fault may occur in State A and B.

Reduction in feedwater temperature due to feedwater system malfunctions event may be caused by:

a) Loss of two ABP [LPFHS] trains;

b) Loss of two AHP [HPFHS] trains.

At Reactor in Power (RP), the initiating events would lead to a decrease of feedwater. The event results to the increasing of core power and there is a risk of DNB. At full power, the power peak is maximum during the event, which is the most penalising case. Thus, the bounding case for analysis is reduction in feedwater temperature at full power level.

12.8.1.1.2 Acceptance Criteria

The reduction in feedwater temperature due to feedwater system malfunctions event is considered as a DBC-3 event. The fuel integrity might be challenged in this fault. For this event, the acceptance criteria of no DNB and no fuel melting, which are criteria for DBC-2, are conservatively applied. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The fuel pellet temperature shall not exceed { }℃.

12.8.1.1.3 Main Safety Functions

The reactor attains a new balance during the transient. Safety function is not required.

12.8.1.1.4 Typical Events Sequences

The reduction in feedwater temperature increases the heat transfer from the primary circuit to the secondary circuit, which results in a decrease of the primary coolant temperature and an insertion of positive reactivity. The core power is increased. The consequence of this event can be attenuated by the thermal capacity of the primary and secondary circuit. The reactor then reaches a new equilibrium.

12.8.1.1.5 Analysis Assumptions

The detailed assumptions are presented in the Reference [35]. The main assumptions are listed as follows:

a) The initial event is considered under full power condition. The hot shutdown condition is not explicitly analysed because the peak nuclear power is low. There is no DNB or fuel melting risk.

b) A conservative decrease of feedwater temperature by 55℃ is considered.

c) The moderator density coefficient is considered as its minimum value so as to penalises the DNBR calculation according to the sensitivity analysis. The Doppler power coefficient is considered as its minimum absolute value so as to maximise the increase of core power.

d) The RCCA having the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion after the reactor trip. The most conservative negative reactivity insertion curve as a function of time is used.

e) The single failure is not considered in this event because no protection signal is actuated.

f) The impact of LOOP after turbine trip is not considered in this event because no reactor protection signal is actuated.

12.8.1.1.6 Results and Conclusions

The detailed analysis of this fault (see Reference [35]) shows that the minimum DNBR is { } which is greater than the design limit { }. The nuclear power changes slightly from the initial moment, and the fuel temperature increases slightly. The fuel melting temperature limit is not challenged.

Thus the acceptance criteria for this event are met.

In this accident, the reactor finally reaches a new equilibrium. There is no radioactivity release to the environment and the RPT-4 BSO is met.

12.8.1.2 Steam System Piping Small Break Including Breaks in Connecting Lines

12.8.1.2.1 Initiating Event

The steam system piping small break including breaks in connecting lines might be caused by the break of steam systems and its connecting lines at the initial time. After the break occurs, the secondary steam flowrate increases. The RCP [RCS] coolant temperature and pressure will decrease, causing core overcooling. The core reactivity will increase due to the overcooling. The increase of reactivity in the core induces a rise in nuclear power at power operation or could result in a return to criticality during zero power condition.

12.8.1.2.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

a) The amount of fuel rods experiencing DNB must remain lower than 10%;

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

c) The peak cladding temperature must remain lower than 1482℃.

12.8.1.2.3 Main Safety Functions

In order to reach the controlled state, the following FC1 main safety functions are required:

a) Reactor trip is actuated by any of the following signals:

   1) Pressure drop of SG high 0;

   2) Pressure drop of SG high l;

   3) SG pressure low 1;

   4) Pressuriser pressure low 2.

b) The safety injection system can be actuated by “Pressuriser pressure low 3” signal.

c) Any of the following signals can lead to the quick closure of the MSIV to protect the RCP [RCS] against overcooling: “SG pressure low 1” or “Pressure drop of SG high l” signal.

d) Any of the following signals can lead to the ARE [MFFCS] isolation to protect the RCP [RCS] against overcooling:

   1) ARE [MFFCS] full load lines isolated on “RT” signal;

   2) ARE [MFFCS] low load lines isolated on “SG pressure low 2” signal.

e) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal.

In order to reach the safe state, the following FC2 manual safety functions are required:

a) Affected SG isolation

The affected SG is isolated manually to prevent the core overcooling and to limit the mass and energy release inside containment.

b) Startup of ASG [EFWS]

If the ASG [EFWS] for the unaffected SGs are not actuated automatically, the operator will start the ASG [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASG [EFWS].

c) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

d) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

e) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

f) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

g) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.8.1.2.4 Typical Sequences of Events

a) From the initiating event to controlled state

After the break occurs, the secondary steam flowrate increases. The RCP [RCS] coolant temperature and pressure will decrease, and causing core overcooling. The core reactivity will increase due to the overcooling. The increase of reactivity in the core induces a rise in nuclear power at power operation or could result in a return to criticality during zero power condition.

For full power condition, if the break size is not large enough, this accident might not cause a reactor trip, and the core power will remain at a higher level. The operator can identify this event via the “high core power” alarm signal. Once confirming the alarm, the operator will bring the reactor to the controlled state (i.e. hot showdown state).

For zero power condition, reactor trip is tripped by “Pressuriser pressure low 2”, “Pressure drop of SG high 0” or “Pressure drop of SG high l”. The closure of all MSIVs are triggered by the “SG pressure low 1” or “Pressure drop of SG high 1” signals, and ARE [MFFCS] full load lines for all SGs are isolated by reactor trip signal. ARE [MFFCS] low load line can also be isolated by “SG pressure low 2” signal. The “Pressuriser pressure low 3” signal would trigger the safety injection (RIS [SIS]). After the ARE [MFFCS] low load lines have been isolated, the “SG level (wide range) low 2” signal should initiate the ASG [EFWS] for the affected SG.

The RCP [RCS] cooldown induces positive reactivity in the core, and the reactor may return to criticality. However, the Doppler effect may limit the power excursion.

The RIS [SIS] supplies sufficient boron to compensate the reactivity insertion, bringing and maintaining the core sub-critical.

Thereafter, when the affected SG is empty and the heat removal is ensured by the VDA [ASDS] and ASG [EFWS] of the unaffected SGs, the controlled state is reached.

b) From the controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, the affected SG will be isolated as the first operator action. After that, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.8.1.2.5 Results and Conclusions

a) From the Initiating Event to Controlled State

For full power condition, this accident may not cause a RT. For zero power condition,

The results of steam system piping small break with a break size of DN50 is that the peaking thermal power is 1.91%FP which is listed in Sub-chapter 12.9.1.1. The core thermal power is relatively low, thus the DNBR is far beyond the design limit {

}

b) From the Controlled State to Safe State

This transient is not explicitly analysed as it is bounded or represented by the other faults from the following aspects:

1) In terms of sub-criticality, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown from controlled state to safe state. The capability of RBS [EBS] is abundant to bring the RCP [RCS] to safe state.

2) In terms of heat removal, it is bounded by “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG” fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case.

The consequences of this fault in State B can be enveloped by analysis in State A since the initial sub-criticality margin and the initial boron concentration are higher in state B, which reduces the moderator effect.

The present results show that no DNB occurs and the integrity of cladding is not challenged. The fuel pellet also remains intact since the nuclear power is not as intensive as rod motion accidents especially for rod ejection accident in which fuel temperature remains under the limit value.

c) Radiological Consequence

The radiological consequence is conservatively assumed to be the same with the accident of steam system piping large break. This is because that the fuel integrity and primary circuit integrity are not challenged with either accident, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of steam system piping large break is analysed in Sub-chapter 12.11.4.7.

12.8.2 Decrease in Heat Removal by the Secondary System

12.8.2.1 Inadvertent Closure of All or One Main Steam Isolation Valves

12.8.2.1.1 Initiating Event

The accident of inadvertent closure of one or all main steam isolation valves (MSIVs) is defined as the inadvertent closure of one or all main steam isolation valves on the steam line at the initial moment, which leads to a decrease in heat removal by the secondary system. The accident is typically caused by spurious Instrumentation and Control (I&C) closure signal.

Inadvertent closure of one MSIV will cause the main steam flowrate of the corresponding steam line reduce to zero, while inadvertent closure of all MSIVs will cause the main steam flowrate of all steam lines reduce to zero. By decreasing the heat removal capability of the secondary system, the temperature and pressure in reactor coolant system [RCS] (RCP) will increase and further lead to a decrease in departure from nucleate boiling ratio (DNBR) margin.

This fault may occur in state A and state B. Compared to state B, the core power is higher in state A, which will worsen the consequences of this fault. Inadvertent closure of one or all main steam isolation valves in state A is analysed.

12.8.2.1.2 Acceptance Criteria

The inadvertent closure of one or all main steam isolation valves (state A and state B) is classified as a DBC-3 event. The following acceptance criteria are used for DBC-3 events:

1) The amount of fuel rods experiencing departure from nucleate boiling (DNB) must remain less than 10%;
2) The peak cladding temperature must remain less than 1482℃;
3) The fuel pellet melting at the hot spot must not exceed 10% by volume.

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. The acceptance criteria to be considered for this event are as follows:

1) The minimum DNBR shall be greater than { };
2) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

12.8.2.1.3 Main Safety Functions

In order to reach the controlled sate, the following FC1 safety functions are required:

a) Reactor trip is triggered by any of the following signals:

1) SG pressure high 1;

2) Pressuriser pressure high 2.

b) Atmospheric steam dump system [ASDS] (VDA) is opened by the “SG pressure high 1” signal;

c) Pressuriser safety valves (PSVs) are opened when the pressure setpoints of pressuriser (PZR) is reached;

d) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) Turbine trips on receipt of reactor trip signal.

In order to reach the safe state, the following FC2 safety functions are required:

a) Startup of ASG [EFWS]

If the ASG [EFWS] are not actuated automatically, the operator will start the ASG [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASG [EFWS].

b) Startup/Isolation of emergency boration system [EBS] (RBS)

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

c) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rates are { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

d) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

e) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

f) Connection of safety injection system (RIS) in residual heat removal (RHR) mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.8.2.1.4 Typical Events Sequences

For this accident, the typical events sequence can be divided into the following two stages:

a) From the Initiating Event to the Controlled State

During the transient, the primary and secondary pressure increase gradually, reactor trip can be triggered by the “SG pressure high 1” signal or “Pressuriser pressure high 2” signal.

After reactor trip, residual heat is removed by the VDA [ASDS] of all available SGs. If the ARE [MFFCS] is not available, the feedwater supply is ensured by ASG [EFWS]. The RCP [RCS] will remain stable and the controlled state is reached.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration is performed via the chemical and volume control system RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit uses the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS] train. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation is performed by the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.8.2.1.5 Analysis Assumptions

The analysis only considers the process in the short-term phase, and includes following two cases:

- Case 1: Inadvertent closure of all main steam isolation valves (with loss of offsite power);
- Case 2: Inadvertent closure of one main steam isolation valve (with loss of offsite power).

All MSIVs are assumed to be inadvertently closed in Case 1 while one MSIV is assumed to be inadvertently closed in Case 2. The other main assumptions for two

cases remain same.

The detailed assumptions are presented in the reference [36]. The main assumptions are listed as follows:

a) Initial Conditions

Uncertainties are taken into account in the direction to penalize the minimum DNBR.

Initial values used in assumptions are as follow:

1) The initial power is the full power plus uncertainty;
2) The initial coolant temperature is the nominal value plus uncertainty;
3) The initial PZR pressure is the nominal value minus uncertainty;
4) The initial flowrate is the thermal design flowrate, considering that 10% of the SG tubes are plugged.

b) Core-related Assumptions：

The core-related assumptions are shown as follows:

1) The moderator temperature coefficient is assumed to be the minimum absolute value to minimize negative reactivity feedback due to the increase in coolant temperature.
2) The Doppler power coefficient is assumed to be the maximum absolute value to minimize the power drop.
3) The RCCA with the maximum worth is assumed to be stuck out of the core to minimize the negative reactivity after the reactor trip; at the same time, the most conservative negative reactivity insertion curve as a function of time is used.

c) LOOP Assumption:

The loss of offsite power (LOOP) is assumed to occur at the time of turbine trip, since it is considered as a consequence of turbine trip. LOOP leads to the loss of power supply to all RCP [RCS] pumps, feed water pumps and condensate pumps.

LOOP is considered in following analysis as it reduces primary coolant flowrate which is pessimistic for DNB analysis.

d) Single Failure：

The safety functions of reactor trip and VDA [ASDS] opening triggered by “SG pressure high 1” signal are actuated to mitigate the event consequences against acceptance criteria, thus the single failure assumption is applied on one channel of “SG pressure high 1” signal.

12.8.2.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see reference [36]) shows that the minimum DNBR is { }which is greater than the design limit { }. The limit of fuel pellet temperature and cladding temperature are not challenged since the core power is limited and no DNB occurs.

Thus the acceptance criteria for this event are met. For this accident, no DNB occurs and the limit of fuel pellet temperature and cladding temperature are not challenged. The fault analysis shows that the acceptance criteria are met.

b) From the Controlled State to the Safe State

This transient to reach safe state is not explicitly analysed as it is bounded or represented by other faults from the following aspects:

1) In terms of sub-criticality, it is bounded by "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From controlled state to safe state, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown, the sub-criticality margin of the bounding case is lowest due to the boron dilution, and more boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by "Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG" fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case, whereas at least two ASG [EFWS] trains are available in this fault.

c) Radiological Consequence

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.8.2.2 Medium Term LOOP of 24 Hours Duration

12.8.2.2.1 Overview

This sub-chapter describes the analysis for medium term loss of offsite power (LOOP) of 24 hours duration, which refers to the scenario that the offsite power supply cannot be restored from 2 hours to 24 hours. The analysis for short term LOOP, which means that the offsite power supply can be recovered within 2 hours, is presented in sub-chapter 12.7.2.2.

State A, state B, state C, state D, state E and state F are taken into account for this fault. LOOP is caused by:

a) A complete loss of offsite grid;

b) An onsite alternating current power distribution system failure;

c) An external grid disturbance (dropped voltage or frequency).

The analysis is divided into two parts according to their different initial conditions:

Part 1: LOOP in state A and B, as the RIS [SIS] in RHR mode is not connected to RCP [RCS] and the heat in RCP [RCS] is removed by the steam generators;

Part 2: LOOP in state C, state D, state E and state F, as the RIS [SIS] in RHR mode is connected and the heat in RCP [RCS] is removed by the RIS [SIS] in RHR mode.

12.8.2.2.2 Medium Term LOOP of 24 Hours Duration (State A\B)

12.8.2.2.2.1 Description

In state A and state B, LOOP leads to the loss of power supply to all reactor coolant pumps, feedwater pumps and condensate pumps. Because of the decrease of reactor coolant flow and the decrease of the secondary system heat removal capacity, the core heat removal capacity of the RCP [RCS] decreases. The event will result in overheating both on primary side and secondary side.

Compared to state B, the core power is higher and initial SG water inventory is lower in state A, which will worsen the consequences of this fault, so the consequence of LOOP in state A is more onerous than that in state B. Therefore, the medium term LOOP of 24 hours duration in state A is analysed in this section.

12.8.2.2.2.2 Acceptance Criteria

The medium term LOOP of 24 hours duration is classified as a DBC-3 event. The following acceptance criteria are used for DBC-3 events:

a) The amount of the fuel experiencing DNB must remain less than 10%;

b) The peak cladding temperature must remain less than 1482℃;

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

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than { };

b) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed{ }℃.

For short term LOOP (< 2 hours), the analysis regarding fuel integrity is performed in sub-chapter 12.7.2.2, which shows the above acceptance criteria are met.

For medium term LOOP (between 2 hours and 24 hours), as long as the following conditions are respected, the analysis regarding fuel integrity can be met.

a) The core remains sub-critical;

b) The residual heat can be continuously removed. For this accident, it means that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted. The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling. Emergency diesel generators can supply electricity to ASG [EFWS] pumps and RIS [SIS] pumps in the medium.

12.8.2.2.2.3 Main Safety Functions

In order to reach the controlled sate, the following FC1 safety functions are required:

a) Emergency diesel generators (EDG) are actuated by the “LOOP” signal;

b) Reactor trip is triggered by the “Low RCP [RCS] pump speed in two loops” signal when the permissive signal P7 exists, whereas reactor trip is triggered by the “Pressuriser pressure high 2” signal when the permissive signal P7 does not exist. The P7 signal is present when primary or secondary power is higher than 10%FP;

c) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

d) ASG [EFWS] can be actuated by the “SG level (wide range) low 2” signal;

e) VDA [ASDS] is actuated by the “SG pressure high 1” signal.

In order to reach the safe state, the following FC2 manual safety functions are required:

a) SG water level control

The SG water level is controlled by operator with adjusting the flowrate of the ASG [EFWS] injection in order to provide continuous heat removal.

b) RCP [RCS] boration

The RBS [EBS] pumps are started/stopped manually by the operator to control the boron concentration of RCP [RCS] and to ensure the sub-criticality margin in the RCP [RCS] is sufficient.

c) RCP [RCS] cooldown

The cooldown is performed by adjusting the steam flowrate via the VDA [ASDS] of available SGs in order to control cooling requested by the operator.

d) RCP [RCS] depressurisation

Because of LOOP, the normal spray is unavailable. The RCP [RCS] depressurisation is achieved by opening/closing PSV.

The operator should switch off the PZR heaters to prevent continuous heating of PZR during depressurisation.

e) Accumulators isolation

The accumulators are isolated to avoid the injection of accumulator water.

f) RIS [SIS] in RHR mode connection

The connection of the RIS [SIS] in RHR mode guarantees continuous heat removal and long-term core cooling.

12.8.2.2.2.4 Typical Sequence of Events

For this accident, the typical sequence of events includes the following two stages:

a) From initiating event to controlled state

LOOP leads to a reactor coolant flow decrease, and then the reduction of heat removal from the RCP [RCS] during the accident causes coolant temperature and pressure increases. After LOOP, the EDGs come into service, supporting the operation of the main systems related to the automatic protection functions. Reactor trip is triggered by the “Low RCP [RCS] pump speed in two loops” signal when the permissive signal P7 exists or by the “Pressuriser pressure high 2” signal when the permissive signal P7 does not exist.

During the transient, the ASG [EFWS] can be actuated when SG level reaches to the setpoint of the “SG level (wide range) low 2” signal, and the PSVs will open when the pressuriser pressure exceeds the opening thresholds. Moreover, the VDA [ASDS] will automatically open if the secondary pressure exceeds its threshold. Then, the reactor can be taken to and maintain in the controlled state.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, the operator performs primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.8.2.2.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [37]. The main assumptions are listed as follows:

a) Initial Conditions

The initial conditions are chosen to maximise RCP [RCS] heat-up and to penalise the consumption of the feedwater in ASG [EFWS] tanks.

1) The initial power is the full power plus 2% uncertainty;

2) The initial coolant temperature is the nominal value plus 2.5℃ uncertainty;

3) The initial PZR pressure is the nominal value plus 0.25MPa uncertainty;

4) Initial reactor coolant flowrate is equal to the thermal design flow (24000m^3/h per loop) considering 10% tube plugging of SGs;

5) The initial PZR level is set to the nominal value plus 7% uncertainty;

6) The initial SG level is set to the nominal value minus 10% uncertainty.

b) Single Failure

One EDG failure is taken into account since EDGs provide electricity to the safety systems, which ensures the mitigation of the accident. One EDG failure results in the failure of one ASG [EFWS] train, one RBS [EBS] train and one RIS [SIS] train.

c) Protection Signals

Reactor trip is triggered by the "Low RCP [RCS] pump speed" signal. VDA [ASDS] opening is actuated by the "SG pressure high 1" signal. ASG [EFWS] startup is actuated by the "SG level (WR) low 2" signal.

The uncertainty of actuation setpoint and the delay time between the setpoint actuation and startup of protective actions are set to maximise the consumption of the feedwater in ASG [EFWS] tanks.

d) Operator Actions

Operator actions from the Main Control Room are assumed to perform no earlier than 30 minutes after the first significant information is transmitted to the operator.

The required operator actions are as follows:

1) SG water level control by ASG [EFWS]

The SGs water level is manually controlled by operator with adjusting the flowrate of the ASG [EFWS].

2) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

Only one RBS [EBS] train is assumed to be available in this analysis.

3) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

In this analysis, the cooling rate is 28℃/h as only one RBS [EBS] train is assumed available.

In order to penalise the consumption of the feedwater in ASG [EFWS] tanks, the plant is maintained at the controlled state for 2 hours after reactor trip signal appeared.

4) RCP [RCS] depressurisation via PSV

The RCP [RCS] depressurisation is performed by operator via opening/closing of PSV.

5) PZR heaters switch-off

The operator switches off the PZR heaters at the beginning of the RCP [RCS] cooldown.

6) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

7) RIS [SIS] in RHR mode connection

The RIS [SIS] in RHR mode is connected to RCP [RCS] when the connection conditions are met:

- RCP [RCS] hot leg temperature ≤ { };
- RCP [RCS] hot leg pressure ≤ { }.

e) Safety Systems Performance

1) VDA [ASDS]

The setpoint of automatic VDA [ASDS] opening is set as the maximum value.

When Reactor cooldown begins, the VDA [ASDS] is manually controlled to realise 28℃/h cooling rate with one RBS [EBS] train in operation.

2) ASG [EFWS]

Only two SGs are fed, since the other ASG [EFWS] pump is lost because of the single failure assumption. The flowrate of ASG [EFWS] is assumed as the minimum value.

During the medium term phase, ASG [EFWS] is manually controlled by the operator to maintain the SG level in the two unaffected SGs at the nominal level.

3) RBS [EBS]

The RBS [EBS] is manually actuated at the beginning of the RCP [RCS] cooldown phase (2 hours after the reactor trip signal appeared) to ensure core sub-criticality during the RCP [RCS] cooldown.

Only one RBS [EBS] train is assumed to be available and thus the RCP [RCS] cooling rate is 28℃/h. This extends the process of the transient, thus increases the RCP [RCS] heat to be removed, and then penalises the consumption of feedwater in ASG [EFWS] tanks. The minimum flowrate is assumed to maximize the RCP [RCS] heat-up.

4) PSVs

Maximum values of opening pressure of the PSVs are selected. This maximises the heat removal through the secondary side and penalises the consumption of feedwater in ASG [EFWS] tanks.

f) Control Systems

Pressuriser heaters are taken into account and are assumed to produce a constant heat into RCP [RCS] to increase the heat to be removed out.

12.8.2.2.2.6 Results

The analysis shows that the RIS [SIS] in RHR mode connection conditions are reached about 7.5 hours after the occurrence of LOOP.

From the beginning of this event to the time when the RIS [SIS] in RHR mode connection conditions are reached, the ASG [EFWS] tanks total feedwater consumption is { } tons, less than the capacity of the ASG [EFWS] tanks { }. Therefore, the RIS [SIS] in RHR mode connection conditions can be reached before the ASG [EFWS] tank inventory is exhausted.

12.8.2.2.3 Medium Term LOOP of 24 Hours Duration (State C\D\E\F)

12.8.2.2.3.1 Description

In state C, D, E and F, LOOP can lead to the loss of power supply to all reactor coolant pumps, feedwater pumps, condensate pumps and RIS [SIS] pumps. As a consequence, the capacity of heat removal from the reactor core reduces, causing overheating in the primary side.

In state F, reactor is totally unloaded. Therefore, the fuel integrity and integrity of RCP [RCS] is not challenged in this state.

In state C to state E, the core is in the shutdown state. The plant cooling is mainly ensured by the RIS [SIS] in RHR mode. The reactor coolant is extracted from RCP [RCS] hot legs, and then injected into the RCP [RCS] cold legs after being cooled down by the RIS [SIS] heat exchangers. Different operating modes are defined according to RCP [RCS] temperature and pressure, RCP [RCS] water inventory, operating status of reactor coolant pumps and RIS [SIS] pumps, etc.

a) State C1: The RCP [RCS] temperature is between 100℃ and 140℃. The RCP [RCS] pressure is between { }. Two RIS [SIS] trains are in service, and at least one RCP [RCS] pump is in service.

b) State C2: The RCP [RCS] temperature is between 10℃ and 100℃. The RCP [RCS] pressure is between { }. At least two RIS [SIS] trains are in service, and at least one RCP [RCS] pump is in service.

c) State C3: The primary temperature is between 10℃ and 60℃. All the coolant pumps are stopped and at least two RIS [SIS] trains are in service. The RCP [RCS] loop level can decrease to 3/4 loop level.

For state C3a, the RCP [RCS] is still pressurisable. For special operation conditions in state C3a, during the nitrogen sweeping operation or the vacuum

operation, the RCP [RCS] pressure can be lower than atmospheric pressure.

For state C3b, the RCP [RCS] is non-closed and not pressurisable. The RCP [RCS] pressure is equal to atmospheric pressure. The reactor cavity is not fillable.

d) State D and E: The primary temperature is between 10℃ and 60℃. All the coolant pumps are stopped and at least two RIS [SIS] trains are in service. Since the RCP [RCS] is non-closed and not pressurisable, the RCP [RCS] pressure is equal to atmospheric pressure. The RCP [RCS] level is greater than or equal to 3/4 loop level.

In state C to state E, LOOP mainly affects the heat removal function and may lead to core uncovery. The main influence factors for the transient results are the decay heat, the RIS [SIS] trains in service, the RCP [RCS] pressure and the RCP [RCS] water inventory. The decay heat, RCP [RCS] water inventory and the RIS [SIS] trains in service determine the magnitude of the RCP [RCS] heat-up. The RCP [RCS] pressure mainly affects the core saturation margin.

For state C1 and state C2, the RCP [RCS] has the similar pressure range { } and RCP [RCS] water inventory. But the decay heat in state C2 is lower than state C1 and the trains of RIS/RHR in service in state C2 are more than or equal to state C2. Therefore, the results of medium term LOOP in state C2 can be enveloped by that in state C1.

For state C3a, the RCP [RCS] pressure and RCP [RCS] water inventory are both lower than state C1, so the results of medium term LOOP in state C3a cannot be enveloped by that in state C1, thus it should be analysed.

For state C3b, state D and state E, the decay heat is lower than state C3a and the RCP [RCS] loop level is equal or higher than state C3a, and the RCP [RCS] pressure (atmospheric pressure) is higher than the special operation conditions in state C3a. So the results of medium term LOOP in state C3b, D and E can be enveloped by that in state C3a.

Overall, only LOOP in state C1 and state C3a are analysed.

12.8.2.2.3.2 Acceptance Criteria

Compared to medium term LOOP in state A and state B, the heat in RCP [RCS] is mainly removed by the RIS [SIS] system in RHR mode in state C to state F. As long as the following conditions are respected, the analysis regarding fuel integrity can be met:

a) The core remains sub-critical;

b) The residual heat can be continuously removed, i.e., RCP [RCS] water inventory remains stable and the capacity of RIS [SIS] trains in RHR mode is able to satisfy the requirement of heat removal. Emergency diesel generators can supply

electricity to RIS [SIS] pumps in the medium term.

12.8.2.2.3.3 Main Safety Functions

In order to reach the controlled sate, the following FC1 safety functions are required:

a) Automatic actuation of EDGs following the LOOP signal can supply electricity to RIS [SIS] pumps and thus ensure the recovery of RIS [SIS] in RHR mode.

b) The safety injection might be actuated by any of the following signals:

   1) Hot leg ΔP_{sat} low 1 (for state C1);
   2) RCP [RCS] loop level low 1 (for state C3a).

c) The RIS [SIS] pumps in RHR mode trip might be actuated by any of the following signals:

   1) Hot leg ΔP_{sat} low 2 (for state C1);
   2) RCP [RCS] loop level low 2 (for state C3a).

The RIS [SIS] pumps are continuously powered by the EDGs in the medium term.

12.8.2.2.3.4 Typical Sequence of Events

The sequence of events consists of two phases: the short term phase until reaching of the controlled state by use of automatic actions, and the medium term phase when the plant is operated from the controlled state to the safe state.

a) From initiating event to controlled state

   LOOP leads to the loss of all the RCP [RCS] pumps in operation, the temporary loss of the heat removal function by the RIS [SIS] in RHR mode and the loss of secondary side feed water supplied (for state C1) by APA [MFPS] or by the AAD [SSFS].

   Following the LOOP, EDGs will be automatically actuated. Then, RIS [SIS] pumps in RHR mode, which are already in service before LOOP, will be automatically restored with the power supply from the EDGs. So, the RHR function can be automatically is restored. Then, the reactor can be taken to and maintained in the controlled state.

b) From controlled state to safe state

   The RHR function is maintained with the power supply from the EDGs in the medium term.

12.8.2.2.3.5 Analysis Assumptions

The detailed assumptions are presented in Reference [37]. The main assumptions are listed as follows:

a) Initial Conditions

The medium term LOOP in state C1 and state C3a are discussed above. For state C3a, two plant operation phases are studied: the reactor shutdown phase and the reactor start-up phase.

The analysed three cases are as follows:

1) Case 1: Medium term LOOP in state C1

- LOOP is assumed to occur at the earliest time of sate C1 (8.5 hours after core shutdown), which leads to the most conservative decay heat;
- The assumptions for RCP [RCS] pressure and temperature (2.4MPa, 143.5℃) lead to the lowest saturation margin;
- The RCP [RCS] loop level is at the RPV flange joint level corresponding to the lowest level for state C1, leads to the fastest temperature rise;

2) Case 2: Medium term LOOP in state C3a of shutdown phase

- LOOP is assumed to occur at the earliest time of the state C3a in shutdown phase (39.5 hours after core shutdown), which leads to the most conservative decay heat;
- The assumptions for RCP [RCS] pressure and temperature lead to the lowest saturation margin (0.09MPa, 63.5 ℃, nitrogen sweeping operation);
- The RCP [RCS] loop level is at the 3/4 loop level corresponding to the lowest level for state C3a, leads to the fastest temperature rise;

3) Case 3: Medium term LOOP in state C3a of start-up phase

- LOOP is assumed to occur at the earliest time of the state C3a in start-up phase (243 hours after core shutdown), which leads to the most conservative decay heat;
- The assumptions for RCP [RCS] pressure and temperature lead to the lowest saturation margin (0.02MPa, 58.5℃, vacuum operation);
- The RCP [RCS] loop level is at the 3/4 loop level corresponding to the lowest level for state C3a, leads to the fastest temperature rise;

b) Core-related Assumptions

For conservative consideration of the core heat generation, the following assumptions are adopted:

1) The maximum decay heat is used.
2) For the analysed cases, the decay heat is assumed to be constant during the transient.

c) Single Failure

Since the core heat removal is mainly ensured by RIS [SIS] in RHR mode, the single failure is postulated as that one EDG is unavailable, which leads to the function failure of one RIS [SIS] train in RHR mode.

d) Protection Signals

The following signals may be triggered after LOOP in state C to state E:

1) Safety injection signals – "Hot leg ΔP_{sat} low 1" or "RCP [RCS] loop level low 1"

   The maximum negative uncertainty is taken into consideration to penalise heat removal by safety injection as much as possible.

2) RIS [SIS] pumps in RHR mode trip signal – "Hot leg ΔP_{sat} low 2" or "RCP [RCS] loop level low 2"

   The maximum positive uncertainty is taken into consideration to penalise heat removal by RHR as much as possible.

e) System Performance

1) For all three cases, two RIS [SIS] trains are in operation in RHR mode at the initial time. About 53s after LOOP occurrence, the RHR function is restored with the power supply from the EDGs. Due to the single failure of one EDG, only one RIS [SIS] train in RHR mode is restarted.

2) The flowrate of LHSI and RRI [CCWS] is the nominal value minus uncertainty and the inlet temperature for the RRI [CCWS] is conservatively set as the maximum value.

3) The power generated by the LHSI pump is set as the maximum value to increase the power transmitted to the fluid.

These assumptions limit the heat removal capacity of RIS [SIS] trains in RHR mode.

12.8.2.2.3.6 Results

Heat balance calculations are performed to verify that the capacity of RIS [SIS] trains in RHR mode is able to satisfy the requirement of heat removal. The analysis results for the three cases are as follows:

a) Case 1

During the period of the temporary loss of the RHR function, 53s after LOOP, the maximum temperature of RCP [RCS] reaches 144.8℃, lower than { } (corresponding to the maximum design temperature of RIS [SIS] trains connected in RHR mode), so the normal RIS [SIS] train in RHR mode can be restarted following the automatic start-up of EDGs. The minimum ΔP_{sat} is 2.0MPa during the transient, which is higher than the "Hot leg ΔP_{sat} low 1" and "Hot leg ΔP_{sat} low 2". There is no risk of core uncovery and the RIS [SIS] pump in RHR mode trip can be avoided. One RIS [SIS] train in RHR mode is able to remove the residual heat in the long term.

b) Case 2

About 2h after LOOP, the maximum RCP [RCS] temperature reaches 86.0℃, lower than the saturation temperature (96.7℃) at 0.09MPa. Therefore, there is no risk of core uncovery and the RIS [SIS] pump in RHR mode trip will not occur. The heat removal can be ensured in the medium term.

c) Case 3

Heat balance calculation result shows that the RCP [RCS] temperature can increase to 75.4℃ about 3h after LOOP. Since LOOP leads to the shutdown of the vacuum pumps, which will not be powered by the EDGs. The RCP [RCS] pressure gradually rises to atmospheric pressure, and the primary coolant will not saturate during the transient. Therefore, there is no risk of core uncovery and the RIS [SIS] pump in RHR mode trip can be avoided. The heat removal can be ensured by RIS [SIS] trains in RHR mode in the medium term.

12.8.2.2.3.7 Conclusions

The fault analysis in state A and state B indicates that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted, and the heat removal can be ensured by RIS [SIS] trains in RHR mode in the medium term, then the plant can be maintained in the safe state within 24 hours.

The fault analysis in state C to state F indicates that there is no risk of core uncovery and the heat removal can be ensured in the medium term.

For medium term LOOP, boration is used to compensate the reactivity resulting from RCP cooldown via RBS [EBS]. The capacity of RBS is able to satisfy the requirement of sub-criticality margin. Therefore, the core can remain sub-critical during the transient.

Therefore, for medium term LOOP of 24 hours duration in state A to state F, the acceptance criteria presented in section 12.8.2.2.2.2 and section 12.8.2.2.3.2 are met.

Considering that there is no fuel failure during the transient and long term cooling is ensured, the radiological consequence could be considered fairly low. The

confinement of radioactive substances is analysed in dedicated source term and dose analysis.

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.8.2.3 Feedwater System Piping Small Break Including Breaks in Connecting Lines to SG (State A\B)

12.8.2.3.1 Initiating Event

This event is defined as the small break occurring in feedwater system line or in a SG connecting line (DN<50mm). As the break occurs, the main feedwater losses through the break, and the feedwater flowrate to the SG is decreased. This reduces the secondary side heat remove capacity, causing the increase of RCP [RCS] temperature and pressure.

State A and state B are taken into account in this fault. For state A and state B, the mitigation measures are similar. The initial reactor power in state B is lower than state A, and the SG secondary water inventory in state B is larger than state A. So the heat removal capacity of secondary side in state B is higher than state A, the consequence of state B is not severe than state A. Therefore, the fault of FLB in state A is analysed in this section.

12.8.2.3.2 Acceptance Criteria

The feedwater system piping small break including breaks in connecting lines to SG is classified as a DBC-3 event. The fuel integrity and RCP [RCS] integrity might be challenged in this fault.

a) For analysis from initiating event to controlled state, the following acceptance criteria are adopted:

    1) The amount of fuel rods experiencing DNB must remain less than 10%;

    2) The peak cladding temperature must remain less than 1482℃;

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

For this transient, it is considered that if the RCP [RCS] loops remain full, the core is covered and the bulk boiling does not occur, the fuel integrity is guaranteed. As result, the criteria presented above are met if the core remains covered and bulk boiling does not occur in the core.

b) For analysis from controlled state to safe state, the aim of the study is to

demonstrate that the plant can be brought from controlled state to safe state and maintained in the safe state by FC1 and FC2 systems before the ASG [EFWS] tank inventory is exhausted, that is:

1) The core remains sub-critical. After reactor trip, boration is used to compensate the reactivity resulting from RCP [RCS] cooldown via RBS [EBS]. The capacity of RBS [EBS] is sufficient to satisfy the requirement of sub-criticality margin. Therefore, the core can remain sub-critical during the transient.

2) The residual heat can be continuously removed. For this accident, it means that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted. The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.8.2.3.3 Main Safety Functions

In order to reach controlled state, the following main FC1 safety functions are required:

a) Reactor trip is triggered by the “SG level (narrow range) low 1” or Pressuriser pressure high 2” signal;

b) Turbine trip and isolation of the full load main feedwater lines of all SGs are actuated on receipt of reactor trip signal;

c) The isolation of low load main feedwater lines of all SGs is triggered by the “Pressure drop of SG high 2” or “SG pressure low 2” signal;

d) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) VDA [ASDS] opening is triggered by the “SG pressure high 1” signal;

f) MSIVs closure is triggered by the “SG pressure low 1” signal;

g) RCP [RCS] pumps are triggered by the “SG level (wide range) low 4” signal;

h) Manual isolation of ASG [EFWS] of affected SG.

i) From Controlled State to Safe State

In order to reach the safe state, the following FC2 manual safety functions are required:

a) Affected SG isolation

The affected SG is isolated manually to prevent the drainage of the corresponding ASG [EFWS] tank and to limit the mass and energy release inside containment, and to allow re-supply of feedwater to the unaffected SGs.

b) Realign of ASG [EFWS] injection

If the ASG [EFWS] of an unaffected SG is unavailable, after affected SG isolation, the ASG [EFWS] of affected SG shall be switched to the unaffected SG, by opening/closing related isolation valves.

c) SG water level control

The SG water level is controlled by operator with adjusting the flowrate of the ASG [EFWS] injection in order to provide continuous heat removal.

d) RCP [RCS] boration

The RBS [EBS] pumps are started/stopped manually by the operator to control the boron concentration of RCP [RCS] and to ensure the sub-criticality margin in the RCP [RCS] is sufficient.

e) RCP [RCS] cooldown

The cooldown is performed by adjusting the steam flowrate via the VDA [ASDS] of unaffected SGs in order to control cooling requested by the operator.

f) RCP [RCS] depressurization

The RCP [RCS] depressurisation is realized by opening the PSVs or pressuriser spray.

g) Accumulators isolation

The accumulators are isolated to avoid unexpected injection.

h) RIS [SIS] in RHR mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous RCP [RCS] heat removal and long term core cooling.

12.8.2.3.4 Typical Events Sequences

A typical sequence of events, where automatic actions and manual actions are presented, can be divided into the following two stages:

a) From initiating event to controlled state

At the beginning of the transient, the affected SG feedwater flowrate decreases due to the feedwater line break, causing the decrease of the affected SG level, which reduces the capacity of heat removal from the RCP [RCS]. Therefore, the RCP [RCS] pressure and temperature will increase.

The affected SG level continues to decrease and once the level reaches the setpoint of the “SG level (narrow range) low 1” signal, reactor trip is triggered, resulting in the turbine trip and main feedwater isolation. When the SG level decreases to the setpoint of “SG level (wide range) low 2”, ASG [EFWS] is activated to supply emergency feedwater to SG. Meanwhile, the RCP [RCS] pressure can be limited by opening of PSVs and the RCP [RCS] decay heat can be removed by the VDA [ASDS] and ASG

[EFWS]. Therefore, the residual heat can be continuously removed. On the other hand, the ASG [EFWS] of affected SG is isolated by operator, and the reactor can be taken to the controlled state.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, the affected SG will be isolated firstly. After that, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray. PSVs can be used when the pressuriser spray is unavailable.

12.8.2.3.5 Results and Conclusions

a) From initiating event to controlled state

The consequence from initiating event to controlled state of this event is bounded by the “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG” for the following reasons:

1) The initial conditions and safety functions used to mitigate the event is same;

2) For the small break in this event, the water break flow is much lower than in the large break size considered in the “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG”, which results in lower RCP [RCS] temperature and pressure. Therefore, the overheating consequence is less severe.

b) From controlled state to safe state

The consequence from controlled state to safe state of this event is also bounded by the “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG”. In the bounding event, not only the main feedwater to the affected SG is lost throuth the break, but also the affected SG water inventory is discharged through the break, causing less usable water mass for the secondary heat removal. This leads more heat remaining in the RCP [RCS] before the ASG [EFWS] is actuated and causes

more ASG [EFWS] tank water consumption. As a result, the consequence from controlled state to safe state is bounded by the "Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG".

c) Radiological Consequence

The radiological consequence of this accident can be bounded by the accident of steam system piping small break including breaks in connecting lines. The fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity release pathways are the same which include the release of secondary coolant through VDA and through piping break. However, more airborne radioactivity will be released to the environment in the accident of the steam system piping small break than that of the feedwater system piping small break.

The radiological consequence of the bounding case of steam system piping small break including breaks in connecting lines is conservatively assumed to be the same with the accident of steam system piping large break, which is analysed in Sub-chapter 12.11.4.7.

12.8.3 Decrease in Reactor Coolant System Flowrate

12.8.3.1 Forced Reduction in Reactor Coolant Flow (3 Pumps)

12.8.3.1.1 Initiating Event

The forced reduction in reactor coolant flow is caused by a simultaneous fault in the power supplies to all the reactor coolant pumps. A rapid decrease in the off-site grid frequency can lead to a reversal of motor torque and thus to decrease the pump speed, which reduces the coolant flow.

The decrease in reactor coolant flow causes deterioration of heat transfer, further leads to an increase in core average coolant temperature, system pressure and a decrease in margin to DNB. The main difference of the initiating event between the forced reduction in reactor coolant flow and the LOOP event is the pump performance. Due to the reversal of motor torque, the pump speed and the coolant flow rate decrease more quickly in the accident of forced reduction in reactor coolant flow.

This fault might occur in state A, state B and state C. Compared to state B and state C, the core power is higher in state A, which will worsen the consequences of this fault. Therefore, the consequence of forced reduction in reactor coolant flow in state A is more onerous than that in state B and state C. Forced reduction in reactor coolant flow in state A is analysed.

12.8.3.1.2 Acceptance Criteria

The forced reduction in reactor coolant flow (3 pumps) is classified as a DBC-3 event. The following acceptance criteria are used for DBC-3 events:

a) The amount of the fuel experiencing DNB must remain less than 10%;

b) The peak cladding temperature must remain less than 1482℃;

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

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than { };

b) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

12.8.3.1.3 Main Safety Functions

In order to reach the controlled state, the following FC1 safety functions are required:

a) Reactor trip is triggered by the “Low RCP [RCS] pump speed in two

loops" signal when the permissive signal P7 exists, whereas reactor trip is triggered by "Pressuriser pressure high 2" signal when the permissive signal P7 does not exist. P7 is present when primary or secondary power is higher than 10%FP;

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) ASG [EFWS] is actuated by the "SG level (wide range) low 2" signal;

d) VDA [ASDS] is opened by the "SG pressure high 1" signal;

e) RCP [RCS] pumps shutdown is triggered by the "Low RCP [RCS] pump speed in two loops" when the permissive signal P7 exists.

In order to reach the safe state, the following FC2 safety functions are required:

a) Startup of ASG [EFWS]

If the ASGs [EFWS] are not actuated automatically, the operator will start the ASGs [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASGs [EFWS].

b) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

c) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

d) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

e) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

f) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.8.3.1.4 Typical Events Sequences

A typical events sequence, where automatic actions and manual actions are presented,

can be divided into the following two stages:

a) From the Initiating Event to the Controlled State

After a frequency drop on the off-site grid, the RCP [RCS] pumps speed decrease and when it reaches the setpoint of "Low RCP pump speed" signal, reactor trip is triggered and then the turbine trips automatically. After this, ARE [MFFCS] full load lines are automatically closed.

The EDGs come into service following the failure of the off-site grid to support the operation of the main systems related to the automatic protection functions.

During the transient, the ASG [EFWS] can be actuated when SG level reaches to the setpoint of the "SG level (wide range) low 2" signal, and the PSVs will open when the pressuriser pressure exceeds the opening thresholds. Moreover, the VDA [ASDS] will automatically open if the secondary pressure exceeds its threshold. Therefore, the reactor can be maintained in the controlled state.

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.8.3.1.5 Analysis Assumptions

The detailed assumptions are presented in the reference [38]. The main assumptions are listed as follows:

a) Initial Conditions

The analysis at 100%FP is addressed since it is the worst case.

The statistical method with { } is applied in DNBR design limit calculation, in which the uncertainties of core power, core temperature, core pressure and enthalpy rise hot channel factor ($F_{\Delta H}$) are taken into account. Therefore, it is

unnecessary to consider the uncertainties of these parameters in the initial state of transient in which the DNBR design limit based on statistical method is applied.

Initial conditions values used in assumptions are as follows:

1) The initial operating power is 100%FP;
2) The initial average coolant temperature is 307℃;
3) The initial pressuriser pressure is 15.5MPa;
4) The initial reactor coolant flowrate is set as the thermal design flow (24000m³/h per loop), considering that 10% of the SG tubes are plugged;
5) The forced reduction in reactor coolant flow happens at initial time, and the drop rate of off-site grid frequency is 4Hz/s. The requirement of frequency variation in GB grid code is 1 Hz/s that is described in Reference [39]. The constant decrease rate of 4 Hz/s covers the possible disturbance of the external grid. So this value is conservative for the forced reduction in RCP flow accident.

b) Core-related Assumptions

The core-related assumptions are shown as follow:

1) The moderator density coefficient is considered as the minimum absolute value (0 $\Delta k/k/g/cm^3$) to minimize negative reactivity feedback due to increase in coolant temperature.
2) Doppler power coefficient is set as the maximum absolute value to minimize the power drop.
3) The RCCA with the maximum worth is assumed to be stuck out of the core to minimize the negative reactivity after the reactor trip; at the same time, the most conservative negative reactivity insertion curve as a function of time is used.
4) The specific axial power distribution and radial power distribution will be adopted in DNB analysis. The enthalpy rise hot channel factor ($F\Delta H$) shall be calculated via the formula below:
   $F\Delta H=1.59, P\geq 1;$
   $F\Delta H=1.59\times[1+0.3(1-P)], P<1;$
   Where P is the fraction of the rated power.

c) LOOP Assumptions

The loss of offsite power (LOOP) is assumed to occur at the time of turbine trip. For this accident, the RCP [RCS] pumps trip due to “Low RCP pump speed” signal, which occurs earlier than LOOP caused by turbine trip. Therefore, LOOP has no

effect for the DNB analysis.

d) Single Failure:

Before minimum DNBR appears, the reactor trip and RCP [RCS] pump trip, which are triggered by “Low RCP pump speed” signal, will be actuated to mitigate the event consequences against acceptance criteria. Thus, the single failure assumption is applied on one channel of “Low RCP pump speed” signal. As a long-term mitigation means which has no effect on DNB analysis, EDGs has not been applied with single failure.

e) Protection Signals

Reactor trip and RCP [RCS] pumps shutdown are triggered by “Low RCP [RCS] pump speed in two loops with the permissive signal P7 presence” signal. In order to delay the protective actions to mitigate the consequences, the actuation setpoint is assumed to be its nominal value minus uncertainty and maximum delay time between the setpoint actuation and startup of protective actions is considered.

f) Safety System Performance

Before minimum DNBR appears, safety systems such as ASG [EFWS], VDA [ASDS] will not be activated. Therefore, the safety systems’ performance has no effect on the transient analysis and DNB analysis.

g) Control Systems

The pressuriser spray is assumed to be available and spray flowrate is set as the maximum value to minimize the primary pressure, which will worsen the consequences of DNB analysis. The pressurizer heaters are not taken into account.

12.8.3.1.6 Results and Conclusions

a) From the Initiating Event to the Controlled State

The detailed analysis of this fault (see Reference [38]) shows that show that the minimum DNBR is { } which is greater than the design limit { }. The limit of fuel pellet temperature and cladding temperature are not challenged, since the core power is limited and no DNB occurs.

For this accident, no DNB occurs and the limit of fuel pellet temperature and cladding temperature are not challenged. The fault analysis shows that the acceptance criteria are met.

b) From the Controlled State to the Safe State

This transient to reach safe state is not explicitly analysed as it is bounded or represented by other faults from the following aspects:

1) In terms of sub-criticality, it is bounded by “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]” fault. From controlled state to safe state, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown, the sub-criticality margin of the bounding case is lowest due to the boron dilution, and more boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG” fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case, whereas at least two ASG [EFWS] trains are available in this fault.

c) Radiological Consequence

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.8.4 Reactivity & Power Distribution Anomalies

12.8.4.1 Inadvertent Core Loading of Fuel Assemblies (State A\B\C\D\E)

12.8.4.1.1 Initiating Event

The inadvertent loading of fuel assembly includes one or more fuel assemblies placed in improper positions, one or more fuel rods made of pellets with improper enrichment or the whole fuel assembly made of pellets with improper enrichment during the manufacturing process. If the enrichment of the fuel assembly misplaced at a certain place in the core is higher than that of the expected fuel assembly, an increase in the neutron flux at the position will be caused.

12.8.4.1.2 Acceptance Criteria

The inadvertent loading of a fuel assembly in an improper position is defined as a DBC-3 event (infrequent event).

The inadvertent loading of fuel assembly can cause significant changes in core power distribution. Various loading errors will increase the peak of power distribution significantly, and will be detected by the in-core neutron flux detector.

The purpose of the inadvertent loading analysis is to show that a loading error will not influence the safe operation of the plant, as it can either be easily detected or be considered acceptable if the DNBR criteria for DBC-3 accident are met.

12.8.4.1.3 Main Safety Functions

The quality control process during the fuel manufactory process limits the possibility of fuel rods or fuel assembly made of pellets with improper enrichment, and also limits the possibility of burnable poison rods being placed in wrong place.

One or more fuel rods made of pellets with improper enrichment or a whole fuel assembly made of pellets with improper enrichment can be avoided by the fuel vendor. During manufacturing process, three actions are realized to avoid any wrong pellet enrichment in a fuel rod:

- Before any enrichment modification, a complete cleaning of the rod manufacturing line is performed in order to remove all residual pellets with a wrong enrichment.

- A traceability is applied to all manufacturing stations to avoid any use of wrong components.

- A gamma-scanning checking is performed on all manufactured rods in order to detect a wrong enrichment which differs from the targeted enrichment. A fuel rod with wrong enrichment is automatically excluded.

After the fuel rod manufacturing, a tracer is placed in each fuel rod to follow it during the fuel assembly manufacturing process. The fuel assembly can then be traced during

shipping process.

As a consequence, only one or more fuel assemblies being placed in improper positions need to be considered for inadvertent core loading of fuel assemblies analysis.

To minimise the possibility of the inadvertent loading, each fuel assembly is marked with a code and loaded as the core loading chart indicates. During the loading, each assembly shall be checked for its identification number before being carried to the core. After the fuel assembly is placed in core, its number will be recorded in the loading chart so that it can be checked that the core has been loaded correctly.

During power operation, the abnormal of power distribution can be detected with the in-core Instrumentation System during startup physical tests while getting the flux map.

12.8.4.1.4 Typical Events Sequence

For each possible inadvertent loading scheme, the following calculations are performed:

{

}

12.8.4.1.5 Analysis Assumptions

Inadvertent loading of instrumented assemblies would be easily detected. For in-core detector positions, the distortion is obvious. Thus, inadvertent loading of instrumented assemblies is not considered.

The top view of the assemblies with and without control rods is quite different and it might cause mechanical impossible when connected to Control Rod Drive Mechanism (CRDM). Thus, the swap between assemblies with and without control rods is not considered.

The following aspects shall be taken into consideration for the inadvertent loading scheme:

{

}

12.8.4.1.6 Results and Conclusions

{

}

The analyses show that inadvertent loading of a fuel assembly in an improper position will not threaten reactor core safety, since it either can be detected by detectors during the start-up due to great power variations or can be considered acceptable if the DNBR criteria for DBC-3 accident are met.

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not

challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.8.4.2 Uncontrolled Single RCCA Withdrawal

12.8.4.2.1 Description

Uncontrolled Single RCCA Withdrawal can occur in the following situations:

a) Case 1: When the core is under manual control mode, a single RCCA can be withdrawn due to operator error, caused by their misunderstanding that the RCCA is misaligned or dropped. In this case, it is assumed there is a:

   1) Malfunction of a single rod position detector;

   2) Disregard of operating procedures and misunderstanding of the alarm signal produced during RCCA withdrawal.

a) Case 2: When the core is under automatic control, several simultaneous electrical or mechanical failures can cause withdrawal of a single RCCA. This assumes:

   1) Simultaneous and independent electrical or mechanical failures;

   2) Misunderstanding of the respective alarm signals.

The Uncontrolled Single RCCA Withdrawal accident cause an insertion of positive reactivity, resulting in an increase in the core power, coolant temperature and hot channel factor, especially around the withdrawal position. Thus, the local power peak may lead to a low DNBR around the withdrawal position. The DNBR could drop below the design limit, potentially leading to fuel cladding failure.

This fault might occur in state A, state B and state C. Compared to state B and state C, the core power is higher and the sub-criticality margin is less in state A, which will worsen the consequences of this fault. Therefore, the consequence of the uncontrolled single RCCA withdrawal accident in state A is more onerous than that in state B and state C. The uncontrolled single RCCA withdrawal accident in state A is analysed.

12.8.4.2.2 Acceptance Criteria

The uncontrolled single RCCA withdrawal (State A) is classified as a DBC-3 event. The following acceptance criteria are used for this fault:

a) The amount of fuel rod experiencing DNB must remain lower than 10%;

b) The peak cladding temperature must remain lower than 1482℃;

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

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than {
};

b) The peak cladding temperature must remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

12.8.4.2.3 Main Safety Functions

In order to reach the controlled state, the following FC1 safety functions are required:

a) Reactor trip is triggered by the “Overtemperature ΔT” signal;

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) VDA [ASDS] is actuated by the “SG pressure high 1” signal;

d) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal.

In order to reach the safe state, the following FC2 manual safety functions are required:

a) Startup of ASG [EFWS]

If the ASGs [EFWS] are not actuated automatically, the operator will start the ASGs [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASGs [EFWS].

b) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

c) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

d) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

e) Accumulators isolation

The accumulators are isolated to avoid the injection of accumulator water.

f) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.8.4.2.4 Typical Events Sequence

A typical event sequence, where automatic actions and manual actions are presented, can be divided into the following two stages:

a) From the initiating event to the controlled state

After the withdrawal of a single RCCA, reactor trip can be triggered. This limits the local power peak and mitigates the consequence of the accident. After reactor trip, the ARE [MFFCS] full load lines are isolated. The decay heat is removed via the VDA [ASDS] of all SGs and the feedwater is supplied by the ARE [MFFCS] low load lines without LOOP or ASG [EFWS] with LOOP. Therefore, the decay heat can be continuously removed and the controlled state is subsequently reached.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.8.4.2.5 Analysis Assumptions

The detailed assumptions are presented in the reference [41]. The main assumptions are listed as follows:

a) Initial Conditions

In order to minimize the DNBR and maximize the cladding temperature, the key thermal hydraulic parameters of transient analysis are set as follows:

1) The initial power is set to the full power plus 2% uncertainty;

2) The initial coolant temperature is set to the nominal value plus 2.5℃ uncertainty,;

3) The initial PZR pressure is set to the nominal value minus 0.25MPa uncertainty;

4) The initial flow is set to the thermal-hydraulic design flow (24000m^3/h per loop);

5) The initial state corresponds to the cases with R bank at the insertion limit when the axial-offset at the extreme right hand-edge of the operating diagram.

b) Core-related Assumptions

1) Neutronic data

- In order to cover the fuel management plan, all fuel cycles and three burn-up levels (BCX, MOC, EOC) are selected in the transient analysis;
- The imbalance of radial power distribution caused by single RCCA withdrawal is considered.

2) Feedback effect

Because different feedback effects affect the core power response which would lead to different protective actions, two sets of feedback coefficients are considered in the transient analysis as follows:

- Minimum reactivity feedback: assuming the minimum moderator density coefficient and minimum doppler power coefficient.
- Maximum reactivity feedback: assuming the maximum moderator density coefficient and maximum doppler power coefficient.

c) LOOP Assumption

The loss of offsite power (LOOP) is assumed to occur at the time of turbine trip as it reduces primary coolant flowrate which is pessimistic for DNB and fuel thermal transient simulation.

d) Single Failure

Before minimum DNBR appears, the reactor trip, which is triggered by “Overtemperature ΔT” signal, will be actuated to mitigate the event consequences against acceptance criteria. Thus, the single failure assumption is applied on one channel of “Overtemperature ΔT” signal.

e) Protection Signals

Reactor trip is triggered by the “Overtemperature ΔT” signal. In order to delay the protective actions to mitigate the consequences of this event, the maximum delay time between the “Overtemperature ΔT” setpoint actuation and reactor trip triggering is considered, which is shown in Table 1. Moreover, the radial power unbalance brought by the withdrawal of a single RCCA has been taken into account, the “Overtemperature ΔT” signal obtained from the coldest loop is used in transient

analysis to delay the reactor trip.

f) Safety Systems Performance

Before minimum DNBR appears, safety systems such as ASG [EFWS], VDA [ASDS] will not be activated. Therefore, the safety systems performance has no effect on the transient analysis and DNB analysis.

g) Control Systems

The uncontrolled single RCCA is withdrawn at the initial time. In order to get the most conservative calculations, reactivity withdrawal speeds are considered from minimum to maximum for the control system. Two typical withdrawal speeds are studied: 8 steps/minute and 72 steps/minute.

The pressuriser spray is assumed to be available and spray flowrate is set as the maximum value to minimize the primary pressure, which will worsen the consequences of DNB analysis. The pressurizer heaters are not taken into account

12.8.4.2.6 Results and Conclusions

a) From the initiating event to the controlled state

1) For the cases with minimum reactivity feedback effect

The uncontrolled single RCCA withdrawal which withdraws at the initial time cause an insertion of positive reactivity and unbalanced heat removal rate between primary and secondary sides on SG resulting in an increase in the core power, coolant temperature and hot channel factor, especially around the withdrawal position. Therefore, the DNBR will decrease after the withdrawal of a single RCCA. When reactor trip occurs, the core power and the average coolant temperature begin to drop, thus the DNBR increases.

The minimum DNBR is { } which is greater than the design limit { }.

For the worst-case (EOC, minimum reactivity feedback, withdrawal speed of 72 steps/minute), the results are:

- The maximum fuel cladding temperature is 1213℃;
- The maximum fuel temperature is { }℃, as the fuel melting temperature limit is { }℃. Thus the amount of fuel melting at the hot spot is 0 %.

2) For the cases with maximum reactivity feedback effect

The nuclear power and temperature in the reactor increase slightly because of the negative reactivity feedback, and the reactor trip signal is not triggered. The minimum DNBR is { } which is greater

than the design limit { }. Therefore, the consequence for these cases is less pessimistic, thus the cladding temperature limit and the fuel pellet melting limit are not challenged. Additionally, “no PCI-SCC” and “no PCMI” is demonstrated, Reference [9].

b) From the controlled state to the safe state

This transient to reach safe state is not explicitly analysed as it is bounded or represented by other faults from the following aspects:

1) In terms of sub-criticality, it is bounded by “Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP[CSTS]” fault. From controlled state to safe state, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown, the sub-criticality margin of the bounding case is lowest due to the boron dilution, and more boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG” fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case, whereas at least two ASG [EFWS] trains are available in this fault.

c) Radiological Consequence

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity are maintained during both accidents, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.8.5 Decrease in Reactor Coolant System Inventory

12.8.5.1 Rupture of a Line Carrying Primary Coolant outside Containment (State A\B\C\D\E)

12.8.5.1.1 Initial Event

The loss of primary coolant outside containment may result from the failure of:

a) The RCV [CVCS], including the RCV [CVCS] connecting lines;

b) The nuclear sampling system (REN [NSS]).

The maximum break equivalent area with regards to reactor coolant depletion corresponds to the minimum area of the RCV [CVCS] letdown line (i.e. 60 cm^2). Small breaks that could be compensated by the RCV [CVCS] are not analysed in this sub-chapter. Therefore, only the largest breaks occurring on the RCV [CVCS] letdown line are analysed.

Austenitic stainless steels are used for the components connecting the RCV [CVCS] and the REN [NSS] that are used for the primary coolant because of its high resistance to generalised corrosion during operation and cold shutdown conditions. Precautions are taken to avoid other sources of localised corrosion by means of monitoring and optimising the chemical composition of the primary coolant and austenitic stainless steels. The chloride and oxygen content in the primary coolant is controlled to avoid pitting of materials during operation, which can also protect the stainless steel against corrosion cracking. The risk of rupture caused by corrosion on the RCV [CVCS] and the REN [NSS] is therefore reduced.

A loss of coolant accident (LOCA) occurring on a line carrying primary coolant outside the containment induces a loss of primary coolant, potential decrease in RCP [RCS] pressure (if the loss flowrate cannot be compensated by the RCV [CVCS]) and radioactive release to the environment. This accident may lead to a decrease in reactor coolant inventory and potential core overheating.

Rupture of a line carrying primary coolant outside containment (state A\B\C\D\E) is classified as a DBC-3 event.

12.8.5.1.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak Cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

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

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

However, if the core remains covered during the transient, above criteria are considered to be met. Thus the consequences of this accident are analysed against the following aspects:

a) Core remains covered;

b) The plant shall be brought to and maintained in controlled state;

c) The plant shall be brought to and maintained in safe state.

12.8.5.1.3 Main Safety Functions

a) FC1 safety functions

1) Reactor trip

In state A, if the core power is higher than 10 % Full Power (FP), reactor trip is triggered by the “Pressuriser pressure low 2” signal, and if the core power is lower than and equal to 10 % FP, reactor trip is triggered by the “Hot leg pressure low 1” signal.

2) Turbine trip

The reactor trip signal triggers the turbine trip.

3) ARE [MFFCS] full load line isolation

Following the reactor trip signal, ARE [MFFCS] full load lines of all SGs are isolated.

4) ARE [MFFCS] low load line isolation

Following the signal, SG level (narrow range) high 0 after reactor trip, ARE [MFFCS] low load lines of all SGs are isolated.

5) MHSI and LHSI startup

MHSI and LHSI are actuated when receiving SI signal. SI signal is triggered by the “Pressuriser pressure low 3" signal.

6) Isolation of Reactor Coolant Pressure Boundary (RCPB)

RCV [CVCS] letdown line is isolated via isolation of RCPB when receiving

SI signal. It isolates the break and stops RCP [RCS] coolant inventory depletion. SI signal is triggered by the “Pressuriser pressure low 3" signal.

7) ASG [EFWS] startup

It is triggered by “LOOP and SI signal” or by the “Steam generator level (wide range) low 2” signal.

8) Medium pressure rapid cooldown (MCD)

Following the SI signal, a MCD is initiated to cool the primary circuit with a rate of { }.

9) Stop of Reactor Coolant Pumps

The shutdown of reactor coolant pumps is triggered by the “RCP ΔP low 1 and SI signal” signal.

10) Accumulator injection

Accumulator injects borated water to cold leg when the primary pressure decreases below the injection pressure of accumulator.

11) Opening of Atmospheric Steam Dump System (VDA [ASDS])

The VDA [ASDS] valves automatically open when the secondary pressure reaches the VDA [ASDS] setpoint.

b) FC2 safety functions

These functions are all manual actions in the main control room.

1) Reactor coolant system boration

The RBS [EBS] pumps are started by the operator before the reactor coolant system cooldown for reactor coolant system boration.

2) Reactor coolant system cooldown by SGs

The cooldown is performed via the VDA [ASDS] of secondary side for primary depressurization.

3) Containment isolation

Containment isolation is performed by isolation valves and therefore prevent leaks from containment building penetration.

4) MHSI stop

The MHSI pumps are shut down for primary depressurization.

5) Accumulators isolation

Accumulators need to be isolated to prevent nitrogen entering the reactor coolant system.

6) RIS [SIS] in RHR mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

In state C\D\E, FC1 safety functions to achieve controlled state and FC2 safety functions to reach safe state are listed below:

a) FC1 safety functions

1) Safety injection (SI)

In state C1/C2, SI is triggered by the "Hot leg ΔP_{sat} low 1" signal.

In state C3/D/E, SI is triggered by the "RCP [RCS] loop level low 1" signal.

2) Isolation of RCPB

RCV [CVCS] letdown line are isolated via isolation of RCPB when receiving SI signal. It isolates the break and stops RCP [RCS] coolant inventory depletion.

3) Stop of Reactor Coolant Pumps (RCPs)

In state C1/C2/C3a, RCPs are stopped by the "RCP ΔP low 1 and SI" signal.

4) Stop of RIS [SIS] pump(s) in RHR mode

In state C1/C2, RIS [SIS] pumps in RHR mode are stopped by the "Hot leg ΔP_{sat} low 2" signal.

In state C3/D/E, RIS [SIS] pumps in RHR mode are stopped by the "RCP [RCS] loop level low 2" signal.

b) FC2 safety functions

1) Reactor coolant system cooldown by SGs

The cooldown is performed via the Atmospheric Steam Dump System (VDA [ASDS]) of SGs.

2) ASG [EFWS] startup

ASG [EFWS] is actuated to control the SGs water level.

3) Containment isolation

Containment isolation is performed by isolation valves and therefore prevent leaks from containment building penetration.

4) MHSI stop

The operator stops the MHSI pumps when the pressuriser level is sufficient, since the water inventory can be guaranteed due to the break isolation.

5) RIS [SIS] train in RHR mode re-established

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

12.8.5.1.4 Typical Events Sequences

a) From the initiating event to controlled state

For short term phase, the break leads to rapid drop of the reactor coolant system pressure and pressuriser level, as well as possible core heat up.
In state A\B, following actions or signals could be triggered:

1) Reactor trip
2) Turbine trip
3) ARE [MFFCS] full load line isolation
4) ARE [MFFCS] low load line isolation
5) MHSI and LHSI startup
6) Isolation of Reactor Coolant Pressure Boundary (RCPB)
7) ASG [EFWS] startup
8) Medium pressure rapid cooldown (MCD)
9) Stop of Reactor Coolant Pumps
10) Opening of Atmospheric Steam Dump System (VDA [ASDS])

In state C\D\E, following actions or signals could be triggered:

1) Safety injection (SI)
2) Isolation of RCPB
3) Stop of Reactor Coolant Pumps (RCPs)
4) Stop of RIS [SIS] pump(s) in RHR mode.

Core sub-criticality is ensured by the rod drop negative reactivity effects, which acts in addition to the RIS [SIS] boron injection.

The controlled state is reached when the following conditions are met:

1) The core is sub-critical;
2) The RCP [RCS] coolant inventory is stable or increasing to the correct level;

b) From controlled state to safe state

In controlled state, the reactor coolant inventory is stable or increasing and the core decay heat is removed via the SGs until the situation where the connecting conditions for the RIS [SIS] to operate in RHR mode are reached. Once one RIS [SIS] train is connected to the RCP [RCS] in RHR mode, the following conditions are met:

1) The core is sub-critical due to the boration performed by the operator.

2) The decay heat is removed via the RIS [SIS] in RHR mode.

12.8.5.1.5 Analysis Assumptions

This fault in terms of decoupling acceptance criteria is bounded by the analysis of IB-LOCA (see Sub-section 12.9.5.2) and RHR-LOCA (see Sub-section 12.9.5.5).

12.8.5.1.6 Results and Conclusions

a) From the initiating event to the controlled state

This fault in terms of decoupling acceptance criteria is bounded by the analysis of IB-LOCA (see Sub-section 12.9.5.2) and RHR-LOCA (see Sub-section 12.9.5.5). Thus the decoupling acceptance criteria are met.

b) From the controlled state to the safe state

The transient to reach safe state is not explicitly analysed as it is bounded by the following aspects:

1) In terms of sub-criticality, for the accidents with comparatively large break size, MHSI injection is able to provide abundant boron to compensate the reactivity and ensure core sub-criticality. For the accidents with comparatively small break size, MHSI injection is not able to ensure core sub-criticality. Without considering MHSI injection, the RBS [EBS] is able to provide abundant boron to compensate the reactivity and ensure core sub-criticality.

2) In terms of heat removal, it is bounded by IB-LOCA (state A\B) (see Sub-section 12.9.5.2.) and RHR-LOCA (state C\D\E) (see Sub-section 12.9.5.5). In this event, the break will be isolated either by automatic signal or manual operation and the water inventory could be guaranteed. In addition, the available safety function for residual heat removal in this event is similar to that in IB-LOCA (state A\B) (see Sub-section 12.9.5.2.) and RHR-LOCA (state C\D\E) (see Sub-section 12.9.5.5).

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed and presented in Sub-section 12.11.4.4.

12.8.5.2 SG Tube Rupture (SGTR) (one tube) (State A\B\C)

12.8.5.2.1 Initiating Event

This sub-chapter describes the thermal-hydraulic analysis of a steam generator tube rupture event. The steam generator tube rupture event is defined as the double-ended guillotine rupture of a single steam generator (SG) tube.

This accident will lead to an increase in radioactivity in the secondary system due to the leak of radioactive coolant to the secondary system from the reactor coolant system (RCP [RCS]). If a loss of offsite power or failure of the condenser steam dump system happens during this event, discharges of steam or liquid from the main steam safety valve (MSSV) and/or the VDA [ASDS] will lead directly to a discharge of activity to the atmosphere, as the damaged steam generator will be contaminated. The radioactivity of the primary side coolant is caused by corrosion and fission products generated through the continuous operation of the reactor with a limited number of damaged fuel rods.

The probability and risk of steam generator tube rupture (SGTR) event is reduced through the following precautions:

a) High ductility of SG tube material;

b) Blowdown system location at the bottom of SG tube bundle to prevent solid deposits on SG tube plate;

c) Chemically conditioned secondary water to protect SG tubes from corrosion;

d) Prevention of projectiles originating from the main feedwater;

e) Specification of SG support plates to prevent tube damage and pipe whip (of neighbouring tubes) following tube rupture;

f) Continuous monitoring and control of secondary side activity.

The SGTR (one tube) in state A\B\C is classified as a DBC-3 event.

The cases studied in this sub-chapter correspond to the double-ended guillotine rupture of one tube in one SG, which allows unimpeded blowdown from both ends of the tube.

The rupture is located in the lower part of the SG tubes bundle, close to the tubesheet, on the cold side. This location maximises the SGTR leak flowrate. For DBC-3 transients, a LOOP is considered part of the event, if it adds further pessimism.

This sub-chapter aims to quantify the maximum amount of radioactivity release to the environment. If overfilling occurs, contaminated water will be directly released to the environment and the radioactivity release will be significant. Therefore, an SG overfilling assessment is performed (see Reference [42]) and the analysis result

demonstrates that, even if under the most onerous conditions, overfilling will not occur. Without overfilling, the radioactivity is released to the environment via steam. The case presenting the most pessimistic radioactivity release is analysed hereafter.

12.8.5.2.2 Acceptance Criteria

The major issue for SGTR is to limit its radiological consequences. The acceptance criteria, adopted in SGTR, aim to ensure core safety and limit radiological consequences. The safety criterion for SGTR is the dose equivalent released to the environment. The main objective of SGTR transient analysis is to evaluate the core safety and provide interface data for radiological consequences analysis.

The SGTR transient is analysed against the following aspects:

a) Core remains covered;

   As there is no significant reactivity insertion during SGTR fault, this criterion indicates that fuel integrity can be ensured in case of SGTR.

b) There shall be no water flowing through the MSSV, to prevent the MSSV from seizing open;

c) The plant shall be brought to and maintained in safe state.

12.8.5.2.3 Main Safety Functions

The following structures, systems and components, their related functions and operator actions are claimed in the analysis of SGTR.

a) Alarm

   SGTR detection by the “high activity in the Plant Radiation Monitoring System (KRT [PRMS])” signal: when high activity is detected in the KRT [PRMS], an alarm is actuated to inform the operator.

b) FC1 safety functions (automatic)

   1) Reactor trip

      Reactor trip is triggered either by the “Pressuriser pressure low 2” signal or by the “SG level (Narrow Range (NR)) high 1” signal.

   2) Turbine trip

      The reactor trip signal triggers the turbine trip.

   3) ARE [MFFCS] full load line isolation

      Following the reactor trip signal, the ARE [MFFCS] full load line for all SGs is isolated. In a penalizing way, the ARE [MFFCS] low load line is supposed to be isolated at the reactor trip signal.

4) APG [SGBS] isolation

APG [SGBS] discharge is isolated when ASG [EFWS] is actuated.

5) Safety injection

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

6) Medium pressure rapid cooldown

Following the SI signal, a medium pressure rapid cooldown (performed by all SGs, including the SGa) is initiated to cool the primary circuit with a rate of { }.

7) ASG [EFWS] actuation

ASG [EFWS] is actuated either by the “SI and LOOP” signal or by the “SG level (Wide Range (WR)) low 2” signal.

8) VDA [ASDS] opening

The VDA [ASDS] is opened by the “SG pressure high 1” signal.

b) FC2 safety functions (manual from the main control room)

1) SGa isolation

After SGTR detection, the operator isolates the SGa (if not already done), comprising ARE [MFFCS] and ASG [EFWS] isolation, MSIV closure and an increase in the VDA [ASDS] setpoint.

2) RCV [CVCS] charging line isolation

The RCV [CVCS] charging line is isolated manually.

3) Reactor coolant system boration

The RBS [EBS] pumps are started by the operator before the reactor coolant system cooldown. The RBS [EBS] injection is stopped when the primary cold shutdown state boron concentration is reached.

4) Reactor coolant system cooldown by unaffected SGs

The cooldown is performed via the VDA [ASDS] of unaffected SGs. The cooling rate is { } with at least two RBS trains in operation.

5) RCP [RCS] and SGa depressurisation:

During RCP [RCS] depressurisation, the accumulators are isolated when the RCP [RCS] pressure has decreased below { }.

Two of the three Medium Head Safety Injection (MHSI) pumps are stopped at the beginning of operation. The last MHSI pump stops when the TRIC is

reduced to { }.

Reactor coolant system is then depressurised until the low head safety injection (LHSI) injection pressure is reached. Because of the normal spray is conservatively assumed unavailable, the reactor coolant system depressurization is achieved by means of opening the VDA [ASDS] of the SGa.

6) RIS [SIS] in RHR mode connection:

The connection of the RIS [SIS] in RHR mode guarantees continuous heat removal and core long term cooling.

As the maximum injection head of MHSI will directly determine the primary and secondary pressure balance behaviour, the performance of MHSI should be verified by SGTR events.

Besides, when the SGa needs to be isolated, the VDA setpoint is adjusted above the maximum injection head of MHSI to prevent continuous opening and unstoppable release. This function is dedicated to SGTR mitigation.

Another important factor to the radiological consequences of SGTR is the cool-down rate of MCD. As the radiological consequences of SGTR challenges the numerical targets, cool-down rate of MCD should be verified of SGTR events.

12.8.5.2.4 Typical Events Sequences

A typical sequence, the most likely to occur during the transient, is described hereafter. Within this sub-chapter, the following description considers only the full power condition for this is the most onerous case for radiological release, and the overfilling case is described in Reference [42].

The sequence of events consists of two phases: the short-term phase until leak elimination and the long-term phase where the plant is operated from the leak elimination to the safe state. A typical sequence of events in state A is described hereafter.

a) From the initiating event to leak elimination (short term)

1) From the initiating event to the controlled state

The controlled state for SGTR is defined as a state when core coolant inventory remains stable and residual heat removal can be ensured via the SGs.

At the beginning of this event, primary coolant leaks to the secondary side through the break, which leads to the contamination of the affected SG. Meanwhile, the primary pressure decreases. The reactor trip signal triggered depends on the initial conditions. For full power operation: The SGTR can be

identified by the operator receiving the “High activity in the main steam system (VVP [MSS]) radiation monitoring system (KRT)” signal. Reactor trip is triggered by the “Pressuriser pressure low 2” signal. Turbine trip and isolation of ARE [MFFCS] full and low load lines for all SGs are initiated following the reactor trip signal.

After reactor trip and turbine trip, the secondary pressure increases and rapidly reaches the setpoint of the VDA [ASDS], if the GCT [TBS] is unusable. Contaminated steam is thus released to the environment and decay heat is removed.

The continuous leakage to secondary side and the decrease in decay heat after reactor trip leads to a primary depressurisation. It is likely the “Pressuriser pressure low 3” signal will be triggered. Within this sub-chapter, the following description assumes the break is large enough to lead to the “Pressuriser pressure low 3” signal.

Following the safety injection signal triggered by the “Pressuriser pressure low 3” signal, the Medium pressure rapid cooldown (MCD) is actuated. The MCD is carried out by reducing the VDA setpoint in order to cool the reactor coolant system with a rate of { }. When the MCD is complete, the secondary pressure is reduced to { }. The medium-head safety injection (MHSI) pumps are actuated by the SI signal and start injecting when the primary pressure is lower than their injection head. The MHSI injection flow can compensate for the leak flow from the SGTR and the controlled state is reached.

2) From the controlled state to the leak elimination

To stop the leak, the operator isolates the SGa from both the steam side and feed side. In other words, the operator closes the ASG [EFWS] and the MSIV. The VDA [ASDS] setpoint of the SGa is adjusted up to a value between the MHSI injection head and MSSV setpoint in order to limit the radioactive release.

The injection of MHSI maintains the primary pressure at a stable level. To reduce the leakage flow, the operator shuts down two of the three MHSI pumps (with the remaining left operating). Due to the isolation of the SGa, the pressure of SGa increases until it reaches primary pressure level and the leak is stopped. Before the leak is stopped, the SGa is not overfilled and only steam is released to the environment.

b) From the leak elimination to the safe state (long term)

The safe state for SGTR is defined as a state when the RIS [SIS] train is connected to the reactor coolant system in residual heat removal (RHR) mode, and the SGa remains

isolated. The operator performs primary cooldown and depressurisation to reach the RHR connection conditions, which are:

1) Reactor coolant system hot leg pressure < { };
2) Reactor coolant system hot leg temperature < { };
3) Reactor coolant system hot leg saturation margin (ΔTsat) and Reactor Pressure Vessel Level (RPVL) consistent with RIS [SIS] in RHR mode suction conditions from the hot leg.

During the reactor coolant system cooldown, to ensure the core sub-criticality, the operator uses RBS [EBS] to compensate the reactivity insertion resulting from the reactor coolant system cooldown. Unaffected Steam Generators (SGu) and MHSI are used to cool the primary at a rate of { } with two or three RBS [EBS] trains or at a rate of { } with one RBS [EBS] train.

When the primary temperature is lower than { }, the last MHSI injection is stopped and the operator prepares to perform final depressurisation via the SGa. Prior to that, the operator shall confirm that the SGa level is lower than the relevant limits. Otherwise, the partner SG shall be isolated, with its level limited to a lower value so that the SGa water inventory can be transferred to the partner SG via the steam generator blowdown system (APG [SGBS]) transfer line. The RIS [SIS] in RHR mode can finally be connected and the safe state is reached.

12.8.5.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [42]. The main assumptions are listed as follows:

a) Single failure

The failure of SGa ASG [EFWS] pump is assumed. This assumption worsens the radioactive release from the SGa as it increases the risk of heat transfer tube exposure.

b) Initial state

The conditions for initial state are chosen to maximise the RCP [RCS] heat to be removed after reactor trip and to assume the SGa tubes are exposed as soon as possible.

c) Core-related Assumptions

The decay heat is considered with an uncertainty of 1.645σ.

d) Loss of offsite power (LOOP)

The LOOP is assumed to occur at the time of turbine trip, considered as a consequence of turbine trip. LOOP leads to the loss of power supply to all Reactor Coolant Pumps (RCP), feed water pumps and condensate pumps. The protection and

safety systems are able to perform the safety functions since these systems can be supplied by Emergency Diesel Generator (EDG). Therefore, the main effect of LOOP is to cause the reactor coolant pumps to coast down.

e) Protection Signals

1) Reactor Trip

Reactor trip is triggered by the “Pressuriser pressure low 2” signal. The maximum positive uncertainty of “Pressuriser pressure low 2” signal is assumed to favour the reactor trip and penalize the steam release. The minimum delay time is taken into consideration to penalize the steam release.

2) Safety Injection

SI is triggered by the “Pressuriser pressure low 3” signal. The “Pressuriser pressure low 3” signal is minimised to penalize the steam release. And the maximum delay time is taken into consideration to penalize the break flowrate.

3) MCD actuation

MCD is initiated by the “SI” signal. The maximum negative uncertainty and the maximum delay time are taken into consideration to penalize the break flowrate.

4) ASG [EFWS] start-up

ASG [EFWS] is actuated either by the “SI and LOOP” signal or by the “SG level (wide range) low 2” signal. The maximum negative uncertainty and the maximum delay time are taken into consideration to penalize the steam release.

5) VDA [ASDS] opening

The VDA [ASDS] isolation valve is opened by “SG pressure high 1”signal. The setpoint is minimised on the SGa and maximised on the unaffected SGs to maximise the steam release from the SGa before the MCD.

f) System Performance

1) ASG [EFWS]

Only two unaffected SGs are fed, since the other ASG [EFWS] pump is lost because of the single failure. After ASG [EFWS] actuation, the SG level in the unaffected SGs is maintained at the reference water level.

The minimum flowrate of ASG [EFWS] is assumed to penalize heat removal.

During the long-term phase, ASG [EFWS] is manually controlled by operator

to maintain the SG level in the two unaffected SGs at their nominal value.

2) MHSI

The maximum MHSI flowrate is chosen to maximise the pressure difference between the reactor coolant system and the SGa.

3) RBS [EBS]

The RBS [EBS] is manually actuated at the beginning of the reactor coolant system cooldown phase (30 minutes after the "high activity in the KRT [PRMS]" signal appeared) to ensure core sub-criticality during the reactor coolant system cooling.

The maximum flowrate is assumed to penalize primary pressure and inventory which maximises the break flowrate.

g) Control Systems

The following FC3 functions are assumed to penalize the radioactivity release:

1) RCV [CVCS]

To maximise the pressure difference between the reactor coolant system and the affected SG, the maximum charging flow rate is assumed.

2) Pressuriser Heaters

The effect of pressuriser heaters is not taken into account to favour the reactor trip and penalize the activity release.

The following FC3 function is not taken into account which could contribute to fault mitigation:

1) Pressuriser sprays

During long term phase, the pressuriser spray could be used to depressurize primary and secondary side. It is not taken into account to penalize radiological consequences.

2) GCT [TBS]

GCT [TBS] is not taken into account to penalize radiological consequences.

h) Other assumptions: operator actions

The first operator action is assumed to be performed at 30 minutes after the "high activity in the VVP KRT [PRMS]" signal. The first local manual operator action is assumed to be performed one hour after this signal.

For long-term mitigation, the operator actions aim at reaching the safe state.

In addition, the impact of operator action to SGTR (one tube) according to the timelines given by human reliability analysis is also evaluated in Reference [42]. The operator actions timelines are based on human reliability analysis. The action timelines in human reliability analysis evaluates the action duration needed by operators. The timelines obtained are different from the assumption in design basis analysis which is a common practice for fault analysis.

12.8.5.2.6 Results and Conclusions

a) Results

The detailed analysis of this fault see Reference [42] shows that the controlled state can be reached after injection of MHSI and the leak elimination can be achieved by operator actions.

The RIS [SIS] in RHR mode connection conditions are met roughly 4 hours after SGTR initiation. In the worst case, the total steam release from VDA of SGa is 109.8 tons, including 90.9 tons released during the short-term phase. Once the RHR is connected, the safe state is reached.

Additional analysis using timelines based on human reliability analysis [43] and penalizing assumptions of the worst case results in a total steam release from VDA of SGa is 111.9 tons, including 93.0 tons released during the short-term phase.

b) Conclusions

As the analysis shows, the reactor can be taken to the safe state.

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed and presented in Sub-section 12.11.4.2.

12.8.5.3 Small Break - Loss of Coolant Accident (State A)

12.8.5.3.1 Description

An SB-LOCA is defined as an accident in which a small break no larger than 5.0 cm equivalent diameter occurs on the pipes of the reactor coolant system or on the upstream line of the second isolation valve connected to it. This accident leads to pressuriser level decrease and primary depressurisation with a possible core heat-up due to lack of cooling. The faults are classified as DBC-3 events.

12.8.5.3.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

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

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

However, if the core remains covered during the transient, above criteria are considered to be met. Thus the consequences of SB-LOCA in state A are analysed against the following aspects:

a) Core remains covered;

b) The plant shall be brought to and maintained in controlled state;

c) The plant shall be brought to and maintained in safe state.

12.8.5.3.3 Main Safety Functions

In this event, FC1 safety functions to achieve controlled state and FC2 safety functions to reach safe state are listed below:

a) FC1 safety functions (automatic)

1) Reactor trip

In state A, if the core power is higher than 10 % Full Power (FP), reactor trip is triggered by the “Pressuriser pressure low 2” signal, and if the core power is no higher than 10 % FP, reactor trip is triggered by the “Hot leg pressure low 1” signal.

2) Turbine trip

The reactor trip signal triggers the turbine trip.

3) Stop of Reactor Coolant Pumps

The Reactor Coolant Pumps (RCP) trip is triggered by the “RCP ΔP low 1 and SI” signal.

4) ARE [MFFCS] full load lines isolation

Following the reactor trip signal, ARE [MFFCS] full load lines of all steam generators are isolated.

5) Safety Injection (SI)

SI is actuated by the “Pressuriser pressure low 3” signal

6) Emergency Feedwater System (ASG [EFWS]) start up

ASG [EFWS] is actuated either by the “LOOP and SI signal” or by the “SG level (wide range) low 2” signal.

7) ASG [EFWS] isolation

ASG [EFWS] in one certain loop is isolated by the “SG level (wide range) high 1” signal of corresponding Steam Generator (SG).

8) Opening of Atmospheric Steam Dump System (VDA [ASDS])

The VDA [ASDS] valves automatically open when the secondary pressure reaches the VDA [ASDS] setpoint.

9) Medium Pressure Rapid Cooldown (MCD)

Following the SI signal, MCD is initiated to cool the primary circuit with a rate of { }.

b) FC2 safety functions (manual from the main control room)

The main operator actions encompass:

1) Reactor coolant system boration

The Emergency Boration System (RBS [EBS]) pumps are started by the operator before the reactor coolant system cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

2) Reactor coolant system cooldown by SGs

The cooldown is performed via the VDA [ASDS] of SGs. The cooling rate is { } with at least two RBS trains in operation and { } if only one RBS train is available.

3) Main Steam Isolation Valve (MSIV) closure

MSIV closure is manually initiated when one SG claimed unavailable. All the main steam lines are then isolated.

4) Reactor coolant system depressurization

During the reactor coolant system depressurization, the accumulators are isolated when the reactor coolant system pressure decreases below 2.0 MPa abs.

The Medium Head Safety Injection (MHSI) pumps are stopped when the reactor coolant system level is sufficient and the hot leg temperature is lower

than { }.

For a very small break, if necessary, reactor coolant depressurization can be achieved by pressuriser spray or opening of the pressuriser safety valves.

Reactor coolant system is then depressurised until the injection pressure of Low Head Safety Injection (LHSI) is reached.

5) Safety Injection System (RIS [SIS]) in Residual Heat Removal (RHR) mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

12.8.5.3.4 Typical Events Sequences

a) From the initiating event to controlled state

Loss of Coolant Accident (LOCA) could lead to a loss of primary coolant inventory and primary depressurization.

The SB-LOCA results in a loss of primary coolant, a potential decrease in reactor coolant system pressure and radioactive release to the environment. This accident may lead to a decrease in reactor coolant inventory and potential core overheating. The SB-LOCA accident is mainly a gravity-driven accident, in which the reactor coolant system discharges slowly with the evident formation of mixing layers throughout the reactor coolant system. These mixing layers change over time, depending on the transient of two phase mass and energy mutual transfer. The first heat-up results from the core level decrease and the formation of a loop seal, and can be mitigated by loop seal clearance during the accident. The second heat-up is due to the boiling and evaporation of the core coolant. During this event, the flow from the MHSI, accumulators and LHSI enter the core and cool the fuel cladding to prevent further temperature increase, and guarantees the core coolant inventory.

Reactor trip is triggered by the “Pressuriser pressure low 2” signal. Following the reactor trip, turbine trip occurs and Main Feedwater Flow Control System (ARE [MFFCS]) full load lines for all SGs are isolated. After reactor trip and turbine trip, the secondary pressure increases rapidly until the setpoint of VDA [ASDS] is reached.

Because of the continuous break flow to the containment and the decrease of decay heat after reactor trip, the SI signal is triggered by the “Pressuriser pressure low 3” signal. Medium Pressure Rapid Cooldown (MCD) is initiated in all SGs following the SI signal. The MCD is carried out by reducing the VDA [ASDS] setpoint, cooling down the reactor coolant system with a rate of { }. When the MCD completes, the secondary pressure is reduced to 6.0 MPa abs. Following the SI signal, the Medium Head Safety Injection (MHSI) and the LHSI pumps are actuated. The Safety Injection System (RIS [SIS]) starts injecting when the reactor coolant system pressure

is below the pump injection head. Then RIS [SIS] injection flow will compensate for the break flow.

After reactor trip and safety injection, the residual heat is mainly removed by the break flow, the RIS [SIS] and the secondary side. The controlled state is achieved when:

1) The primary residual heat can be continuously removed via the break and the plant safety systems including RIS [SIS] and VDA [ASDS];

2) Core sub-criticality is ensured;

3) Core coolant inventory stabilises or increases via the Safety Injection (SI).

b) From controlled state to safe state

The safe state is defined as a state at which the break flow rate is compensated by the RIS [SIS] flow rate with long-term core cooling ensured. The following actions need to be performed (by operators) in order to reach the safe state:

1) Reactor coolant boration

During the reactor coolant system cooldown, to ensure the core sub-criticality, the operator uses RBS [EBS] to compensate the reactivity insertion resulting from the reactor coolant system cooldown.

2) Reactor coolant cooldown

The cooldown, to achieve suitable connecting conditions for the RIS [SIS] in RHR mode, is performed for the units via the secondary side by reducing the VDA [ASDS] setpoint.

3) Primary depressurization

In order to achieve connection conditions of the RIS [SIS] train in RHR mode, the operator stops MHSI pumps to depressurize primary circuit.

4) Connection of RIS [SIS] in RHR mode.

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

12.8.5.3.5 Analysis Assumptions

The detailed assumptions are presented in Reference [44].The main assumptions are listed as follows:

a) Initial conditions

1) Initial reactor power is the nominal power plus the maximum uncertainty. The higher initial thermal power, the more the residual heat will be generated

during the transient;

2) The initial coolant flow rate is the thermal-hydraulic design flow rate, which is considered to penalize heat removal;

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

4) The initial pressure of the pressuriser is the rated value plus the maximum uncertainty. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant;

5) The initial level of the pressuriser is the rated level at power minus 7% based on uncertainties. Because the less the initial primary inventory, the less core inventory after the break occurs;

6) The total core bypass flow rate takes the maximum value (6.5%) to minimise the flow rate passing through the core.

b) Core-related assumptions

In the short term analysis, Term A is calculated based on the specific neutronic data by LOCUST-K. The decay heat of actinides and fission products in Term B+C, given by LOCUST-K, meets the requirements in the Appendix K of 10 CFR 50, in which the decay heat of fission products is assumed to be 1.2 times of the value for infinite operating time in the ANS standard (October 1971).

In the long term analysis, the decay heat is considered with an uncertainty of 2σ.

c) LOOP assumption

Loss of Offsite Power (LOOP) is assumed to occur at the time of turbine trip, considered as a consequential event of turbine trip. LOOP leads to the loss of power supply to all reactor coolant system pumps, feedwater pumps and condensate pumps. The protection and safety systems are able to perform the safety functions since these systems can be supplied by Emergency Diesel Generator (EDG). Therefore, the main effects of LOOP are coasting down of RCPs and delay of safety systems.

d) Single failure

It is assumed that the single failure occurs on the EDG because one RIS [SIS] train (one MHSI pump and one LHSI pump), one RBS [EBS] train and ASG [EFWS] for one unaffected loop are unavailable. This assumption penalizes the water inventory and heat removal for primary side. It penalizes core heat-up and makes the primary side cool down slower.

12.8.5.3.6 Results and Conclusions

a) From the initiating event to the controlled state

The detailed analysis of this fault (see Reference [44]) shows that for the break conditions with the equivalent diameters of 2.5 cm and 5.0 cm, the SI system is able to provide sufficient flow to keep the core covered and continuously cooled. The relevant safety acceptance criteria are thus met.

b) From the controlled state to the safe state

After the controlled state, the RHR connecting condition is reached through the primary boration, cooling and depressurisation with at least one LHSI train in RIS [SIS] mode and at least one LHSI train in RHR mode, which brings the reactor to a safe state.

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed and presented in Sub-section 12.11.4.3.

12.8.5.4 Uncontrolled RCP [RCS] Level Drop

12.8.5.4.1 Description

During normal shutdown operation, the cooling of the plant is performed by the RIS [SIS] in RHR mode. When the RCP [RCS] temperature is comprised between 140℃ and 100℃(State C1), the RIS [SIS] train A and train B are used in RHR mode. When the RCP [RCS] temperature is below 60℃, the RCP [RCS] loop level can be lowered to ¾ loop. The corresponding reactor states are C3 (RCP [RCS] partially open, rapidly re-closable) or D (RCP [RCS] open). This event reduces the RCP [RCS] water level which may lead to the trip of the RIS [SIS]\RHR pumps by the “RCP [RCS] loop level low 2” signal. Therefore, the RCP [RCS] cooling may not be ensured.

An uncontrolled RCP [RCS] level drop in a shutdown state with the RIS [SIS] connected in RHR mode may be caused by:

a) The abnormality of seal injection function of RCV [CVCS];

b) The abnormality of high pressure letdown function of RCV [CVCS];

c) The abnormality of low pressure letdown function of RCV [CVCS];

d) The abnormality of charging function of RCV [CVCS].

From State C, the residual heat is removed by RIS [SIS] in RHR mode. Because the RCP [RCS] is pressurisable in State C1\C2, if the RIS [SIS]\RHR pumps are not available, the residual heat removal can be ensured by steam generators. The reactor cavity is flooded in State E, thus the change of RCP [RCS] level is slow and monitored. The RCP [RCS] loop level can be lowered to ¾ loop in State C3\D. With respect to the disturbances of the heat removal, the plant conditions with lowered RCP [RCS] level, i.e. ¾ loop operations, are the most penalizing conditions because the RCP [RCS] water inventory is small. Therefore, the accidental phenomena and

consequences of uncontrolled RCP [RCS] level in State C\D\E can be enveloped by those in State C3\D. Thus the chosen case for the fault analysis is an excessive discharge by the letdown line due to a malfunction of the RCV [CVCS] low pressure reducing station valve in State C3\D.

12.8.5.4.2 Acceptance Criteria

This accident is considered as a DBC-3 event. The acceptance criteria to be considered for this event are:

a) Core water inventory is stable;

b) Residual heat removal is ensured on a long term basis.

Both criteria are verified if the RIS [SIS]\RHR pumps are maintained in operation.

12.8.5.4.3 Main Safety Functions

The reactor is protected by the following mitigation actions (FC1):

a) The SI is actuated on an “RCP [RCS] loop level low 1” signal.

b) Isolation of the RCV [CVCS] letdown line is initiated by the SI signal.

12.8.5.4.4 Typical Events Sequences

The transient of this event can be divided into two phases: the short-term phase to the controlled state and the long-term phase to the safe state. A typical sequence of events is described hereafter.

a) From the initiating event to the controlled state

After a malfunction of the RCV [CVCS] low pressure reducing station valve, the primary water is discharged by the letdown line. The water level starts to drop. The SI signal is triggered when the water level reach the “RCP [RCS] loop level low 1” threshold. The MHSI pumps are started and the RCV [CVCS] letdown line is isolated.

b) From the controlled state to the safe state

The RIS [SIS]\RHR trains initially in service remain in operation during the transient, which allows keeping the power removal in the same conditions as before the accident.

12.8.5.4.5 Analysis Assumptions

The detailed assumptions are presented in Reference [45]. The main assumptions are listed as follows:

a) The initiating event is the primary coolant level begins to drop due to the drain of primary water through the letdown line of the RCV [CVCS].

b) The maximum RCV [CVCS] letdown flowrate is used.

c) The primary average coolant temperature is considered as its maximum value.

d) The single failure is applied on one MHSI pump as it penalises the SI flowrate.

12.8.5.4.6 Results and Conclusions

The detailed analysis of this fault [45] shows that the primary water inventory can be restored and the RIS [SIS]\RHR pumps are maintained in operation.

Thus the acceptance criteria for this event are met.

In this accident, there is no radioactivity release to the environment and the RPT-4 BSO is met.

12.8.5.5 Inadvertent Opening of one Pressuriser Safety Valve (State B\C)

This event may be caused by spurious activation of PSV when PZR is under operation.

Since the core power and coolant temperature at full power level in State A are higher than that in State B\C, the consequence of inadvertent opening of a pressuriser safety valve in State B\C is covered by that in State A, in Sub-chapter 12.7.6.2.

12.8.6 Fuel Pool Accidents

12.8.6.1 LOOP (>2 hours) Affecting Fuel Pool Cooling

12.8.6.1.1 Initiating Event

LOOP leads to the loss of electrical supply for all plant auxiliary systems including all pumps and the supporting systems of PTR [FPCTS] trains which provide cooling for the SFP. As the SFP temporarily loses cooling, the temperature, and the risks associated, may increase. An analysis is performed to demonstrate that cooling of SFP can be recovered and that safe state of SFP is ensured.

In this section, DBC-3 accident “LOOP (>2 hours) Affecting Fuel Pool Cooling (State A-F)” is analysed from the perspective of SFP cooling aspects.

In the short term (<2 hours) Loop accident, the controlled and safety shutdown state can be considered as reached from the initial time because of the long grace period before spent fuel exposure.

Under plant normal operation condition (State A-D), there is one PTR[FPCTS] train (train A or train B) in operation, the other two PTR [FPCTS] trains are in backup. Since the decay heat of spent fuel pool in state A can bound that of state B-D, which is more onerous for spent fuel pool cooling than state B to D, only analysis to state A is carried out.

Under normal refuelling condition (State E) and abnormal condition (State F), two PTR [FPCTS] cooling trains are used to cool the SFP, the other one PTR [FPCTS] train is in backup.

12.8.6.1.2 Acceptance Criteria

The safety criteria for the DBC accidents associated with spent fuel storage pool are as follows:

a) Permanent maintenance of sub-criticality;

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

12.8.6.1.3 Main Safety functions

In case of “LOOP (>2 hours) Affecting Fuel Pool Cooling” event, following safety function is designed to remove the decay heat of spent fuel pool:

a) PTR [FPCTS]

Three independent PTR [FPCTS] trains (A/B/C) are designed to remove decay heat from the SFP.

In case of a LOOP event, Emergency Diesel Generator (EDG) is triggered by the signal of “LOOP” to provide electric supporting for the performance of PTR [FPCTS]

cooling train. Each PTR [FPCTS] pump can be powered by EDG.

b) Secondary Passive Heat Removal System (ASP [SPHRS])

ASP [SPHRS] provide water makeup to SFP.

12.8.6.1.4 Typical Events Sequence

a) Accident happened in State A

In state A, one PTR [FPCTS] train is in operation. According to the PTR [FPCTS] EMIT window in Reference [46], one PTR [FPCTS] train may be under maintenance. One PTR [FPCTS] train is considered to be lost due to single failure. In case of LOOP, all PTR [FPCTS] trains are lost and SFP water temperature increases until EDGs are started up.

Once the EDGs are started up, there is one PTR [FPCTS] train which is available to provide cooling for SFP. Powered by the EDG, cooling for SFP is recovered, the temperature increase is stopped and safety is ensured.

b) Accident happened in State E

For accident happened in state E, one PTR[FPCTS] cooling train is considered as unavailable due to single failure. There is no EMIT (induce PTR [FPCTS] unavailable) to PTR [FPCTS] train or its supporting system in state E referred to Reference [46].

Once the EDGs are started up, there is at least one PTR [FPCTS] train available to provide cooling for SFP. Powered by the EDG, cooling for SFP is recovered, the temperature increase is stopped and safety is ensured.

c) Accident happened in State F

For accident happened in state F, two EDGs may be under maintenance at the same time in state F. Considering the most pessimistic SFC, one PTR cooling train is considered as unavailable, which can be caused by either one PTR pump failure or failure of start-up of one EDG. In case of LOOP, under the most onerous condition in state F, all PTR [FPCTS] trains will be lost and no EDG can be used for SFP cooling. As the SFP cooling is failed, it leads to the increase of SFP water temperature. The ASP [SPHRS] will provide water makeup to the SFP and compensate for mass losses due to boiling.

12.8.6.1.5 Analysis Assumptions

Conservative assumptions are adopted in the analysis as follows:

a) The decay heat of the SFP in state A, state E and state F are conservatively assumed. The decay heat of the fuel assemblies in state A at Begin of Cycle (BOC) is assumed, which is the maximum for this state.

b) The initial SFP water temperature is conservatively considered as 50℃.

c) The initial water volume of the SFP is 1265.8 m^3 corresponding to a water level of 16.9m at normal operation.

d) The SFP and the PTR [FPCTS] pipes are considered as adiabatic.

e) Water heating is only localised in the SFP compartment, and the water is heated homogeneously in this area.

f) Once the SFP cooling system is recovered, a maximum RRI [CCWS] inlet temperature of 45℃ is used.

g) EDGs are started up 1 hour after the accident, which is a very conservative assumption compared to expected plant response.

h) The most pessimistic Single Failure Criterion (SFC), one PTR cooling train is considered as unavailable in the analysis, which can be caused by either one PTR pump failure or failure of start-up of one EDG.

12.8.6.1.6 Results and Conclusions

The detailed result is presented in the Reference [47]. For accident happened in state A and state E, the SFP water temperature increases at first and then stabilized at 56.4℃, 58.4℃, respectively. For accident happened in state F, the decay heat is removed efficiently by the ASP [SPHRS] water makeup and evaporation mode. The fuel assemblies remain covered during the entire transient. Sub-criticality can be ensured by the design of the storage rack which is analysed in detail in Reference [48].

All acceptance criteria are met for this accident.

In terms of radiological consequence, since there is no risk for departure from nucleate boiling and spent fuel integrity failure, very limited radionuclides are released to the environment through steam evaporation after SFP boiling. As a result, the radiological consequences are very limited both on the site and off the site.

12.8.6.2 Loss of One PTR [FPCTS] Train (State E\F)

12.8.6.2.1 Initiating Event

During refuelling, two PTR [FPCTS] cooling trains are operating to maintain cooling of the SFP, into which fuel assemblies are unloaded from the reactor vessel. If one operating cooling train of the PTR [FPCTS] is lost, caused by failure of the pump or heat exchanger for example, SFP temperature may increase. Therefore, an analysis has been performed to demonstrate that SFP cooling can be recovered and the safe state of SFP can be ensured.

12.8.6.2.2 Acceptance Criteria

The safety criteria for the DBC accidents associated with spent fuel storage pool are as follows:

a) Permanent maintenance of sub-criticality;

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

12.8.6.2.3 Main Safety functions

Three independent PTR [FPCTS] trains (A/B/C) are designed to remove decay heat from the SFP.

12.8.6.2.4 Typical Events Sequence

Under the most penalizing case, cooling train A of the PTR [FPCTS] is lost as the initial event and cooling train B is also lost due to the maintenance to the PTR [FPCTS] supporting systems. PTR train C, is already in service, remains available for SFP cooling.

12.8.6.2.5 Analysis Assumptions

The main assumptions adopted in the analysis are listed as follows:

a) The maximum decay heat of the SFP for the last fuel assemblies unloaded into the SFP in state F is taken into account;

b) The initial water temperature of the SFP is assumed to be 50℃, which covers all the normal operating conditions;

c) The initial water volume of SFP is 1265.8m^3 corresponding to a water level of 16.9m;

d) The SFP and the PTR [FPCTS] pipes are considered as adiabatic;

e) Water heating is only localized in the SFP compartment, and the water is heated homogeneously in this area;

f) Once the SFP cooling system has been recovered, a maximum RRI [CCWS] inlet

temperature of 45℃ is used;

g) The most pessimistic Single Failure Criterion (SFC), one PTR cooling train is unavailable, is considered in the analysis.

However, it should be noted that, if one train of PTR or of its supporting system is under maintenance in the initial state, SFC is not considered. Since the third backup PTR [FPCTS] train shall be started up first before the maintenance to one PTR [FPCTS] train, there is no requirement for change of state for the PTR [FPCTS].

12.8.6.2.6 Results and Conclusions

The detailed analysis is presented in the Reference [49]. The analysis demonstrated that when cooled by PTR [FPCTS] train C, the SFP water temperature increases at first and then stabilised below 80℃. The fuel assemblies remain covered during the entire transient and the sub-criticality of fuel assemblies is ensured by the design of the storage rack which is analysed in detail in Reference [48].

All acceptance criteria are met for this accident.

In terms of radiological consequence, since no boiling occurs in the accident and fuel assemblies are always covered in the SFP, there is no radioactivity release.

12.8.6.3 Isolatable Piping Failure on a System Connected to Spent Fuel Pool (State A to F)

12.8.6.3.1 Initiating Event

Isolatable piping failure on a system connected to the spent fuel pool could happen in all states. The break may occur on a purification line, a skimming line, a water makeup line or a PTR [FPCTS] cooling train. To maximize the temperature increase of the spent fuel pool, the break is assumed to be located downstream of the second isolation valve of a PTR [FPCTS] train. The break leads to the drainage of the SFP and connected compartment. In state A-D, one of the PTR [FPCTS] cooling trains is used to cool the spent fuel pool. Since the decay heat of SFP in state A can bound that of state B-D, which is more onerous for SFP cooling than state B to D, only analysis to state A is carried out. In states E and F, two PTR [FPCTS] cooling trains are used to cool the pool.

12.8.6.3.2 Acceptance Criteria

The safety criteria for DBC accidents associated with the spent fuel storage pool are as follows:

a) Permanent maintenance of sub-criticality;

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

12.8.6.3.3 Main Safety functions

For this event, the following plant safety functions can mitigate the event:

a) Three independent PTR [FPCTS] trains (A/B/C) are designed to remove decay heat from the SFP;

b) Isolation of the PTR [FPCTS] trains following the signal “Spent fuel pool water level low 4”;

c) Secondary Passive Heat Removal System ASP [SPHRS] tank provide water makeup to SFP.

12.8.6.3.4 Typical Events Sequence

a) For accident happened in State A and State F:

A break in the PTR [FPCTS] train leads to the drainage of the SFP. The break is assumed to be located downstream of the second isolation valve of PTR [FPCTS] train A. When the water level drops to “low-level L4” (+16.0m), the isolation signal of the PTR [FPCTS] trains is triggered. 80 seconds later (signal time delay and time for valve isolation action), the PTR [FPCTS] trains are isolated. The result shows that the water level is stabilised at 15.89m. Considering the PTR[FPCTS] train A failed due to initiating event, PTR[FPCTS] train B failed due to maintenance, and

PTR[FPCTS] train C failed due to SFC, all cooling trains are lost. The SFP water temperature continues to increase. Then, the saturation temperature is reached and the SFP begins to boil. The SFP water begins to evaporate continuously. ASP [SPHRS] water makeup is required to fill the SFP. The decay heat of SFP is removed by the water makeup and evaporation mode in the long term. In order to avoid the over-pressure of fuel building, the damper and rupture disc in the fuel building are used to control the fuel building pressure.

b) For accident happened in State E:

A break in the PTR [FPCTS] train leads to the drainage of the SFP. The break is assumed to be located downstream of the second isolation valve of PTR [FPCTS] train A. When the water level drops to “low-level L4” (+16.0m), the isolation signal of the PTR [FPCTS] trains is triggered. 80 seconds later (signal time delay and time for valve isolation action), the PTR [FPCTS] trains are isolated. The result shows that the water level is stabilised at 15.89m. PTR [FPCTS] train B is considered to be unavailable for SFC. Since there is no maintenance on PTR [FPCTS] cooling trains and its supporting systems, one PTR [FPCTS] cooling train C is available.

12.8.6.3.5 Analysis Assumptions

Main assumptions adopted in the analysis are listed as follows:

a) The decay heat of the SFP in state A, state E and state F are conservatively assumed as 5.32MW, 12.53MW, 15.29MW, respectively. The decay heat of the fuel assemblies in state A at Begin of Cycle (BOC) is assumed, which is the maximum for this state.

b) The break is conservatively assumed to be located in the lowest position of the PTR train, to maximize the break flowrate.

c) The initial SFP water temperature is assumed to be 50℃, which covers all the normal operating conditions.

d) The initial water volume of the SFP is 1265.8m^3 corresponding to a water level of 16.9m.

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

f) The water heating is only localized in the SFP compartment, and the water is heated homogeneously in this area.

g) The most pessimistic Single Failure Criterion (SFC), one PTR [FPCTS] cooling train is unavailable, is considered in the analysis.

h) The isolation signal of the PTR [FPCTS] train will be triggered when the water level of the SFP drops to “low-level L4” (+16.0m).

i) 80s is considered for the isolation signal time delay and valve isolation action.

j) One cooling train of the PTR [FPCTS] is considered to be unavailable for its preventive maintenance in state A, and for maintenance to its supporting system in state F. There is no maintenance to PTR [FPCTS] cooling trains and its supporting systems in state E.

12.8.6.3.6 Results and Conclusions

The detailed analysis is presented in the Reference [50]. The decay heat is removed efficiently by the water makeup in evaporation mode in state A and F or one PTR[FPCTS] cooling train in state E. The fuel assemblies in the SFP remain covered during the entire transient in all states. The sub-criticality of the fuel assemblies is ensured by the design of spent fuel storage rack which is analysed in detail in Reference [48].

All acceptance criteria are met in this accident.

In terms of radiological consequence, since there is no risk for departure from nucleate boiling and spent fuel integrity failure, very limited radionuclides are released to the environment through steam evaporation after SFP boiling. As a result, the radiological consequences are very limited both on the site and off the site.

12.8.7 Radiological Release of Systems or Components

12.8.7.1 Volume Control Tank Break (State A to F)

Leakage of or damage to the RCV [CVCS] tank will cause leakage of untreated primary coolant which may cause radioactivity release to the environment. The analysis in terms of source terms and radiological consequences is provided in Sub-chapter 12.11.4.5.

12.8.8 Loss of Support Systems

12.8.8.1 Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinets Rooms of Safeguard Building Division B (State A\B)

12.8.8.1.1 Description

This event is the representative of the event below which causes similar transient impact on the reactor core (Reference [100]):

a) Loss of LHB [EPDS(NI-10kV)].

This event leads to loss of main feedwater superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]) and loss of RCP [RCS] pumps (i.e. pump shutdown). Besides, the additional impact on other key safety functions is loss of division B and channel II, which means that one train safety functions fail altogether, i.e. loss of ASG [EFWS] train B, loss of RBS [EBS] train B, loss of MHSI train B, loss of LHSI train B, loss of RIS-RHR train B, loss of VDA [ASDS] train B, loss of I&C division B and channel II, etc. This event may occur in

State A and B.

The loss of main feedwater results in decrease in heat removal by the secondary system and increase in primary coolant temperature, which may lead to the risk of DNB.

The increase in charging flow or decrease in letdown flow due to control failure of RCV [CVCS] results in increase in primary coolant inventory, pressuriser pressure and level.

The decrease in charging flow or increase in letdown flow due to control failure of RCV [CVCS] results in decrease in primary coolant inventory and inadequate core cooling, which may lead to the risk of DNB.

The loss of RCP [RCS] pumps results in decrease of reactor coolant flow and capacity to remove the core heat, which may lead to the risk of DNB.

The bounding case for analysis of this event is at full power level.

The following DBC-2 events cause similar transient impact on the reactor core:

a) Short Term LOOP of 2 Hours Duration (Sub-chapter 12.7.2.2) which causes coastdown of RCP [RCS] pumps and trip of the condensate pumps and main feedwater pumps;

b) Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sub-chapter 12.7.5.1);

c) Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sub-chapter 12.7.6.1).

12.8.8.1.2 Acceptance Criteria

The loss of DVL [EDSBVS] ventilation in switchgear and I&C cabinets rooms of Safeguard Building Division B (state A\B) is classified as a DBC-3 event. The following acceptance criteria are used for DBC-3 events:

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

b) The peak cladding temperature must remain less than 1482℃;

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

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied as follows:

a) The minimum DNBR shall be greater than { };

b) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

12.8.8.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions (FC1) are required:

a) Reactor trip is actuated by the “Low RCP [RCS] pump speed” signal, “SG level (narrow range) low 1” signal, “Pressuriser level high 1” signal or “Pressuriser level low 2” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

d) The VDA [ASDS] is actuated by the “SG pressure high 1” signal;

e) The PSVs are opened when the pressuriser pressure reaches the setpoint;

f) The RCV [CVCS] charging line is isolated following the “Pressuriser level high 1” signal;

g) The seal water injection for RCP [RCS] pumps is isolated on “Pressuriser level high 2” signal;

h) The RCV [CVCS] letdown line is isolated by “Pressuriser level low 1” and reactor trip signals.

In order to reach the safe state, the following manual safety functions (FC2) are required:

a) Startup of ASG [EFWS];

b) Startup/Isolation of RBS [EBS];

c) Startup of cooldown via VDA [ASDS];

d) RCP [RCS] depressurisation;

e) Accumulators isolation;

f) Connection of RIS [SIS] in RHR mode.

12.8.8.1.4 Typical Events Sequences

a) From the Initiating Event to the Controlled State

Although this event leads to multiple transient impact, it is estimated that the impact of loss of RCP [RCS] pumps is quicker than that of loss of main feedwater or increase/decrease in RCV [CVCS] flow. Therefore, it is anticipated that reactor trip is automatically triggered by the earlier signal of “Low RCP [RCS] pump speed”, and thus leading to turbine trip.

After reactor trip, the PSVs may open to limit the increase of primary pressure since

the normal spray is unavailable. The secondary pressure is limited by the VDA [ASDS] if the GCT [TBS] is unavailable. The ASG [EFWS] is automatically actuated by "SG level (wide range) low 2" signal to compensate for the secondary side inventory.

The RCV [CVCS] charging line, seal injection line and letdown line are automatically isolated if the corresponding signals are actuated.

Finally, the controlled state is reached. The core residual heat is removed by the VDA [ASDS] and the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration is performed via the chemical and volume control system RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit uses the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS] train. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation is performed by the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.8.8.1.5 Results and Conclusions

Compared with short term LOOP of 2 hours duration event (Sub-chapter 12.7.2.2), the reactor trip time of increase/decrease in RCV [CVCS] flow event (Sub-chapter 12.7.5.1 and 12.7.6.1) is later and the variation of primary coolant temperature and flow is less significant. Hence, there are reasons to believe that the transient evolution of loss of DVL [EDSBVS] ventilation in switchgear and I&C cabinets rooms of Safeguard Building Division B (state A\B) event before reactor trip is similar to that of short term LOOP of 2 hours duration event (Sub-chapter 12.7.2.2). Considering the DNBR margins shown in Sub-chapter 12.7.2.2, 12.7.5.1 and 12.7.6.1, it is justified that the DNBR limit will not be exceeded for the event concerned. The limit of fuel pellet temperature and cladding temperature are not challenged since the core power is limited and no DNB occurs. Therefore, all the acceptance criteria are met.

Because the main safety functions claimed in Sub-chapter 12.7.2.2, 12.7.5.1 and 12.7.6.1 are very similar to and still available for the event concerned, it is justified

that the controlled state and safe state can be reached.

The radiological consequence can be represented by the “Turbine Trip” fault, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sup-chapter 12.11.4.1.

12.8.8.2 Loss of RRI [CCWS] or SEC [ESWS] Train A (State C\D\E)

12.8.8.2.1 Description

This event is the representative of the following events which cause similar transient impact on the reactor core (Reference [100]):

a) Loss of LHA [EPDS(NI-10kV)];

b) Loss of LHB [EPDS(NI-10kV)];

c) Loss of NI 690V SBO Power Distribution System (LJA/LJU [SBOPDS(NI-690V)]).

This event leads to loss of one RIS-RHR train in operation (train A assumed) superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]). Besides, the additional impact on other key safety functions is loss of MHSI train A and loss of LHSI train A. This event may occur in State C, D and E.

The loss of one RIS-RHR train in operation results in increase of primary coolant temperature and reduction of the capacity of heat removal, which may lead to the risk of core uncovery.

The increase in charging flow or decrease in letdown flow due to control failure of RCV [CVCS] results in increase in primary coolant inventory, pressuriser pressure and level.

The decrease in charging flow or increase in letdown flow due to control failure of RCV [CVCS] results in decrease in RCP [RCS] level and may lead to trip of the RIS-RHR pumps by the “RCP [RCS] loop level low 2” signal, which may challenge the core cooling.

The bounding case for analysis of this event is in State C1, C3 or D.

The following DBC-2 and DBC-3 events cause similar transient impact on the reactor core:

a) Loss of One RIS [SIS] Train in RHR Mode (Sub-chapter 12.7.2.5);

b) Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sub-chapter

12.7.5.1);

c) Uncontrolled RCP [RCS] Level Drop (Sub-chapter 12.8.5.4).

12.8.8.2.2 Acceptance Criteria

This accident is considered as a DBC-3 event. The acceptance criteria to be considered for this event are:

a) Core water inventory is stable;

b) Residual heat removal is ensured on a long term basis.

Both criteria are verified if the RIS [SIS]\RHR pumps are maintained in operation.

12.8.8.2.3 Main Safety Functions

In this event, the following main safety functions (FC2) are required:

a) SI is actuated on “RCP [RCS] loop level low 1” signal;

b) Isolation of the RCV [CVCS] letdown line is initiated by the SI signal.

c) The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.8.8.2.4 Typical Events Sequences

Although this event leads to multiple transient impact, it is estimated that the main impact is increase of primary coolant temperature and reduction of the capacity to remove core heat caused by loss of one RIS-RHR train in operation, which may lead to the risk of core uncovery. Moreover, decrease in RCP [RCS] level due to control failure of RCV [CVCS] may aggravate the consequence.

If primary coolant temperature attains the saturation temperature, the RCP [RCS] level drops following the evaporation of primary coolant. The MHSI is actuated by the “RCP [RCS] loop level low 1” signal and RCV [CVCS] letdown line is isolated subsequently. Then the primary coolant inventory is compensated and the RCP [RCS] level is restored.

In the long term, heat removal is ensured by the unaffected RIS [SIS] train, the reactor reaches the safe state.

12.8.8.2.5 Results and Conclusions

Compared with loss of one RIS [SIS] train in RHR mode (Sub-chapter 12.7.2.5) and uncontrolled RCP [RCS] level drop (Sub-chapter 12.8.5.4), the initiating event, transient evolution and consequence of loss of RRI [CCWS] or SEC [ESWS] train A (State C\D\E) event are similar but not worse. Considering the margins of analysis results shown in Sub-chapter 12.7.2.5, 12.7.5.1 and 12.8.5.4, it is justified that there is no core uncovery and the core heat removal is ensured for long term for the event

concerned. Therefore, all the acceptance criteria are met.

In this accident, there is no radioactivity release to the environment and the RPT-4 BSO is met.

12.9 Analyses of DBC-4 Events

This sub-chapter describes the analysis of DBC-4 events that are not expected to occur but are postulated because their consequences could include the potential release of significant amounts of radioactive materials. They are the most extreme conditions which must be considered in the design and represent limiting cases.

12.9.1 Increase in Heat Removal by the Secondary Side

12.9.1.1 Steam System Piping Large Break

12.9.1.1.1 Description

The steam system piping large break might be caused by the break of steam systems and its connecting lines at the initial time. The steam system piping break induces an initial increase in the steam flow which then decreases during the accident as the steam pressure falls.

The energy removed from the RCP [RCS] increases, causing decreases in RCP [RCS] coolant temperature and pressure, which lead to the core overcooling and an insertion of positive reactivity caused by a negative moderator temperature coefficient. The increase of reactivity in the core induces a rise in nuclear power at power operation or results in a return to criticality during zero power condition.

The studied cases at present consist of the double-ended guillotine break and small breaks of the main steam line (MSL). If the break locates at the upstream of MSIV, the break is non-isolatable and it will strengthen the overcooling effect.

The steam system piping large break is considered in state A and state B. The consequences of this fault in State B can be enveloped by analysis in State A since the initial sub-criticality margin and the initial boron concentration are higher in state B, which weakens the moderator effect. Therefore, the quantitative analysis for this fault is performed only in State A.

To evaluate the impact of the initial reactor power, two states is analysis in this chapter:

a) Steam system piping large break occurs at zero power;

b) Steam system piping large break occurs at full power.

12.9.1.1.2 Acceptance Criteria

The steam system piping large break accident is classified as a DBC-4 event. The following acceptance criteria are used for DBC-4:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.9.1.1.3 Steam System Piping Large Break at Zero Power

12.9.1.1.3.1 Main Safety Functions

In order to reach the controlled state, the following FC1 main safety functions are required:

a) Reactor trip is actuated by any of the following signals:

   1) Pressuriser pressure low 2;

   2) Pressure drop of SG high 0;

   3) Pressure drop of SG high l.

b) Isolations of the full load main feedwater lines on all SGs are actuated on receipt of reactor trip signal;

c) Isolation of the low load main feedwater line on corresponding SG is actuated on "SG pressure low 2" signal; Isolations of the low load main feedwater line on all SGs are actuated on "Pressure drop of SG high 2";

d) Isolations of the main steam line on all SGs are actuated on "SG pressure low 1" signal or "Pressure drop of SG high 1" signal;

e) Safety injection is triggered by the "Pressuriser pressure low 3" signal;

f) ASG [EFWS] is actuated by the "SG level (wide range) low 2" signal;

g) Manual isolation of ASG [EFWS] of affected SG.

In order to reach the safe state, the following FC2 manual safety functions are required:

a) Affected SG isolation

The affected SG is isolated manually to prevent the core overcooling and to limit the mass and energy release inside containment.

b) Startup of ASG [EFWS]

If the ASG [EFWS] for the unaffected SGs are not actuated automatically, the operator will start the ASG [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASG [EFWS].

c) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

d) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

e) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

f) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

g) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.9.1.1.3.2 Typical Events Sequences

A typical events sequence, during which automatic actions and manual actions are presented, can be divided into the following two stages:

a) From initiating event to controlled state

Initially, the fault leads to the secondary side depressurisation. Reactor trip is tripped by “Pressuriser pressure low 2”, “Pressure drop of SG high 0” or “Pressure drop of SG high l”. The closure of all MSIVs are triggered by the “SG pressure low 1” or “Pressure drop of SG high 1” signals, and ARE [MFFCS] full load lines for all SGs are isolated by reactor trip signal. ARE [MFFCS] low load line may also be isolated by the “Pressure drop of SG high 2” or “SG pressure low 2” signals. The “Pressuriser pressure low 3” signal would trigger the safety injection (RIS [SIS]). After the ARE [MFFCS] low load lines have been isolated, the “SG level (wide range) low 2” signal should initiate the ASG [EFWS] for the affected SG.

The RCP [RCS] cooldown induces positive reactivity in the core, and the reactor may return to criticality. However, the Doppler effect may limit the power excursion.

The RIS [SIS] supplies sufficient boron to compensate the reactivity insertion, bringing and maintaining the core sub-critical.

Thereafter, when the affected SG is empty and the heat removal is ensured by the VDA [ASDS] and ASG [EFWS] of the unaffected SGs, the controlled state is reached.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, the affected SG will be isolated as the first operator action. After that, operators perform primary cooldown and

depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.9.1.1.3.3 Analysis Assumptions

The detailed assumptions are presented in Reference [51]. The main assumptions are listed as follows:

a) Initial Conditions

The initial condition is assumed as a zero power state. In order to fully study the consequence of this event and find the most pessimistic case, the break spectrum is analysed ranged from DN50 (corresponding to nominal diameter 50 mm) to double ended guillotine break. Considering the impact of the SG outlet flowrate limiter (corresponding to nominal diameter 407mm), the transient response for the break greater than DN407 is the same with that for DN407.

1) The initial operating power is 0%FP;

2) Initial reactor coolant average temperature is nominal value;

3) Initial pressuriser pressure is nominal value;

4) The initial reactor coolant Flowrate is set as the thermal design flow (24000m³/h per loop), considering that 0% of the SG tubes are plugged;

5) The RCCA with the highest worth is assumed to be stuck out of the core to minimise the negative reactivity insertion;

6) The heat transferred from two unaffected SGs to the reactor coolant (i.e., SG reversed heat transfer) is not considered, so as to penalize the reactor coolant overcooling;

7) Both main feedwater flow (nominal flow rate of full power) and the emergency feedwater flow are injected to all three steam generators from the beginning of the accident until the complete main feedwater isolation. Afterward, the emergency feedwater flow rate is considered as the maximum flow rate.

b) Core Related Assumptions

The calculation on the specific neutronic data is conducted for all fuel cycles in the fuel management scheme and envelopes all rod-stuck conditions.

1) Moderator density coefficient

The moderator density coefficients are calculated with consideration of different boron concentrations and moderator densities (boron concentrations (35% enrichment ^{10}B): 0 ppm, 279 ppm, 558 ppm; moderator densities: 0.75 g/cm^3, 0.80 g/cm^3, 0.85 g/cm^3, 0.90 g/cm^3, 0.95 g/cm^3).

The moderator density coefficient is set to the maximum absolute value to maximize insertion of positive reactivity due to decrease in coolant temperature.

2) Boron differential worth

The boron differential worth for combinations of different boron concentrations and moderator densities (boron concentrations (35% enrichment ^{10}B): 0 ppm, 279 ppm, 558 ppm; moderator densities: 0.75 g/cm^3, 0.80 g/cm^3, 0.85 g/cm^3, 0.90 g/cm^3, 0.95 g/cm^3) is calculated.

The boron differential worth is set to the minimum absolute value to minimize insertion of negative reactivity due to boron injection.

3) Doppler power defect

The Doppler power defect, tending to slowdown the nuclear power increase, is set to the minimum value to maximize the core power.

Depending on the results of Doppler power defect for all fuel cycles and all rod-stuck conditions and in order to meet the tougher DNBR design limit, two sets of envelope values are considered for double-ended guillotine break:

Case A - with a Doppler power defect of 1167 pcm at 20%FP, which covers all the cycles and stuck rods conditions resulting in a Doppler power defect between 1167 pcm and 1699 pcm at 20%FP.

Case B - with a Doppler power defect of 1699 pcm at 20%FP, which covers all the cycles and stuck rods conditions resulting in a Doppler power defect higher than 1699 pcm at 20%FP.

For other break sizes, one set of bounding values covering all fuel cycles and all stuck rods conditions is considered: the Doppler power defect is more than 1167 pcm at the power level of 20% FP. This assumption is very conservative.

4) Shutdown margin

The shutdown margin is set to the minimum value to maximize the core power.

c) LOOP Assumption

If the LOOP is assumed at the time of turbine trip, it will lead to the trip of the main feedwater and reactor coolant pumps. The decrease of reactor coolant flowrate and feedwater flowrate reduces the core overcooling which leads to a less reactivity insertion compared to the case without LOOP. So the power production is much lower than the case without LOOP. Even though the MHSI is delayed longer when LOOP occurs, it has little effect on peak thermal power. As a result, only the most penalizing case, corresponding to without LOOP configuration, is studied.

d) Single Failure

The single failure is considered as the failure of one train of medium head safety injection [MHSI] at present, as the MHSI would be actuated after the primary pressure decreased to the MHSI start-up setpoint and the borated water of MHSI is key to limit the reactivity insertion and power excursion.

e) Protection Signals

For this event, the following protection actions can be used to mitigate the sequence of the event:

1) Reactor trip is actuated by “Pressuriser pressure low 2”, “Pressure drop of SG high l” or “Pressure drop of SG high 0”;

2) MSIVs are isolated by the “SG pressure low 1” signal or “Pressure drop of SG high 1” signal;

3) ARE [MFFCS] full load lines are isolated by the reactor trip signal;

4) Isolation of the low load main feedwater line on corresponding SG is actuated on “SG pressure low 2” signal; Isolations of the low load main feedwater line on all SGs are actuated on “Pressure drop of SG high 2”;

5) Safety injection is triggered by the “Pressuriser pressure low 3” signal.

In order to delay the protective actions to mitigate the consequences of this event, except for the startup of ASG [EFWS], the actuation setpoint is assumed to be its nominal value plus uncertainty and maximum delay time between the setpoint actuation and startup of protective actions is considered.

f) Safety Systems Performance

Minimum safety injection capability is assumed to minimize insertion of negative reactivity due to boron injection. The flow variation of safety injection due to changes in reactor coolant pressure is taken into account.

Maximum ASG [EFWS] capability is assumed to promote core overcooling.

g) Control Systems

Primary pressure control system includes pressuriser heaters and spray system. In the present transient, both the pressuriser pressure and water level drops rapidly. The pressuriser spray system which is intended to lower the primary pressure is mainly used for overpressure transients and does not function for this accident. The pressuriser heaters are stopped when the pressuriser level is too low. The actuation of pressuriser heaters reduce the core overcooling. Hence, the pressuriser pressure control system is not simulated in the analysis.

12.9.1.1.3.4 Results

A break spectrum analysis has been performed at zero power. The break spectrum covers the break size from double ended guillotine break (equivalent to area of steam generator outlet flow limiter, which is DN407) to DN50.

The detailed analysis of this fault is shown reference [51]. It can be concluded that the double ended guillotine break is the most pessimistic case due to the most severe core overcooling effect which leads to more reactivity insertion compared to smaller break size. The minimum DNBR is { } for double-ended guillotine break which is greater than the design limit { }.

The present results show that no DNB occurs and the integrity of cladding is not challenged. The fuel pellet also remains intact since the nuclear power is not as intensive as rod motion accidents especially for rod ejection accident in which fuel temperature remains under the limit value.

12.9.1.1.4 Steam System Piping Large Break at Full Power

12.9.1.1.4.1 Main Safety Functions

In order to reach the controlled state, the following main safety functions are required:

a) Reactor trip is actuated by any of the following signals:

   1) High neutron flux (power range, high setpoint);

   2) Pressure drop of SG high 0;

   3) Overpower ΔT;

b) Turbine trip and isolations of the full load main feedwater lines on all SGs are actuated on receipt of reactor trip signal;

c) Isolation of the low load main feedwater line on corresponding SG is actuated on “SG pressure low 2” signal; Isolations of the low load main feedwater line on all SGs are actuated on “Pressure drop of SG high 2”;

d) Isolations of the main steam lines on all SGs are actuated on “SG pressure low 1” signal or “Pressure drop of SG high 1” signal;

e) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

f) VDA [ASDS] is opened by the “SG pressure high 1” signal;

g) Manual isolation of ASG [EFWS] of affected SG.

In order to reach the safe state, the following manual safety functions are required:

a) Affected SG isolation

The affected SG is isolated manually to prevent the core overcooling and to limit the mass and energy release inside containment.

b) Startup of ASG [EFWS]

If the ASGs [EFWS] for the unaffected SGs are not actuated automatically, the operator will start the ASGs [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASGs [EFWS].

c) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

d) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

e) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

f) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than { }.

g) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.9.1.1.4.2 Typical Events Sequences

A typical events sequence, during which automatic actions and manual actions are presented, can be divided into the following two stages:

a) From initiating event to controlled state

Initially, the fault leads to the secondary side depressurisation and power increase. Reactor trip is trigger by “High neutron flux (power range, high setpoint)”, “Pressure drop of SG high 0” or “Overpower ΔT” signals. The closure of all MSIVs is triggered by the “SG pressure low 1” or “Pressure drop of SG high 1” signals, and ARE [MFFCS] full load lines for all SGs are isolated by reactor trip signal. ARE [MFFCS] low load line might also be isolated by the “Pressure drop of SG high 2” or “SG pressure low 2” signal.

During the transient, the ASG [EFWS] can be actuated when SG level reaches to the setpoint of the “SG level (wide range) low 2” signal. Moreover, the VDA [ASDS] of unaffected SG will automatically open if the secondary pressure exceeds its threshold.

Thereafter, when the affected SG is empty and the heat removal is ensured by the VDA [ASDS] and ASG [EFWS] of the unaffected SGs, the controlled state is reached.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, the affected SG will be isolated as the first operator action. After that, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.9.1.1.4.3 Analysis Assumptions

The detailed assumptions are presented in Reference [51]. The main assumptions are listed as follows:

a) Initial Conditions

In order to fully study the consequence of this event and find the most pessimistic case, the break spectrum is analysed ranged from DN50 (corresponding to nominal diameter 50 mm) to double ended guillotine break. Considering the impact of the SG outlet flowrate limiter (corresponding to nominal diameter 407mm), the transient response for the break greater than DN407 is the same with that for DN407.

The initial condition is assumed as a full power state. In order to minimize the DNBR

and maximize the cladding temperature, the key thermal hydraulic parameters of transient analysis are set as follows:

1) The initial operating power is 102%FP considering a positive power uncertainty 2%;

2) The initial average coolant temperature is 309.5℃ considering a positive temperature uncertainty 2.5℃;

3) The initial pressuriser pressure is 15.25MPa considering a negative pressure uncertainty 0.25 MPa;

4) The initial reactor coolant flowrate is set as the thermal design flow (24000m³/h per loop), considering that 0% of the SG tubes are plugged;

5) The heat transferred from two unaffected SGs to the reactor coolant (i.e., SG reversed heat transfer) is not considered, so as to enhance the reactor coolant overcooling.

b) Core Related Assumptions

The following core related assumptions are used for full power condition.

1) The moderator density coefficient is set to the maximum absolute value to maximise negative reactivity feedback due to decrease in coolant temperature.

2) The Doppler power defect, tending to slowdown the nuclear power increase, is set to the minimum value to maximize the core power.

3) The RCCA with the maximum worth is assumed to be stuck out of the core to minimize the negative reactivity after the reactor trip; at the same time, the most conservative negative reactivity insertion curve as a function of time is used.

c) LOOP Assumption

The loss of offsite power (LOOP) is assumed to occur at the time of turbine trip. For this accident, since minimum DNBR occurs before turbine trip. Therefore, LOOP has no effect for the DNB analysis.

d) Single Failure

Before minimum DNBR appears, “Pressure drop of SG high 0”, “High neutron flux (power range, high setpoint)” or “Overpower ΔT” signal will be actuated to mitigate the event consequences against acceptance criteria. Thus, the single failure assumption is applied on one channel of reactor trip signal.

e) Protection Signals

For this event, the following protection actions can be used to mitigate the sequence

of the event:

1) Reactor trip is actuated by any of the following signals:

- High neutron flux (power range, high setpoint);
- Pressure drop of SG high 0;
- Overpower ΔT;

2) MSIVs are isolated by the "SG pressure low 1" signal or "Pressure drop of SG high 1" signal;

3) ARE [MFFCS] full load lines are isolated by the reactor trip signal;

4) Isolation of the low load main feedwater line on corresponding SG is actuated on "SG pressure low 2" signal; Isolations of the low load main feedwater line on all SGs are actuated on "Pressure drop of SG high 2";

5) ASG [EFWS] is triggered by the "SG level (wide range) low 2" signal;

6) VDA [ASDS] is opened by the "SG pressure high 1" signal.

In order to delay the protective actions to mitigate the consequences of this event, except for the startup of ASG [EFWS], the actuation setpoint is assumed to be its nominal value plus uncertainty and maximum delay time between the setpoint actuation and startup of protective actions is considered.

f) Safety Systems Performance

Before minimum DNBR appears, safety systems such as ASG [EFWS], VDA [ASDS] will not be activated. Therefore, the safety systems' performance has no effect on the transient analysis and DNB analysis.

g) Control Systems

The pressuriser spray is assumed to be available and spray flowrate is set as the maximum value to minimize the primary pressure, which will worsen the consequences of DNB analysis. The pressurizer heaters are not taken into account.

12.9.1.1.4.4 Results

A break spectrum assessment is performed at full power. The analysed break sizes are ranged from DN50 to double ended guillotine break. The detailed analysis results is shown in reference [51].

For the break size less than DN210, the break is relatively small and the reactor isn't tripped by any automatic protection signal. For the break from DN210 to DN260, the reactor is tripped by "overpower ΔT". For the break from DN260 to DN297, the reactor is tripped by "high neutron flux (power range, high setpoint)". For the break

size larger than DN297, the reactor is tripped by “pressure drop of SG high 0”.

According to the analysis results, the worst case is break DN260. For the break DN260, the “high neutron flux (power range, high setpoint)” and “overpower ΔT” signals trip the reactor at the same time. The minimum DNBR is { } corresponding to the break DN260, which is greater than the design limit { }.

The analysis shows that no DNB occurs and the integrity of cladding is not challenged. The fuel pellet also remains intact since the nuclear power is not as intensive as rod motion accidents especially for rod ejection accident in which fuel temperature remains under the limit value.

12.9.1.1.5 Conclusions

a) From Initiating Event to Controlled State

For this accident, no DNB occurs and the limit of fuel pellet temperature and cladding temperature are not challenged. The fault analysis shows that the acceptance criteria are met.

b) From the Controlled State to the Safe State

This transient to reach safe state is not explicitly analysed as it is bounded by other faults or quantitatively analysed from the following aspects:

1) In terms of sub-criticality, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown from controlled state to safe state. The capability of RBS [EBS] is abundant to bring the RCP [RCS] to safe state.

2) In terms of heat removal, it is bounded by “Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG” fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case.

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed in Sub-chapter 12.11.4.7.

12.9.2 Decrease in Heat Removal by the Secondary System

12.9.2.1 Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG

12.9.2.1.1 Description

Feedwater system piping large break including breaks in connecting lines to SG is defined as the feedwater line break (FLB) occurs on the feedwater system, which is large enough to prevent the feedwater from reaching the SGs. When the large break is postulated to be happened between the check valve and the SG, the fluid in the affected SG may be discharged through the break, resulting in the decrease of SG pressure. After the turbine trip while the MSIVs are not closed, the pressure in unaffected SGs is higher, causing a reversal of steam flow from the two unaffected SGs to the affected SG.

Considering that if the break located upstream of the check valve, the consequence is similar to that of “Loss of Normal Feedwater Flow” accident. In this section, the break located between the check valve and the SG is evaluated.

Depending on the break size and the plant operating conditions at the time of break, this event might either cause RCP [RCS] overcooling by excessive steam discharge through the break or RCP [RCS] overheating by excessive liquid discharge through the break.

During the feedwater system piping break transient, liquid in affected SG could leak from the break. In the “Large Steam System Piping Break” transient analysis, saturated steam is released. Since saturated steam can remove more heat from the primary circuit than water, overcooling from a “Large Steam System Piping Break” transient is more onerous and thus, the analysis of “Large Steam System Piping Break” can bound the effects of RCP [RCS] overcooling caused by a feedwater system piping break. Therefore, only the RCP [RCS] heat-up effects of a feedwater line break are evaluated in this section.

A feedwater line break reduces the ability to remove heat generated by the core from the RCP [RCS] for the following reasons:

a) The flow rate of the main feedwater flow to the SGs is reduced;

b) The emergency feedwater leaks through the break of affected SG.

This reduction of heat removal capability results in RCP [RCS] pressure and temperature increasing. The bulk boiling may occur and the pressuriser may be filled due to decay heat.

State A and state B are taken into account in this fault. Considering the same break sizes and the similar mitigation measures in state B and in state A, the initial reactor power in state B is lower than state A, and the SG secondary water inventory in state

B is larger than state A. So the heat removal capacity of secondary side in state B is higher than state A, the consequence of state B is not severe than state A. Therefore, the fault of FLB in state A is analysed in this section.

The main consequence of the FLB is overheating. Considering the contribution of RCP [RCS] pump power to the primary heating, the fault with or without the loss of offsite power (LOOP) are carried out to evaluate the impact of LOOP in accident analysis.

The main consequence of the FLB is overheating. Considering the contribution of RCP [RCS] pump power to the primary heating, the fault with or without the loss of offsite power (LOOP) are carried out to evaluate the impact of LOOP in accident analysis.

The following two cases are analysed from initiating event to controlled state:

Case 1a: LOOP is not considered;

Case 1b: LOOP occurs at the time of turbine trip.

The following two cases are analysed from controlled state to safe state:

Case 2a: LOOP is not considered;

Case 2b: LOOP occurs at the time of turbine trip.

12.9.2.1.2 Acceptance Criteria

Feedwater system piping large break including breaks in connecting lines to SG is classified as a DBC-4 event. The fuel integrity and RCP [RCS] integrity might be challenged in this fault.

a) For analysis from initiating event to controlled state, the following acceptance criteria are adopted:

   1) The amount of fuel rods experiencing DNB must remain less than 10%;

   2) The peak cladding temperature must remain less than 1482℃;

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

   For this transient, it is considered that if the RCP [RCS] loops remain full, the core is covered and the bulk boiling does not occur, the fuel integrity is guaranteed. As result, the criteria presented above are met if the core remains covered and bulk boiling does not occur in the core.

b) For analysis from controlled state to safe state, the aim of the study is to demonstrate that the plant can be brought from controlled state to safe state and maintained in the safe state by FC1 and FC2 systems before the ASG [EFWS] tank inventory is exhausted, that is:

1) The core remains sub-critical. After reactor trip, boration is used to compensate the reactivity resulting from RCP [RCS] cooldown via RBS [EBS]. The capacity of RBS [EBS] is sufficient to satisfy the requirement of sub-criticality margin. Therefore, the core can remain sub-critical during the transient.

2) The residual heat can be continuously removed. For this accident, it means that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted. The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.9.2.1.3 Main Safety Functions

In order to reach controlled state, the following main FC1 safety functions are required:

a) Reactor trip is triggered by the “SG level (narrow range) low 1” signal;

b) Turbine trip and isolation of the full load main feedwater lines of all SGs are actuated on receipt of reactor trip signal;

c) The isolation of low load main feedwater lines of all SGs is triggered by the “Pressure drop of SG high 2” signal;

d) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) VDA [ASDS] open is triggered by the “SG pressure high 1” signal;

f) MSIVs closure is triggered by the “SG pressure low 1” signal;

g) RCP [RCS] pumps are triggered by the “SG level (wide range) low 4” signal;

h) Manual isolation of ASG [EFWS] of affected SG.

In order to reach the safe state, the following FC2 manual safety functions are required:

a) Affected SG isolation

The affected SG is isolated manually to prevent the drainage of the corresponding ASG [EFWS] tank and to limit the mass and energy release inside containment, and to allow re-supply of feedwater to the unaffected SGs.

b) Realign of ASG [EFWS] injection

If the ASG [EFWS] of an unaffected SG is unavailable, after affected SG isolation, the ASG [EFWS] of affected SG shall be switched to the unaffected SG, by opening/closing related isolation valves.

c) SG water level control

The SG water level is controlled by operator with adjusting the flowrate of the ASG [EFWS] injection in order to provide continuous heat removal.

d) RCP [RCS] boration

The RBS [EBS] pumps are started/stopped manually by the operator to control the boron concentration of RCP [RCS] and to ensure the sub-criticality margin in the RCP [RCS] is sufficient.

e) RCP [RCS] cooldown

The cooldown is performed by adjusting the steam flowrate via the VDA [ASDS] of unaffected SGs in order to control cooling requested by the operator.

f) RCP [RCS] depressurization

The RCP [RCS] depressurisation is achieved by opening the PSVs or pressuriser spray.

g) Accumulators isolation

The accumulators are isolated to avoid unexpected injection.

h) RIS [SIS] in RHR mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous RCP [RCS] heat removal and long term core cooling.

FLB is the sizing condition for the ASG [EFWS] minimum flowrate. The ASG [EFWS] minimum flowrate combined with the maximum delay time should ensure that the controlled state can be reached during the transient.

FLB is the limiting case to verify the ASG [EFWS] tanks water inventory. In the case of FLB, the total capacity of ASG [EFWS] tank should be able to bring the plant from controlled state to safe state and maintain the plant in the safe state.

12.9.2.1.4 Typical Events Sequences

A typical sequence of events, where automatic actions and manual actions are presented, can be divided into the following two stages:

a) From initiating event to controlled state

After the feedwater line break, the water level in the unaffected SGs will decrease before the isolation of the affected SG, leading to a primary heating. reactor trip signals can be triggered as the SG level decreases, after which the primary temperature and pressure continue to increase due to the core decay heat. Bulk boiling may occur and the pressuriser may be filled.

However, the RCP [RCS] pressure can be limited by opening of PSVs. The main steam line will be isolated as the decrease of affected SG pressure. After that, the

pressure of unaffected SGs increase and VDAs [ASDS] actuate. The ASG [EFWS] will be actuated as the water level decrease of affected SG. Therefore, the residual heat can be continuously removed. On the other hand, the ASG [EFWS] of affected SG is isolated by operator, and the reactor can be taken to the controlled state.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, the affected SG will be isolated firstly. After that, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray. PSVs can be used when the pressuriser spray is unavailable.

12.9.2.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [52].

a) From Initiating Event to Controlled State

The break is assumed to occur between SG feedwater inlet nozzle and check valve. The size of break is assumed to be the most conservative, corresponding to the area of the SG feedwater inlet nozzle.

Main feedwater to all SGs is assumed to be lost after the break occurs. All main feedwater flows out through the break.

1) Initial conditions

In order to maximise the consequence of overheating, the key thermal hydraulic parameters of transient analysis are set as follows:

- The initial power is the full power plus 2% uncertainty;
- The initial coolant temperature is nominal value plus 2.5℃ uncertainty;
- The initial pressuriser pressure is nominal value minus 0.25 MPa uncertainty;
- The initial pressuriser level is nominal value minus 7% uncertainty;

- The initial SG water level is nominal level minus 10% uncertainty;

2) Core-Related Assumptions

The conservative decay heat data is used to penalise the overheating of RCP [RCS].

3) LOOP Assumptions

The impact of the LOOP is considered in this analysis:

- For Case 1a, LOOP is not considered. This increases the total heat produced by the reactor coolant pumps during the transient. The heat to be removed of the RCP [RCS] is increased, thus the RCP [RCS] overheating might be strengthened.
- For Case 1b, LOOP occurs at the time of turbine trip. The RCP [RCS] flowrate is decreased due to the stop of reactor coolant pump. The decrease of the RCP [RCS] flowrate will reduce the heat exchange between the RCP [RCS] and the SG secondary side, which may strengthen the RCP [RCS] overheating.

4) Single Failure

For case 1a and case 1b, the single failure is postulated as that one ASG [EFWS] is unavailable. Moreover, the ASG [EFWS] flow is set to the minimum value. This will reduce the heat exchange between the RCP [RCS] and the SG secondary side, and strengthen the RCP [RCS] overheating.

b) From Controlled State to Safe State

The main concern of FLB analysis from controlled state to safe state is to demonstrate that the safe state can be reached when the RIS [SIS] connected in RHR mode before the ASG [EFWS] tanks inventory is exhausted. Some assumptions are not same as analysis from initiating event to controlled state due to the different criteria.

1) Initial conditions

In order to maximize the ASG [EFWS] tanks water consumption, the key thermal hydraulic parameters of transient analysis are set as follows:

- The initial power is the full power plus 2% uncertainty;
- The initial coolant temperature is nominal value plus 2.5℃ uncertainty;
- The initial pressuriser pressure is nominal value plus 0.25 MPa uncertainty;
- The initial pressuriser level is nominal value plus 7% uncertainty;
- The initial SG water level is nominal level minus 10% uncertainty;

2) Core-Related Assumptions

The conservative decay heat data is used to penalise the overheating of RCP [RCS], so as to maximize the ASG [EFWS] tanks water consumption.

3) LOOP Assumptions

The impact of the LOOP is considered in this analysis:

- For Case 2a, LOOP is not considered. This increases the total heat produced by the reactor coolant pumps during the transient. The heat to be removed of the RCP [RCS] is increased, thus the RCP [RCS] overheating might be strengthened.
- For Case 2b, LOOP occurs at the time of turbine trip. The RCP [RCS] flowrate is decreased due to the stop of reactor coolant pump. The decrease of the RCP [RCS] flowrate will reduce the heat exchange between the RCP [RCS] and the SG secondary side, which may strengthen the RCP [RCS] overheating.

4) Single Failure

For Case 2a, the single failure is postulated as that one RBS [EBS] train is unavailable. In this case, the water level of the unaffected SGs may not decrease to "SG level (wide range) low 4" setpoint. Therefore, the RCP [RCS] pumps may not trip and the heat produced by RCP [RCS] pumps will increase the consumption of feedwater in ASG [EFWS] tanks.

For Case 2b, the single failure is postulated as that one EDG train corresponding to the unaffected loop is failed. During the transient, only one ASG [EFWS] train is functioning for one unaffected SG before the operator action, which decreases the heat removal capability. Therefore, this assumption extends the duration of the transient, and exhausts more ASG [EFWS] tanks water.

5) Operator Actions

Operator actions from the Main Control Room (MCR) are assumed to perform no earlier than 30 minutes after the first significant information is transmitted to the operator.

12.9.2.1.6 Results and Conclusions

a) From Initiating Event to Controlled State

The detailed analysis of this fault (see reference [52]) shows that, for Case 1a, the minimum margin between hot leg temperature and saturation temperature is 8.1℃. For Case 1b, The minimum margin between hot leg temperature and saturation temperature is 9.3℃. The results show that:

1) Bulk boiling does not occur in the RCP [RCS];

2) The core are covered;

3) The emergency feedwater flow at the required time is sufficient for decay heat removal with reactor coolant temperature while pressure then begins to decrease.

Thus, the acceptance criteria from initiating event to controlled state are met.

b) From Controlled State to Safe State

The detailed analysis of this fault (see reference [52]) shows that:

For Case 2a, from the beginning of this event to the time where the RIS [SIS] in RHR mode connection conditions are reached, the consumption of ASG [EFWS] in the unaffected SGs is 817 tons, the mass leaked from the break before ASG [EFWS] isolation in the affected SG is about 100 tons, so the total feedwater consumption in ASG [EFWS] tanks is about 917 tons. The consumption is less than the capacity of the ASG [EFWS] tanks (1530 tons).

For Case 2b, from the beginning of this event to the time when the RIS [SIS] in RHR mode connection conditions are reached, the consumption of ASG [EFWS] in the unaffected SGs is 795 tons, the mass leaked from the break before ASG [EFWS] isolation in the affected SG is about 100 tons, so the total feedwater consumption in ASG [EFWS] tanks is about 895 tons. The consumption is less than the capacity of the ASG [EFWS] tanks (1530 tons).

For these two cases, the RIS [SIS] in RHR mode connection conditions can be reached before the ASG [EFWS] tanks are exhausted. Therefore, the plant can reach the safe state and the core and reactor coolant system integrity can be maintained during the transient. The acceptance criteria from controlled state to safe state are met.

The fault analysis show that after the FLB occurs, the fuel integrity is maintained during the transient from the initial event to the controlled state. The plant can reach and be maintained in the safe state, before the ASG [EFWS] tanks inventory is exhausted during the transient from the controlled state to the safe state. Therefore, the acceptance criterion for this event is met.

c) Radiological Consequence

The radiological consequence can be bounded by the accident of steam system piping large break. The fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity release pathways are the same which include the release of secondary coolant through VDA and through piping break. However, more airborne radioactivity will release to the environment in the accident of the steam system piping large break than that of the feedwater system piping large break.

The source term and radiological consequence of bounding accident of steam system piping large break is analysed in Sub-chapter 12.11.4.7.

12.9.2.2 Long Term LOOP of 168 Hours Duration

12.9.2.2.1 Description

This sub-chapter describes the analysis for long term loss of offsite power (LOOP) of 168 hours duration, which refers to that the offsite power supply cannot be restored within 168 hours. The analysis for short term LOOP (< 2 hours) and medium term (2 hours ~ 24 hours) are presented in sub-chapter 12.7.2.2 and sub-chapter 12.8.2.2. State A, state B, state C, state D, state E and state F are taken into account for this fault. LOOP is caused by:

a) A complete loss of offsite grid;

b) An onsite alternating current power distribution system failure;

c) An external grid disturbance (dropped voltage or frequency).

The analysis is divided into two parts according to their different initial conditions:

Part 1: LOOP in state A and B, as the RIS [SIS] in RHR mode is not connected to RCP [RCS] and the heat in RCP [RCS] is removed by the steam generators;

Part 2: LOOP in state C, state D, state E and state F, as the RIS [SIS] in RHR mode is connected and the heat in RCP [RCS] is removed by the RIS [SIS] in RHR mode.

In state A and state B, LOOP leads to the loss of power supply to all reactor coolant pumps, feedwater pumps and condensate pumps. Because of the decrease of reactor coolant flow and the decrease of the secondary system heat removal capacity, the core heat removal capacity of the RCP [RCS] decreases. The event will result in overheating both on primary side and secondary side.

In state C, D, E and F, LOOP can lead to the loss of power supply to all reactor coolant pumps, feedwater pumps, condensate pumps and RIS [SIS] pumps. As a consequence, the capacity of heat removal from the reactor core reduces, causing overheating in the primary side.

12.9.2.2.2 Acceptance Criteria

Long term LOOP of 168 hours duration is classified as a DBC-4 event. The following acceptance criteria are used for DBC-4 events:

a) The amount of the fuel experiencing DNB must remain less than 10%;

b) The peak cladding temperature must remain less than 1482℃;

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

For state A to state B, the following acceptance criteria should also be respected:

a) The core remains sub-critical;

b) The residual heat can be continuously removed. For this accident, it means that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted. The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling. Emergency diesel generators can supply electricity to ASG [EFWS] pumps and RIS [SIS] pumps.

For state C to state F, the RCP [RCS] heat is mainly removed by the RIS [SIS] system in RHR mode, and the following acceptance criteria should also be respected:

a) The core remains sub-critical;

b) The residual heat can be continuously removed, i.e., RCP [RCS] water inventory remains stable and the capacity of RIS [SIS] trains in RHR mode is able to satisfy the requirement of heat removal. Emergency diesel generators can supply electricity to RIS [SIS] pumps in the medium term.

12.9.2.2.3 Results and Conclusions

For the 24 hours duration, the typical sequence of the long term LOOP is the same with that of the medium term LOOP. So the results of long term LOOP within 24 hours can be bounded by the medium term LOOP accident (DBC-3) in sub-chapter 12.8.2.2.

During the safe state, the decay heat can be removed by RIS [SIS] (supplied by EDG) in RHR mode. Since the EDG can operate continuously for at least 7 days (168h) at the rated power and the duration of LOOP (DBC) is less than 168h, the EDG operation will cover the duration. So the acceptance criteria are met.

The fault analysis in state A and state B indicates that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted; The heat removal can be ensured by RIS [SIS] trains in RHR mode in the long term, then the plant can be maintained in the safe state within 168 hours.

The fault analysis in state C to state F indicates that there is no risk of core uncovery and the heat removal can be ensured in the long term.

For long term LOOP, boration is used to compensate the reactivity resulting from RCP cooldown via RBS [EBS]. The capacity of RBS is able to satisfy the requirement of sub-criticality margin. Therefore, the core can maintain sub-critical during the transient.

Therefore, for long term LOOP of 168 hours duration in state A to state F, the acceptance criteria presented in section 12.9.2.2.2.2 and section 12.9.2.2.3.2 are met.

The radiological consequence can be represented by the accident of turbine trip, because the fuel integrity and primary circuit integrity of both accidents are not challenged, and the radioactivity transport and release pathway are the same.

The source term and radiological consequence of turbine trip is analysed in Sub-chapter 12.11.4.1.

12.9.3 Decrease in Reactor Coolant System Flowrate

12.9.3.1 Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break

12.9.3.1.1 Description

Reactor coolant pump seizure (locked rotor) or reactor coolant pump shaft break is caused by mechanical failure. Seizure of shaft break of one reactor coolant pump will cause an instant core flow reduction and a rapid increase in reactor coolant temperature, which may result in fuel rods experiencing DNB and subsequent possible fuel damage.

The result of a reactor coolant pump shaft break is bounded by a reactor coolant pump seizure, as the coolant flow reduction rate is lower for the former. Therefore, only the locked rotor is considered further.

This fault may occur in state A, state B and state C. Compared to state B and state C, the core power is higher in state A, which will worsen the consequences of this fault. Therefore, the consequence of reactor coolant pump seizure (locked rotor) in state A is more onerous than that in state B and state C. In this sub-chapter, reactor coolant pump seizure (locked rotor) in state A is analysed.

12.9.3.1.2 Acceptance Criteria

Reactor coolant pump seizure (locked rotor) or reactor coolant pump shaft break accident is classified as a DBC-4 event. The following acceptance criteria are used for DBC-4 events:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.9.3.1.3 Main Safety Functions

In order to reach controlled state, the following main FC1 safety functions are required:

a) Reactor trip is triggered by the “Low flow rate in one primary loop” signal when the permissive signal P8 exists. If P8 does not exist (the primary power is lower than 30%FP), reactor trip might not be triggered by automatic signal. Since the core flowrate is relatively high due to the two unaffected RCP [RCS] pumps and the core power is relatively low. So there is no challenge of the integrity of fuel and RCP [RCS] when P8 does not exist.

b) Turbine trip and isolation of the full load main feedwater line on all SGs are actuated on receipt of reactor trip signal;

c) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

d) VDA [ASDS] is opened by the “SG pressure high 1” signal.

In order to reach the safe state, the following FC2 manual safety functions are required:

a) Startup of ASG [EFWS]

If the ASGs [EFWS] are not actuated automatically, the operator will start the ASGs [EFWS] manually. The SG level is also controlled by operator with adjusting the flowrate of the ASGs [EFWS].

b) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration corresponding to cold shutdown state is reached.

c) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

d) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is achieved by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

e) Accumulators isolation

The accumulators are isolated to avoid the injection of accumulator water.

f) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.9.3.1.4 Typical Events Sequences

a) From the initiating event to the controlled state

At the beginning of the transient, the flowrates in the core and the affected loop decrease rapidly. The decrease in core flow will result in rapid rise of coolant temperature and pressure. When the primary flowrate reduces to the setpoint of the “Low flow rate in one primary loop” signal, reactor trip is triggered and then the turbine trips automatically. ARE [MFFCS] full load lines are automatically closed by reactor trip signal. LOOP may occur due to the turbine trip. Subsequently, the two unaffected RCP [RCS] pumps begin to coast down.

During the transient, the ASG [EFWS] can be actuated when SG level reaches the setpoint of the "SG level (wide range) low 2" signal, and the PSVs will open when the PZR pressure exceeds the opening thresholds. Moreover, the VDA [ASDS] will automatically open if the secondary pressure exceeds its threshold. Therefore, the reactor can be maintained in controlled state.

b) From the controlled state to the safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary PZR spray and the PSVs can be used when the PZR sprays are unavailable.

12.9.3.1.5 Analysis Assumptions

Considering the different consequence severity level under different power level, the moderator density coefficient with different enveloping scope (power level) are considered in the safety analysis. The analysed two cases are as below.

a) Case 1: The accident occurs at full power;

b) Case 2: The accident occurs at 80%FP.

For Case 1, the moderator density coefficient covers 80%FP~100%FP. For Case 2, moderator density coefficient covers 0%FP~100%FP.

The detailed assumptions are presented in Reference [53]. The main assumptions are listed as follows:

a) Initial conditions

In order to minimize the DNBR and maximize the cladding temperature, the key thermal hydraulic parameters of transient analysis are set as follows:

1) For Case 1, the initial power is set to the 100%FP plus 2% uncertainty. For Case 2, the initial power is set to the 80%FP plus 2% uncertainty;

2) Initial reactor coolant average temperature is nominal value plus 2.5℃ uncertainty;

3) Initial PZR pressure is nominal value minus 0.25MPa uncertainty;

4) Initial reactor coolant flowrate is equal to the thermal design flowrate (24000m3/h per loop), considering 10% tube plugging of steam generators.

b) Core-related Assumptions

1) For Case 1, the moderator density coefficient is assumed to be 0.038 (10^5pcm)/(g/cm^3), which covers 80%FP~100%FP. For Case 2, moderator density coefficient is assumed to be 0 (10^5pcm)/(g/cm^3), which covers 0%FP~100%FP;

2) Doppler power coefficient is set as the maximum absolute value to minimize the power drop;

3) The RCCA with the maximum worth is assumed to be stuck out of the core to minimise the negative reactivity after the reactor trip; at the same time, the most conservative negative reactivity insertion curve as a function of time is used;

4) The specific axial power distribution and radial power distribution will be adopted in DNBR calculation and the enthalpy rise hot channel factor ($F_{\triangle H}$) shall be calculated via the formula below:

$F_{\triangle H}=1.65$, $P \geqslant 1$;

$F_{\triangle H}=1.65 \times [1+0.3(1-P)]$, $P < 1$;

Where P is the fraction of the rated power.

c) LOOP Assumption

LOOP is assumed to occur at the time of turbine trip. LOOP leads to the loss of power supply to all RCP [RCS] pumps, feed water pumps and condensate pumps. The protection and safety system are able to perform the safety functions since these systems can be supplied by emergency diesel generator (EDG). Therefore, the main effect of LOOP is to cause the RCP [RCS] pumps to coast down.

LOOP is considered as it reduces primary coolant flowrate which is pessimistic for DNB and fuel thermal transient analysis.

d) Single failure

Before the most pessimistic consequences against acceptance criteria appear, the reactor trip, which is triggered by “Low flow rate in one primary loop” signal, will be actuated to mitigate the event consequences. Thus, the single failure assumption is applied on one channel of “Low flow rate in one primary loop”

signal.

e) Protection Signals

Reactor trip is triggered by “Low flow rate in one primary loop” signal. In order to delay the protective actions to mitigate the consequences of this event, the actuation setpoint is assumed to be its nominal value minus uncertainty. Maximum delay time between the setpoint actuation and startup of protective actions is considered.

f) Systems Performance

Before the most pessimistic consequences against acceptance criteria appear, safety systems such as ASG [EFWS], VDA [ASDS] will not be activated. Therefore, the safety systems’ performance has no effect on the transient analysis.

g) Control Systems

The pressuriser spray is assumed to be available and spray flowrate is set as the maximum value to minimize the primary pressure, which will worsen the consequences of DNB analysis. The pressuriser heaters are not taken into account.

12.9.3.1.6 Results and Conclusions

a) From the initiating event to the controlled state

For Case 1, the amount of fuel rods experiencing DNB is { }, and the maximum cladding temperature is 983℃. The fuel pellet also remains intact since the nuclear power is not as intensive as rod motion accidents especially for rod ejection accident in which fuel temperature remains under the limit value. The acceptance criteria are met.

For Case 2, the minimum DNBR during the transient is { }, larger than the DNBR limit { }, thus there is no fuel rod experiencing DNB. During the transient, the nuclear power is continuously decreasing, and the initial nuclear power is lower than Case 1, thus the peak cladding temperature limit and the fuel pellet melting limit are not challenged.

During the transient, the amount of fuel rods experiencing DNB remains less than 10%, and the peak cladding temperature remains less than 1482℃. The fuel pellet melting also remains intact. The fault analysis shows that all the acceptance criteria are met.

b) From the controlled state to the safe state

The transient to reach safe state is not explicitly analysed as it is bounded by the following aspects:

1) In terms of sub-criticality, it is bounded by "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From controlled state to safe state, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown, the sub-criticality margin of the bounding case is lowest due to the boron dilution, and more boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by "Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG" fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case, whereas at least two ASG [EFWS] trains are available in this fault.

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed in Sub-chapter 12.11.4.11.

12.9.4 Reactivity & Power Distribution Anomalies

12.9.4.1 Spectrum of RCCA Ejection Accident

12.9.4.1.1 Initiating Event

The rod cluster control assembly (RCCA) ejection accident is defined as the scenario where an RCCA is vertically ejected from the reactor core due to the mechanical failure of the RCCA drive mechanism housing at the top of the pressure vessel.

This accident leads to a rapid reactivity transient by inducing an uncontrolled positive reactivity, followed by a nuclear power increase and a power distribution disturbance. The magnitude of the inserted reactivity is related to the inserted depth of the ejected RCCA. The nuclear power increase is limited by reactivity feedback effects, such as the Doppler feedback effect caused by the fuel temperature increase. This may result in DNB among the adjacent fuel channels, and the potential failure for the fuel cladding.

This accident may lead to a loss of reactor coolant through the break of the RCCA drive mechanism housing. Analysis in this scenario can be enveloped by the LOCA analysis.

In fact, the considered prevention measures for the design, fabrication, test and examination of the RCCA drive housing can help to avoid the accident caused by the failure of pressure-resistant shell.

This fault may occur in state A and state B. Compared to state B, the core power is higher and the sub-criticality margin is less in state A, which will worsen the consequences of this fault. Therefore, the consequence of RCCA ejection accident in state A is more onerous than that in state B. In this analysis, the RCCA ejection accident in state A is analysed.

12.9.4.1.2 Acceptance Criteria

RCCA ejection accident is classified as a DBC-4 event. The specific criteria are considered in this study as listed:

a) The enthalpy of fuel pellet must be less than design limit (942J/g for non-irradiated fuel and 837 J/g for irradiated fuel);

b) The fuel cladding temperature must not be greater than design limit (1482℃);

c) The amount of fuel rods experiencing DNB must not exceed design limit (10%);

d) The melting fuel pellet amount at the hot spot must remain below the design limit (10%);

e) {

}

12.9.4.1.3 Main Safety Functions

a) From Initiating Event to Controlled State

In order to reach the controlled state, the following FC1 plant safety functions are required:

1) Reactor trip is triggered by the “High neutron flux (power range)” signal or “High positive neutron flux rate” signal;

2) Turbine trip and isolations of the full load main feedwater lines on all SGs are actuated on receipt of reactor trip signal;

3) VDA [ASDS] is opened by the “SG pressure high 1” signal;

4) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal.

b) From Controlled State to Safe State

In order to reach the safe state, the following FC2 plant safety functions are required:

1) Startup of ASG [EFWS]

   If the ASGs [EFWS] are not actuated automatically, the operator will start the ASGs [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASGs [EFWS].

2) Startup/Isolation of RBS [EBS]

   The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

3) Startup of cooldown via VDA [ASDS]

   The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

4) RCP [RCS] depressurisation

   The RCP [RCS] depressurisation is achieved by PZR normal spray or opening

the PSV when the PZR normal spray is unavailable.

5) Accumulators isolation

The accumulators are isolated to avoid the injection of accumulator water.

6) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.9.4.1.4 Typical Events Sequences

A typical events sequence, during which automatic actions and manual actions are presented, can be divided into the following two stages:

a) From initiating event to controlled state

After the RCCA is ejected vertically from the reactor core, an uncontrolled positive reactivity insertion will be induced in the core, leading to a nuclear power excursion and a power distribution disturbance. During the initial phase, the nuclear power increase will be limited by reactivity feedback effects, i.e. the Doppler feedback effect. Then, the reactor trip is triggered by the “High neutron flux (power range)” signal or “High positive neutron flux rate” signal, causing a rapid decrease in nuclear power. The reactor core controlled state is reached by the actuation of the reactor protection system.

b) From controlled state to the safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.9.4.1.5 Analysis Assumptions

The detailed assumptions are presented in the reference [54]. The main assumptions are listed as follows:

a) Initial Conditions

The inserted reactivity during the RCCA ejection accident is closely related to RCCA configuration and therefore to the power level. Thus, all the fuel cycles, the typical burnup and power levels (0 %FP, 100 %FP and other intermediate power levels) are considered.

The following uncertainties are considered in the initial condition to worsen the consequences of the transient:

1) Power: +2 %FP;

2) Coolant temperature: +3.5 ℃ for 0%FP; +2.5 ℃ for other power levels;

3) Primary pressure: -0.25 MPa;

Initial reactor coolant flowrate is equal to the thermal design flowrate (24000m^3/h per loop), considering 10% tube plugging of steam generators, so as to penalise the heat removal.

b) Core-related Assumptions

1) Delayed neutron fraction. The adopted delayed neutron fraction value is conservatively set as the minimum value to promote power increase.

2) Moderator temperature coefficient. The value is set to the minimum absolute value for each burnup to minimize negative reactivity feedback due to increase in coolant temperature.

3) Doppler temperature coefficient. The minimum absolute value is adopted to minimize the limit on power increase.

4) Prompt neutron life. The minimum absolute value is applied to promote power increase.

5) Insertion of negative reactivity during RT. The RCCA with the maximum worth is assumed to be stuck out of the core to minimize the negative reactivity after the reactor trip; at the same time, the most conservative negative reactivity insertion curve as a function of time is used.

6) The RCCA ejection time. The RCCA is conservatively assumed to be ejected within 0.1s.

7) Initial core power distribution. The axial power shape is supposed for a specific power level, to tilt to the upper core to cause the pessimistic ejected RCCA worth, i.e. axial offset is set on the right boundary of the operation domain.

c) LOOP Assumption

LOOP is considered as it reduces primary coolant flowrate which is pessimistic for DNB and fuel temperature analysis. In principle, LOOP should be considered at the time of turbine trip because it is considered as a consequential event of the turbine trip. Since the transient of this accident is quite momentary, LOOP at the time of turbine trip could have minor impact to the results.

d) Single Failure

The safety functions except for reactor trip will not be actuated to mitigate the event consequences against acceptance criteria, thus the single failure is applied on one "High neutron flux (power range)" signal or on "High positive neutron flux rate" signal (sensor or channel).

e) Protection Signals

Reactor trip is triggered by the "High neutron flux" signal or "High positive neutron flux rate" signal. In order to delay the protective actions to mitigate the consequences of this event, the actuation setpoint is assumed to be its nominal value plus uncertainty and maximum delay time between the setpoint actuation and startup of protective actions is considered.

f) System Performance

Before the most pessimistic consequences against acceptance criteria appear, safety systems such as ASG [EFWS], VDA [ASDS] will not be activated. Therefore, the safety systems performance has no effect on the transient analysis.

g) Control Systems

In terms of DNB analysis, the pressuriser spray is assumed to be available and spray flowrate is set as the maximum value to minimize the primary pressure, which will worsen the consequences of DNB analysis. The pressuriser heaters are not taken into account.

h) Specific Assumptions

The DNB analysis adopts the thermal hydraulic condition and power shape at the time of the minimum DNBR during power transient. The DNB occurs if the DNBR is less than the design limit.
The hot spot factor for fuel thermal transient analysis is set to the pessimistic value, i.e. the calculated envelope of nuclear data plus the uncertainty and margin. DNB is conservatively assumed to occur at the start of the transient.

12.9.4.1.6 Results and Conclusions

a) From the initiating event to the controlled state

The analysis of this fault (see reference [54]) shows that the calculated amount of fuel rods experiencing DNB in the worst case is less than the design limit. The maximum

fuel temperature and maximum cladding temperature for the hotspot are under the design limit. For the medium and high burnup assemblies, the maximum fuel enthalpy rise is less than the limit value and the minimum pulse width is greater than the limit value.

Thus the acceptance criteria for this event are met.

b) From the controlled state to the safe state

This transient to reach safe state is not explicitly analysed as it is bounded or represented by other faults from the following aspects:

1) In terms of sub-criticality, it is bounded by "Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP [CSTS]" fault. From controlled state to safe state, RCP [RCS] is borated by RBS [EBS] to compensate the positive reactivity insertion resulting from RCP [RCS] cooldown, the sub-criticality margin of the bounding case is lowest due to the boron dilution, and more boron is needed to reach safe state in the bounding case.

2) In terms of heat removal, it is bounded by "Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG" fault. From controlled state to safe state, ASG [EFWS] is used to cooldown RCP [RCS], only one ASG [EFWS] train is available in the bounding case, whereas at least two ASG [EFWS] trains are available in this fault.

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed in Sub-chapter 12.11.4.6.

12.9.5 Decrease in Reactor Coolant System Inventory

12.9.5.1 SG Tube Rupture (Two Tubes in One SG) (State A\B\C)

12.9.5.1.1 Initiating Event

This sub-chapter describes the thermal-hydraulic analysis of a SGTR event (two tubes in one SG), which is defined as the double-ended guillotine rupture of two steam generator tubes in one SG.

This accident will lead to an increase in the radioactivity in the secondary system due to the leak of radioactive coolant from the reactor coolant system. If a LOOP or a failure of the condenser steam dump system occurs during the event, discharges of steam or liquid from the MSSV and/or the VDA [ASDS] will lead to a direct activity discharge to the atmosphere since the SGa has been contaminated. The radioactivity of the primary side coolant is due to corrosion and fission products generated by the continuous operation of the reactor with a limited number of damaged fuel rods.

The probability and risk of SGTR event is reduced through the following precautions:

a) High ductility of the SG tube material;

b) Blowdown system location at the bottom of SG tube bundle to prevent solid deposits on SG tube plate;

c) Chemically conditioned secondary water to protect SG tubes from corrosion;

d) Prevention of projectiles from originating from the main feedwater;

e) Designation of SG support plates to prevent tube damage and pipe whip of neighbouring tubes;

f) Continuous monitoring and control of secondary side activity.

The SGTR (two tubes in one SG) in state A\B\C is classified as a DBC-4 event.

The cases studied in this sub-chapter correspond to the double-ended guillotine rupture of two tubes in one SG, which allows unimpeded blowdown from both ends of the tube.

The rupture is located in the lower part of the SG tubes bundle, close to the tubesheet, on the cold side. This location maximises the SGTR leak flowrate. For the DBC-4 transients, a LOOP is superimposed on the accident, if conservative.

This sub-chapter aims to quantify the maximum radioactivity release to the environment. If overfilling occurs, contaminated water will be directly released to environment and the radioactivity release will be significant. The SG overfilling assessment (see Reference [55]) demonstrates that even under the most onerous conditions, overfilling will not occur. Without overfilling, the radioactivity release is carried by steam released to the environment. The case which analyses the most

pessimistic radioactivity release is presented hereafter.

12.9.5.1.2 Acceptance Criteria

The major issue for SGTR is to limit its radiological consequences. The acceptance criteria, adopted in SGTR, aim to ensure core safety and limit radiological consequences. The safety criterion for SGTR is the dose equivalent released to the environment. The main objective of SGTR transient analysis is to evaluate the core safety and provide interface data for radiological consequences analysis which will be discussed in Sub-chapter 12.11.

The SGTR transient is analysed against the following aspects:

a) Core remains covered;

   As there is no significant reactivity insertion during SGTR fault, this criterion indicates that fuel integrity can be ensured in case of SGTR.

b) There shall be no liquid discharge through the MSSV, to prevent the MSSV seizing open;

c) The plant shall be brought to and maintained in safe state.

12.9.5.1.3 Main Safety Functions

The following structures, systems and components, their related functions and operator actions are claimed in the analysis of SGTR.

a) Alarm

   SGTR detection by the “high activity in the Plant Radiation Monitoring System (KRT [PRMS])” signal: when high activity is detected in the KRT [PRMS], an alarm is actuated to inform the operator.

b) FC1 safety functions (automatic)

   1) Reactor trip

      Reactor trip is triggered either by the “Pressuriser pressure low 2” signal or by the “SG level (NR) high 1” signal.

   2) Turbine trip

      The reactor trip signal triggers the turbine trip.

   3) ARE [MFFCS] full load line isolation

      Following an reactor trip signal, ARE [MFFCS] full load line for all SGs is isolated. In a penalizing way, ARE [MFFCS] low load line is supposed to be isolated by the reactor trip signal.

   4) APG [SGBS] isolation

APG [SGBS] discharge is isolated when the ASG [EFWS] is actuated.

5) Safety injection

SI is actuated by the "Pressuriser pressure low 3" signal or "Hot leg ΔP_{sat} low 1" signal. This signal initiates a medium-pressure rapid cooldown. The maximum MHSI flowrate curve is chosen to maximise the pressure difference between the RCP [RCS] and the SGa.

6) Medium pressure rapid cooldown

Following the SI signal or "SG level (NR) high 2" signal, a medium pressure rapid cooldown (performed by all SGs, including the SGa) is initiated to cool the primary circuit with a rate of{ }.

7) ASG [EFWS] actuation

ASG [EFWS] is actuated automatically by the "LOOP and SI" signal or by "SG level (WR) low 2" signal.

8) ASG [EFWS] isolation

ASG [EFWS] in one certain loop is isolated by the "SG level (WR) high 1" signal of corresponding SG.

9) MSIV closure

The automatic MSIV isolation is triggered by the "Pressure drop of SG high 1" signal or by the "SG level (NR) high 2 after MCD finished" signal.

10) VDA [ASDS] opening

The VDA [ASDS] is opened by the "SG pressure high 1" signal.

11) VDA [ASDS] isolation

The VDA [ASDS] isolation is triggered by the "SG level (NR) high 2 after MCD finished" signal. And the VDA [ASDS] setpoint is adjusted to { } abs thereafter.

12) RCV [CVCS] charging line isolation

The RCV [CVCS] charging line is isolated automatically following the "SG level (NR) high 2 after MCD finished" signal.

c) FC2 safety functions (manual from the main control room):

1) SGa isolation:

After SGTR detection, the operator isolates the SGa (if not already done): ARE [MFFCS] and ASG [EFWS] isolation, MSIV closure and increase in the VDA [ASDS] setpoint.

2) RCV [CVCS] charging line isolation

   The RCV [CVCS] charging line is isolated manually, if not done automatically.

3) Reactor coolant system boration:

   The RBS [EBS] pumps are started by the operator before the reactor coolant system cooldown. The RBS [EBS] injection is stopped when the primary cold shutdown state boron concentration is reached.

4) Reactor coolant system cooldown by unaffected SGs:

   The cooldown is performed via the VDA [ASDS] of unaffected SGs. The cooling rate is { } with at least two RBS trains in operation.

5) Reactor coolant system and SGa depressurisation:

   During the reactor coolant system depressurisation, the accumulators are isolated when the reactor coolant system pressure decreases below { }.

   Two of the three MHSI pumps are stopped at the beginning of operation. The last MHSI pump stops when the TRIC is reduced to { }.

   Reactor coolant system is then depressurised until the LHSI injection pressure is reached. Because of the normal spray is conservatively assumed unavailable, the reactor coolant system depressurization is achieved by means of opening the VDA [ASDS] of the SGa.

6) RIS [SIS] in RHR mode connection:

   The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

As the maximum injection head of MHSI will directly determine the primary and secondary pressure balance behaviour, the performance of MHSI should be verified by SGTR events.

When the SGa needs to be isolated, the VDA setpoint is adjusted above the maximum injection head of MHSI to prevent continuous opening and unstoppable release. This function is dedicated to SGTR mitigation.

Another important factor to the radiological consequences of SGTR is the cool-down rate of MCD. As the radiological consequences of SGTR challenges the numerical targets, cool-down rate of MCD should be verified of SGTR events.

12.9.5.1.4 Typical Events Sequences

A typical sequence, the most likely to occur during the transient, is described hereafter.

Within this sub-chapter, the following description considers only the full power condition for this is the most onerous case for radiological release, and the overfilling case is described in Reference [55].

The sequence of events consists of two phases: the short-term phase, until leak elimination, and the long-term phase, where the plant is operated from leak elimination to the safe state. A typical sequence of events in state A is described hereafter.

a) From the initiating event to the leak elimination (short term)

1) From the initiating event to the controlled state

The controlled state for an SGTR is defined as a state where the core coolant inventory remains stable and residual heat removal can be ensured via the SGs.

At the beginning of this event, primary coolant leaks to the secondary side through the break, which leads to the contamination of the affected SG. Meanwhile, the primary pressure decreases. The reactor trip signal triggered depends on the initial conditions. For full power operation: The SGTR can be identified by the operator on receipt of the “High activity in the KRT [PRMS]” signal. Reactor trip is triggered by the “Pressuriser pressure low 2” signal. Turbine trip and isolation of the ARE [MFFCS] full and low load lines for all SGs are initiated following the reactor trip signal.

After reactor trip and turbine trip, the secondary pressure increases and rapidly reaches the VDA [ASDS] setpoint if GCT [TBS] is unusable. Contaminated steam is thus released to the environment and decay heat is removed.

The continuous leak to secondary side and the decrease in decay heat after reactor trip lead to a primary depressurisation. It is likely the “Pressuriser pressure low 3” signal will be triggered. Within this sub-chapter, the following description assumes the break is large enough to lead to the “Pressuriser pressure low 3” signal.

Following the safety injection signal triggered by the “Pressuriser pressure low 3” signal, the MCD is actuated. The MCD is carried out by reducing the VDA setpoint in order to cool the reactor coolant system with a rate of{ }. When the MCD is completed, the secondary pressure is reduced to 6.0 MPa abs. The MHSI pumps are actuated following the SI signal and start injecting when the primary pressure is lower than their injection head. The MHSI injection flow can compensate the leak flow from an SGTR and the controlled state is reached.

2) From the controlled state to the leak elimination

To stop the leakage, the operator isolates the SGa both on steam side and on feed side. In other words, the operator closes the ASG [EFWS] and the MSIV. In addition, the VDA [ASDS] setpoint for the SGa is adjusted up to a value between the MHSI injection head and MSSV setpoint in order to limit the radioactivity release.

The injection of MHSI maintains the primary pressure at a stable level. To reduce the leakage flow, the operator shuts down two of the three MHSI pumps (with the remaining left operating). Due to the isolation of the SGa, the pressure of SGa increases until it reaches primary pressure level and the leak is stopped. Before the leak is stopped, the SGa is not overfilled and only steam is released to the environment.

b) From the leak elimination to the safe state (long term)

The safe state for an SGTR is defined as a state when the RIS [SIS] train is connected to the reactor coolant system in residual heat removal (RHR) mode and the SGa remains isolated. The operator performs a primary cooldown and depressurisation to reach the RHR connection conditions, which are:

1) Reactor coolant system hot leg pressure < { } abs;

2) Reactor coolant system hot leg temperature < { };

3) Reactor coolant system hot leg saturation margin (ΔT_{sat}) and RPVL consistent with RIS [SIS] in RHR mode suction conditions from the hot leg.

During the reactor coolant system cooldown, to ensure the core sub-criticality, the operator uses RBS [EBS] to compensate the reactivity insertion resulting from the reactor coolant system cooldown. SGu and MHSI are used to cool the primary at a rate of { } with two or three RBS [EBS] trains or at a rate of { } with one RBS [EBS] train.

When the primary temperature is lower than { }, the last MHSI injection is stopped and the operator prepares to perform final depressurisation via the SGa. Prior to that, the operator shall confirm that the SGa level is lower than the relevant limits. Otherwise, one of the unaffected SGs shall be isolated, with its level limited to a lower value so that the SGa water inventory can be transferred to the this SGu via the APG [SGBS] transfer line. The RIS [SIS] in RHR mode can finally be connected and the safe state is reached.

12.9.5.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [45]. The main assumptions are listed as follows:

a) Single failure

The failure of SGa ASG [EFWS] pump is assumed. This assumption worsens the radioactive release from the SGa as it increases the risk of heat transfer tube exposure.

b) Initial state

The conditions for the initial state are chosen to maximise the RCP [RCS] heat to be removed after reactor trip and to make the SGa tubes exposed as soon as possible.

c) Core-related Assumptions

The decay heat is considered with an uncertainty of 1.645σ.

d) LOOP Assumption

The LOOP is assumed to occur at the time of turbine trip, considered as a consequence of turbine trip. LOOP leads to the loss of power supply to all RCP, feed water pumps and condensate pumps. The protection and safety systems are able to perform the safety functions since these systems can be supplied by EDG. Therefore, the main effect of LOOP is to cause the reactor coolant pumps to coast down.

e) Protection Signals

1) Reactor Trip

Reactor trip is triggered by the “Pressuriser pressure low 2” signal. The maximum positive uncertainty of “Pressuriser pressure low 2” signal is assumed to favour the reactor trip and penalize the steam release. The minimum delay time is uesd to penalize the steam release.

2) Safety Injection

SI is triggered by the “Pressuriser pressure low 3” signal. The “Pressuriser pressure low 3” signal is minimised to penalize the steam release. And the maximum delay time is taken into consideration to penalize the break flowrate.

3) MCD actuation

MCD is initiated by the “SI” signal. The maximum negative uncertainty and the maximum delay time are taken into consideration to penalize the break flowrate.

4) ASG [EFWS] start-up

ASG [EFWS] is actuated either by the “SI and LOOP” signal or by the “SG level (WR) low 2” signal. The maximum negative uncertainty and the maximum delay time are taken into consideration to penalize the steam release.

5) VDA [ASDS] opening

The VDA [ASDS] isolation valve is opened by “SG pressure high 1”signal. The setpoint is minimised on the SGa and maximised on the unaffected SGs to maximise the steam release from the SGa before the MCD.

f) System Performance

1) ASG [EFWS]

Only two unaffected SGs are fed, since the other ASG [EFWS] pump is lost because of the single failure. After ASG [EFWS] actuation, the SG level in the unaffected SGs is maintained at the reference water level.

The minimum flowrate of ASG [EFWS] is assumed to penalize heat removal.

During the long-term phase, ASG [EFWS] is manually controlled by operator to maintain the SG level in the two unaffected SGs at their nominal value.

2) MHSI

The maximum MHSI flowrate is chosen to maximise the pressure difference between the reactor coolant system and the SGa.

3) RBS [EBS]

The RBS [EBS] is manually actuated at the beginning of the reactor coolant system cooldown phase (30 minutes after the “High activity in the KRT [PRMS]” signal appeared) to ensure core sub-criticality during the reactor coolant system cooling.

The maximum flowrate is assumed to penalize primary pressure and inventory which maximises the break flowrate.

g) Control Systems

The following FC3 functions are assumed to penalize the radioactivity release:

1) RCV [CVCS]

To maximise the pressure difference between the reactor coolant system and the affected SG, the maximum charging flow rate is assumed.

2) Pressuriser Heaters

The effect of pressuriser heaters is not taken into account to favour the reactor trip and penalize the activity release.

The following FC3 function is not taken into account which could contribute to fault mitigation:

1) Pressuriser sprays

During long term phase, pressuriser spray could be used to depressurize primary and secondary side. It is not taken into account to penalize radiological consequences.

2) GCT [TBS]

GCT [TBS] is not taken into account to penalize radiological consequences.

h) Other assumptions: operator actions

The first operator action is assumed to be performed 30 minutes after the "High activity in the VVP KRT [PRMS]" signal. The first local manual operator action is assumed to be performed one hour after this signal.

For long-term mitigation, the operator actions aim at reaching the safe state.

12.9.5.1.6 Result and Conclusions

a) Results

The detailed analysis of this fault (see Reference [55]) shows that the controlled state can be reached after injection by the MHSI and the leak can be stopped by operator actions.

The RIS [SIS] in RHR mode connection conditions are met roughly 4 hours after SGTR initiation. In the worst case, the total steam release from VDA of SGa is 75.3 tons, including 69.8 tons released during the short-term phase. Once the RHR is connected, the safe state is reached.

b) Conclusions

As the analysis shows, the reactor can be taken to the safe state.

c) Radiological Consequence

The source term and radiological consequence of this accident is analysed and presented in Sub-section 12.11.4.9.

12.9.5.2 Intermediate Break and up to Surge Line Break - Loss of Coolant Accident (State A\B)

12.9.5.2.1 Intermediate Break and up to Surge Line Break (State A)

12.9.5.2.1.1 Initiating Event

An Intermediate Break - Loss of Coolant Accident (IB-LOCA) is defined as an accident in which a break larger than SB-LOCA occurs on the lines connected to primary coolant loops. The surge line of the pressuriser has the largest diameter among the lines connected to reactor coolant system and the equivalent diameter is 28.4 cm. The faults are classified as DBC-4 events.

This event results in a decrease in the pressure and water inventory of reactor coolant system with a possible core uncovery and heat-up.

12.9.5.2.1.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

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

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

12.9.5.2.1.3 Main Safety Functions

In this event, FC1 safety functions to achieve controlled state and FC2 safety functions to reach safe state are listed below:

a) FC1 safety functions

   1) Reactor trip

      In state A, if the core power is higher than 10 % Full Power (FP), reactor trip is triggered by the “Pressuriser pressure low 2” signal, and if the core power is lower than and equal to 10 % FP, reactor trip is triggered by the “Hot leg pressure low 1” signal.

   2) Turbine trip

The reactor trip signal triggers the turbine trip.

3) ARE [MFFCS] full load line isolation

Following the reactor trip signal, ARE [MFFCS] full load lines of all SGs are isolated.

4) ARE [MFFCS] low load line isolation

Following the signal, SG level (narrow range) high 0 after reactor trip, ARE [MFFCS] low load lines of all SGs are isolated.

5) MHSI and LHSI startup

MHSI and LHSI are actuated when receiving SI signal. SI signal is triggered by the “Pressuriser pressure low 3" signal.

6) ASG [EFWS] startup

It is triggered by “LOOP and SI signal” or by the “Steam generator level (wide range) low 2” signal.

7) Medium pressure rapid cooldown (MCD)

Following the SI signal, a MCD is initiated to cool the primary circuit with a rate of { }.

8) Stop of Reactor Coolant Pumps

The shutdown of reactor coolant pumps is triggered by the “RCP ΔP low 1 and SI signal” signal.

9) Accumulator injection

Accumulator injects borated water to cold leg when the primary pressure decreases below the injection pressure of accumulator.

10) Opening of Atmospheric Steam Dump System (VDA [ASDS])

The VDA [ASDS] valves automatically open when the secondary pressure reaches the VDA [ASDS] setpoint.

b) FC2 safety functions

These functions are all manual actions in the main control room.

1) Reactor coolant system boration

The RBS [EBS] pumps are started by the operator before the reactor coolant system cooldown for reactor coolant system boration.

2) Reactor coolant system cooldown by SGs

The cooldown is performed via the VDA [ASDS] of secondary side for

primary depressurization.

3) MHSI stop

The MHSI pumps are shut down for primary depressurization.

4) Accumulators isolation

Accumulators need to be isolated to prevent nitrogen coming into reactor coolant system.

5) RIS [SIS] in RHR mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

6) Switch the LHSI pumps to simultaneous injection to the cold leg and hot leg

The connection of this function guarantees a continuous heat removal and core long-term cooling.

12.9.5.2.1.4 Typical Events Sequences

The transient of an event can be divided into two phases: the short-term phase to controlled state and the long-term phase to safe state. A typical sequence of events is described hereafter.

a) Analysis from the initiating event to the controlled state

LOCA events lead to a loss of primary coolant inventory and primary depressurization.

Intermediate Break and up to Surge Line Break - Loss of Coolant Accident (State A\B) is mainly a gravity-driven accident. In those cases, the reactor coolant system discharges slowly, and evident mixing layers will appear in the reactor coolant system. Depending on the variation of the mass and energy transfer during the transient, these mixing layers change over time.

For a typical sequence, core heat-up may happen twice during the transient. The first heat-up results from the core level decrease and the formation of loop seal, and it can be mitigated by loop seal clearance during the transient. The second heat-up results from the boiling and evaporation of the core coolant. During the second heat-up, the primary pressure might drop to the accumulator actuation setpoint. And this core heat-up might be interrupted by the reflooding of the accumulator injection flow. The increase of core temperature is affected by various factors which include the break size, safety injection flowrate, bypass flow rate from the upper head to the descending section, hot rod burn-up, etc.

Reactor trip is triggered by the “Pressuriser pressure low 2” signal. Following the reactor trip, turbine trip occurs and Main Feedwater Flow Control System (ARE

[MFFCS]) full load lines for all SGs are Isolated. After reactor trip and turbine trip, the secondary pressure increases rapidly until the setpoint of VDA [ASDS] is reached.

Because of the continuous break flow to the containment and the decrease of decay heat after reactor trip, the SI signal is triggered by the "Pressuriser pressure low 3" signal at power or by the "Hot leg ΔPsat low 1" signal at shutdown state. Medium Pressure Rapid Cooldown (MCD) is initiated in all SGs following the SI signal. The MCD is carried out by reducing the VDA [ASDS] setpoint, cooling down the reactor coolant system with a rate of { }. When the MCD completes, the secondary pressure is reduced to 6.0 MPa abs. Following the SI signal, the Medium Head Safety Injection (MHSI) and the Low Head Safety Injection (LHSI) pumps are actuated. The Safety Injection System (RIS [SIS]) starts injecting when the reactor coolant system pressure is below the pump injection head. The RIS [SIS] injection flow will compensate for the break flow.

After reactor trip and safety injection, the residual heat is mainly removed by the break flow, the RIS [SIS] and the secondary side. Controlled state is achieved when:

1) The primary residual heat can be continuously removed via the break and the plant safety systems including RIS [SIS] and VDA [ASDS];
2) Core sub-criticality is ensured;
3) Core coolant inventory stabilises or increases via the Safety Injection (SI).

b) From Controlled State to Safe State (long term)

The safe state is defined as a state at which the break flow rate is compensated by the RIS [SIS] flow rate with long-term core cooling ensured. Depending on the break size, the primary state may not meet the required connection conditions of RIS [SIS] in Residual Heat Removal (RHR) mode in the late phase of Intermediate Break and up to Surge Line Break - Loss of Coolant Accident (State A\B). In this situation, the operator should switch the LHSI pumps to the simultaneous injection to the cold leg and hot leg at the late stage of the accident, and the MHSI pumps continue to inject into the cold legs.

Strategies used to meet the above conditions can be claimed as into two cases.

For the case where the connection conditions of RIS [SIS] in RHR mode can be reached, the strategies are:

1) Primary boration by Emergency Boration System (RBS [EBS]) injection to maintain core sub-criticality;
2) Reactor coolant system cooldown via VDA [ASDS] of secondary side;
3) Reactor coolant system depressurization;
4) Connection of RIS [SIS] in RHR mode.

These operations are consistent with those of Small Break (Loss of Coolant Accident) (SB-LOCA).

For the case where the connection conditions of RIS [SIS] in RHR mode cannot be reached, the strategies are:

1) Primary boration by Emergency Boration System (RBS [EBS]) injection to maintain core sub-criticality;

2) Reactor coolant system cooldown via VDA [ASDS] secondary side;

12.9.5.2.1.5 Analysis Assumptions

a) Accident conditions

1) The break is conservatively assumed to be located in the cold leg between the pumps and the reactor pressure vessel. Surge line break located on hot leg can be bounded by this condition;

2) Break size sensitivity analyses (equivalent diameter up to 28.4 cm) are performed.

b) Initial condition assumptions

The break is assumed to be located on the cold leg of the reactor coolant system. Assumptions for the initial conditions are shown as follows:

1) The reactor initial power is the nominal power plus the maximum uncertainty. of the steady state measurement. The higher initial thermal power is, the more the residual heat will be generated during the transient;

2) The initial coolant flowrate is the thermal-hydraulic design flowrate, which is considered to penalize heat removal;

3) The average temperature of the coolant is the rated value plus the maximum steady state control range and measurement error;

4) The initial pressuriser pressure is the rated value plus the maximum uncertainty. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant. Additionally, the actuation of RIS [SIS] and reactor trip is delayed with a higher initial primary pressure;

5) The initial pressuriser level is the rated level at power minus 7% based on uncertainties. Because the less the initial level is, the less initial inventory is;

6) The total core bypass flow rate takes the maximum value (6.5%) to minimise the flow rate passing through the core.

c) Core-related assumptions

In the system thermal-hydraulic analysis, the core is simulated as a typical core with a severe axial power distribution.

For the hot rod analysis, the core enthalpy rise factor $F_{\Delta H}$ is set at its maximum value, and the hot spot factor F_Q is set at its maximum value.

In the short term analysis, Term A is calculated based on the specific neutronic data by LOCUST-K. The decay heat of actinides and fission products in Term B+C, given by LOCUST-K, meets the requirements in the Appendix K of 10 CFR 50, in which the decay heat of fission products is assumed to be 1.2 times of the value for infinite operating time in the ANS standard (October 1971).

In the long term analysis, the conservative decay heat data is used to maximise primary heat.

d) LOOP assumption

Loss of Offsite Power (LOOP) is assumed to occur at the time of turbine trip, considered as a consequential event of turbine trip. LOOP leads to the loss of power supply to all reactor coolant system pumps, feedwater pumps and condensate pumps. The protection and safety systems are able to perform the safety functions since these systems can be supplied by Emergency Diesel Generator (EDG). Therefore, the main effects of LOOP are coasting down of RCPs and delay of safety systems.

e) Single failure

For Intermediate Break and up to Surge Line Break - Loss of Coolant Accident, the most important safety system is RIS. Hence, single failures related to RIS are considered.

The failure of one safety injection train (including accumulator) on the intact loop is considered as single failure, which is caused by the check valve failure of the intact loop injection line [6]. As another train is assumed to be lost due to the break (located at safety injection point), only one safety injection train (1MHSI+1LHSI+1Accumulator) is taken into account for the RIS [SIS].

This assumption penalizes the water inventory and heat removal from primary side.

12.9.5.2.1.6 Result and Conclusions

a) From the initiating event to the controlled state

The most conservative burn-up assumption for PCT is BOL, and the highest PCT is 619 ℃. The most conservative burn-up assumption for oxidation ratio is EOC3, and the highest oxidation ratio is 3.8% (including initial oxidation ratio of EOC3). The detailed analysis of this fault (see Reference [56]) shows that the criteria are met.

b) From the controlled state to the safe state

The safe state is reached with the operation in Sub-section 12.9.5.2.1.4. 30 minutes after the reactor trip signal, the manual action from the MCR is assumed to take place. The LHSI pumps to the simultaneous injection to the cold leg and hot leg is switched 5409 seconds after break.

c) Radiological Consequence

The radiological release characteristics of this accident is the same with LB-LOCA, however the latter would result a higher containment pressure, and the degree of fuel failure is worse. The radiological consequence can be bounded by the accident of large break-loss of coolant accident.

The source term and radiological consequence of LB-LOCA is analysed in Sub-section 12.11.4.8.

12.9.5.2.2 Intermediate Break and up to Surge Line Break (State B)

12.9.5.2.2.1 Initiating Event

The intermediate break and up to surge line break LOCA (State B) can be divided into two conditions regarding to the availability of accumulators.

For cases with the initial primary pressure higher than { }, the accumulators are not isolated. Here, the safety functions available are the same as those for cases in State A, while the residual heat in the primary coolant and the core power are both lower and so the analysis in Sub-section 12.9.5.2.1.1 bounds this condition.

For cases with the initial primary pressure lower than { }, the accumulators are isolated. This condition is analysed in this section. The following differences in terms of FC1 mitigation methods, when compared to state A, are considered:

a) The triggering signal of SI signal.

b) The isolation of accumulators.

12.9.5.2.2.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

d) The ability to cool the core geometry shall be maintained, i.e. calculated changes

in core geometry shall be such that the core remains amenable to cooling;

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

12.9.5.2.2.3 Main Safety Functions

In this event, FC1 safety functions to achieve controlled state and FC2 safety functions to reach safe state are listed below:

a) FC1 safety functions

1) ARE [MFFCS] low load line isolation

Following the signal, SG level (narrow range) high 0 after reactor trip, ARE [MFFCS] low load lines of all SGs are isolated.

2) MHSI and LHSI startup

MHSI and LHSI are actuated when receiving SI signal is triggered by the "Hot leg $\triangle P_{sat}$ low 1"signal.

3) ASG [EFWS] startup

It is triggered by the "SG level (wide range) low 2" signal.

4) Medium pressure rapid cooldown (MCD)

Following the SI signal, a MCD is initiated to cool the primary circuit with a rate of { }.

5) Stop of Reactor Coolant Pumps

The shutdown of reactor coolant pumps is triggered by the "RCP ΔP low 1 and SI signal" signal.

6) Opening of Atmospheric Steam Dump System (VDA [ASDS])

The VDA [ASDS] valves automatically open when the secondary pressure reaches the VDA [ASDS] setpoint.

b) FC2 safety functions

These functions are all manual actions in the main control room.

1) Reactor coolant system boration

The RBS [EBS] pumps are started by the operator before the reactor coolant system cooldown for reactor coolant system boration.

2) Reactor coolant system cooldown by SGs

The cooldown is performed via the VDA [ASDS] of secondary side for primary depressurization.

3) MHSI stop

The MHSI pumps are shut down for primary depressurization.

4) Accumulators isolation

Accumulators need to be isolated to prevent nitrogen coming into reactor coolant system.

5) RIS [SIS] in RHR mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

6) Switch the LHSI pumps to simultaneous injection to the cold leg and hot leg

The connection of this function guarantees a continuous heat removal and core long-term cooling.

12.9.5.2.2.4 Typical Events Sequences

a) From the initiating event to the controlled state

An IB-LOCA in normal shutdown state where the RIS [SIS] in RHR mode is not connected induces a loss of coolant inventory. As it is assumed not compensable by the RCV [CVCS], it results in an abrupt RCP [RCS] pressure and pressuriser level decrease with a possible core heat up.

The safety injection (SI) signal is emitted on “Hot leg ΔPsat low 1” signal, inducing the following actions:

1) Starting of medium head safety injection (MHSI) and low head safety injection (LHSI) pumps;

2) Medium pressure rapid cooldown (MCD) realised through a controlled lowering of the main steam bypass system (GCT [TBS]) (if available) or of the atmospheric steam dump system (VDA [ASDS]) setpoints;

3) Containment isolation stage: the reactor coolant pressure boundary is isolated, in particular the RCV [CVCS] letdown line and the steam generator (SG) blowdown lines are isolated.

Reactor coolant pumps (RCPs) are tripped by the “ΔP low 1 over two RCPs” signal cumulated with the “Safety injection” signal.

As long as the SI flowrate does not compensate for the break flowrate, RCP [RCS] coolant water inventory continues to decrease. During this phase the break flow is subsaturated and eventually reaches saturation conditions.

The break flowrate decreases as the void fraction in the affected leg increases. Eventually, the break flow changes to single steam phase. The primary coolant

inventory depletion stops when the SI flowrate compensates for the break flowrate. If the accident occurred before the isolation of the accumulators by the operator, they may discharge their content of borated water into the RCP [RCS]. Later on, the controlled state is reached. This corresponds to the achievement of stable heat removal conditions via the operation of MHSI and the GCT [TBS] or VDA [ASDS] of all SGs, core sub-criticality and a stabilised or increasing core coolant inventory through use of the SI. The feedwater supply is ensured by the SG main feedwater system (ARE [MFFCS]) or the emergency feedwater system (ASG [EFWS]) if ARE [MFFCS] is not available.

b) From controlled state to safe state

The safe shutdown and the way to reach the safe state from the controlled state are the same as in state A, see Sub-section 12.9.5.2.1.4.

12.9.5.2.2.5 Analysis Assumptions

a) Accident conditions

1) The break is conservatively assumed to be located in the cold leg between the pumps and the reactor pressure vessel. Surge line break located on hot leg can be bounded by this condition;

2) Break size sensitivity analyses (equivalent diameter up to 28.4 cm) are performed.

b) Initial condition assumptions

The main concern is to maximise the heat in the core, minimise capacity of heat removal and penalize the PCT.

1) The decay heat during the transient is assumed to be constant for conservative consideration. This constant is the decay heat 4 hours after reactor shutdown considering +2σ of uncertainty, which is the shortest time to operate the plant from full power to state B. The higher initial thermal power is, the more the residual heat will be generated during the transient;

2) The initial primary flow rate is the thermal-hydraulic design flow rate, which is considered to penalize heat removal;

3) The maximum pressure of the state B operating domain is chosen and the maximum uncertainty is considered. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant. Additionally, the actuation of RIS [SIS] is delayed with a higher initial primary pressure;

4) The average temperature of the coolant is the value which complies with Net Positive Suction Head Required (NPSHr) curve (T = Tsat – 40 ℃, Tsat is

saturation temperature corresponding to the initial primary pressure), plus the maximum uncertainty, which is considered to maximise primary heat;

5) The initial water level of the pressuriser is the rated level in state B minus maximum uncertainty, which is considered to penalize the primary mass. Because the less initial level means that the initial inventory is less;

6) The total core bypass flow rate takes the maximum value (6.5%) to minimise the flow rate passing through the core.

c) Core-related assumptions

In the system thermal-hydraulic analysis, the core is simulated as an average core with a severe axial power distribution.

In the hot rod analysis, the core enthalpy rise factor $F_{\Delta H}$ is set at its maximum value, and the hot spot factor F_Q is set at its maximum value. The decay heat is conservatively assumed to be constant, which equal to the initial thermal power.

d) LOOP assumption

The Loss of Offsite Power (LOOP) is not considered as the turbine is stopped under state B.

e) Single Failure

For Intermediate Break and up to Surge Line Break - Loss of Coolant Accident, the most important safety system is RIS. Hence, single failures related to RIS are considered.

The failure of one safety injection train on the intact loop is considered as single failure, which is caused by the check valve failure of the intact loop injection line. As another train is assumed to be lost due to the break (located at safety injection point), only one safety injection train (1MHSI+1LHSI) is taken into account for the RIS [SIS].

This assumption penalizes the water inventory and heat removal from primary side.

12.9.5.2.2.6 Result and Conclusions

a) From the initiating event to the controlled state

The detailed analysis of this fault (see Reference [56]) shows that the criteria are met.

The analysis result of the break spectrum shows that, for the break conditions with the equivalent diameters from 7.5 cm to 28.4 cm, no significant core heat-up occurs. The most conservative break size is 7.5cm, which appears the highest PCT.

b) From the controlled state to the safe state

The safe shutdown and the way to reach the safe state from the controlled state are the

same as in state A, see Sub-section 12.9.5.2.1. The safe state is reached with the operation in Sub-section 12.9.5.2.2.4.

c) Radiological Consequence

The radiological release characteristics of this accident is the same with LB-LOCA, however the latter would result a higher containment pressure, and the degree of fuel failure is worse. The radiological consequence can be bounded by the accident of large break-loss of coolant accident.

The source term and radiological consequence of LB-LOCA is analysed in Sub-section 12.11.4.8.

12.9.5.2.3 Inherent Boron Dilution Risk Assessment

The risk of inherent boron dilution may occur during a LOCA, after trip of the reactor coolant pumps. Inherent boron dilution refers to the unborated water slug somewhere in the primary circuit, which enters the core as the natural circulation is restarted, thereby causing the risk of re-criticality of the core.

This phenomenon is studied and assessed. The boron dilution analysis methods are mainly divided into three successive parts (thermal hydraulic system analysis, mixing analysis and safety margin analysis). The thermo-hydraulic system code LOCUST is used to analyse the behaviour of reactor coolant system and provide initial and boundary conditions. The mixing effect of the unborated water slug and coolant is calculated and the concentration of boron at the core inlet is given by the Computational Fluid Dynamics code. Finally, the calculated minimum boron concentration at the core inlet is compared with the critical boron concentration to evaluate the subcritical margin to re-criticality.

The coupling analysis results show that, for inherent heterogeneous boron dilution, the recriticality will not be reached during the transient. The detailed information is presented in Reference [57].

12.9.5.3 Small Break - Loss of Coolant Accident (State B)

12.9.5.3.1 Initiating Event

A small break loss of coolant accident (SB-LOCA) is defined as an accident in which a small break occurs on the pipes of the reactor coolant system or on the upstream line of the second isolation valve connected to it.

A SB-LOCA on the RCP [RCS] induces a loss of coolant inventory, potential pressure decrease of the RCP [RCS] and potential core overheating.

The small break loss of coolant accident (at shutdown conditions) can be divided into two conditions regarding to the availability of accumulators.

For cases with the hot leg pressure higher than { }, the accumulators are not isolated. In this case, the Safety Injection (SI) can be actuated by the "Hot leg ΔP_{sat} low 1" signal, while the SI is actuated by the "Pressuriser pressure low 3" signal in state A. The availability of safety functions in this cases are the same as those in state A. And, the residual heat in the primary coolant and the core power of this case is lower than that in state A. Therefore, the analysis of this case is bounded by those in state A in Sub-section 12.8.5.3.1.

For cases with the hot leg pressure lower than { }, the accumulators are isolated. This condition is analysed in this section. The following differences in terms of FC1 mitigation methods are considered compared to state A:

a) The change of SI signal.

b) The isolation of accumulators.

12.9.5.3.2 Acceptance Criteria

The SB-LOCA analyses should meet the following acceptance criteria:

a) The peak cladding temperature shall not exceed 1204℃;

b) Maximum clad oxidation. The total oxidation of the cladding at the limiting point shall not exceed 17% of the total clad thickness before oxidation;

c) Maximum hydrogen generation. The total amount of hydrogen generated from the chemical reaction of the cladding with water or steam shall not exceed 1% of the amount that would be generated if all of the cladding material in the active core, were to react;

d) Coolable geometry. Changes in core geometry shall be such that the core remains capable of being cooled;

e) Long-term cooling. After any successful initial operation of the Emergency Core Cooling System (ECCS), the core temperature shall be maintained at an acceptably low value and decay heat shall be removed for the extended period of

time required by the long-lived radioactivity remaining in the core.

12.9.5.3.3 Main Safety Functions

For this event, the following plant safety functions can mitigate the event:

a) Safety injection (SI) signal is actuated by:

"Hot leg ΔP_{sat} low 1" signal;

b) Medium pressure rapid cooldown (MCD) is actuated by:

SI signal;

c) The reactor coolant pumps (RCPs) are tripped by:

"RCP ΔP low 1 and SI" signal;

d) ASG [EFWS] is started-up by

"SG level (wide range) low 2" signal;

e) ASG [EFWS] is isolated by

"SG level (wide range) high 1" signal;

f) ARE [MEFCS] low load line is isolated by

"SG level (narrow range) high 0" signal.

12.9.5.3.4 Typical Events Sequences

The SB-LOCA in state B is classified as a DBC-3 event. A typical sequence of events is described below.

a) From the initiating event to controlled state

A SB-LOCA in state B can induces a loss of coolant inventory. If this loss cannot be complemented by the Chemical and Volume Control System (RCV [CVCS]), it will result in a decrease in the Reactor Coolant System pressure and potential core heat-up.

With Reactor Coolant System depressurizing, the hot leg saturation margin ΔP_{sat} decrease. When the hot leg saturation margin ΔP_{sat} reaches "Hot leg ΔP_{sat} low 1" setpoint, the SI signal is triggered.

Following the SI signal, the MHSI and the Low Head Safety Injection (LHSI) pumps are started-up and the MCD is actuated. The MCD cools the Reactor Coolant System with a rate of{ } by decreasing the setpoint of VDA [ASDS]. After MCD, the Reactor Coolant System pressure decreases sufficiently to allow MHSI pumps injection into the cold legs.

After blowdown and MCD phase, the primary pressure stabilises to a value that is higher or equal to the secondary side pressure. If the safety injection flow cannot

compensate for the break flowrate, RCP [RCS] coolant water inventory continues to decrease.

The break flowrate decreases as the void fraction in the broken cold leg increases. Eventually, the SI flowrate is able to compensate for the break flowrate.

Then, the controlled state is reached. It corresponds to the achievement of stable heat removal conditions, via the operation of the MHSI and the GCT [TBS] or VDA [ASDS] of all SGs, core sub-criticality and a stabilised or increasing core coolant inventory due to SI flow. The feedwater supply is ensured by the SG main feedwater system or the ASG [EFWS] if ARE [MFFCS] is not available.

b) From Controlled State to Safe State

The controlled state cannot be sustained due to the following reasons:

1) The ASG [EFWS] system tanks will empty;

2) The containment pressure and temperature will increase.

Thus, the transition to safe state is needed. The safe state is reached through several key means:

1) RCP [RCS] boration to keep core sub-criticality;

2) RCP [RCS] cooling to ensure LHSI injection;

3) RCP [RCS] depressurisation to reach RHR connection condition;

4) RHR connection.

12.9.5.3.5 Analysis Assumptions

The detailed assumptions are presented in Reference [58]. The main assumptions are listed as follows:

a) Initial conditions

1) The core power during the transient is assumed to be constant for conservative consideration. This constant is the decay heat 4 hours after reactor shutdown considering + 2σ of uncertainty, which is the shortest time to operate the plant from full power to state B.

2) The initial coolant flowrate is the thermal-hydraulic design flowrate, which minimises heat removal.

3) The average temperature of the coolant is the value which complies with Net Positive Suction Head Required curve (T = Tsat – 40 ℃, Tsat is saturation temperature corresponding to the primary pressure), with the maximum uncertainty considered, which maximises primary stored energy.

4) The initial hot leg pressure is the value which is corresponding to the maximise value of isolating accumulators, with the maximum uncertainty considered, which maximises mass flow rate at the break.

5) The initial level of the pressuriser is the rated level minus uncertainties, which minimises the initial inventory.

b) Core-related assumptions

The decay heat of actinides and fission products in Term B+C, given by LOCUST-K, meets the requirements in the Appendix K of 10 CFR 50, in which the decay heat of fission products is assumed to be 1.2 times of the value for infinite operating time in the ANS standard (October 1971).

c) LOOP assumptions

Since the turbine has already been stopped, the Loss of Offsite Power (LOOP) is not considered in this case.

d) Single failure

The failure of one SI train on the intact loop is considered as single failure, which is caused by the check valve failure of the intact loop injection line. This assumption penalizes the water inventory and the heat removal from primary side.

Furthermore, another train of SI, located on the broken loop, is conservatively assumed to be lost through the break.

Thereby, only one train of SI is effective in short-term analysis.

12.9.5.3.6 Results and Conclusions

a) From the initiating event to the controlled state

The detailed analysis of this fault (see Reference [58]) shows that, for the SB-LOCA with an equivalent diameter of 5.0 cm in state B, the SI system can provide sufficient flow rates to compensate for the break flowrate and the core remains covered. Thus, the decoupled acceptance criteria are met.

b) From the controlled state to the safe state

The residual heat of the plant in Small Break Loss of Coolant Accident at State B is lower than that in Small Break Loss of Coolant Accident at State A.

And, the available safety function to achieve safe state from controlled state in SB-LOCA at State B is same as that in SB-LOCA at State A.

Therefore, the analysis from controlled to safe state of SB-LOCA in state B can be bounded by that in state A Sub-section 12.8.5.3.1.

c) Radiological Consequence

The radiological consequences for this event are covered by SB-LOCA in State A since the thermal state of primary coolant in state A is higher than that in state B. The source term and radiological consequence of SB-LOCA (state A) are analysed in Sub-section 12.11.4.3.

12.9.5.4 Small Break - Loss of Coolant Accident (State C\D\E)

A Small Break - Loss of Coolant Accident (SB-LOCA), defined as an accident in which a small break with equivalent diameter no larger than 5.0 cm, occurs on the pipes of the reactor coolant system or on the upstream line of the second isolation valve connected to it, and induces a loss of coolant inventory, thereby leading to a possible core heat-up.

During the nuclear power plant in state C\D\E operating mode, the heat in reactor coolant system is removed by the Safety Injection System (RIS [SIS]) in Residual Heat Removal (RHR) mode. The various states are described below:

a) When the RCP [RCS] temperature is between 100℃ and 140℃ (state C1), 2 trains of RIS [SIS] are used in RHR mode, and at least one RCP is running.

b) When the RCP [RCS] temperature is between 10℃ and 100℃ (state C2), at least 2 trains of RIS [SIS] are used in RHR mode and at least one RCP is running.

c) When the RCP [RCS] temperature is between 10℃ and 60℃ (state C3), at least 2 trains of RIS [SIS] are used in RHR mode. In the early phase of this state, at least one RCP is running, and in the later phase of this phase, all the RCPs are stopped.

d) When the RCP [RCS] temperature is between 10℃ and 60℃ (state D and state E), at least 2 trains of RIS [SIS] are used in RHR mode and all the RCPs are stopped.

12.9.5.4.1 SB-LOCA in state C with three RCPs are running

12.9.5.4.1.1 Initiating Event

A non-isolatable break with an equivalent diameter smaller than or equal to 5.0 cm (equivalent area smaller than or equal to 20 cm^2) on the pipes of the reactor coolant system or on the upstream line of the second isolation valve connected to it in state C\D\E, induces a loss of coolant inventory and an RCP [RCS] pressure decrease, thereby leading to a possible core heat-up.

The break is assumed to be located on safety injection point of the cold leg, and it is between the RCP and the reactor pressure vessel inlet. The injection flow of RIS [SIS] will leak from the break when the break is assumed to be located on safety injection point. Compared to the break in hot leg, the break in cold leg will penalize the capability of core cooling. Besides, the break is assumed to be located at the loop with pressuriser, which will penalize the primary water inventory. Due to this assumption, the SI in the broken loop is considered to be lost and the pressuriser water inventory tends to be directly discharged through the break.

A break with an equivalent diameter of 5.0 cm is considered.

SB-LOCA in state C\D\E is classified as a DBC-4 event.

12.9.5.4.1.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The peak cladding temperature must remain lower than 1204℃;

b) The maximum cladding oxidation must remain lower than 17% of the total cladding thickness before oxidation;

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

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

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

However, if the core remains covered during the transient, the above criteria are considered to be met. Thus the consequences of SB-LOCA in state C\D\E are analysed against the following aspects:

a) Core remains covered;

b) The plant shall be brought to and maintained in the controlled state;

c) The plant shall be brought to and maintained in the safe state.

12.9.5.4.1.3 Main Safety Function

In this analysis, FC1 and FC2 safety functions are listed below:

a) FC1 safety functions (automatic)

1) Safety injection (SI)

In state C1/C2, SI is triggered by the “Hot leg ΔPsat low 1” signal.

In state C3/D, SI is triggered by the “RCP [RCS] loop level low 1” signal.

In state E, SI is start up by operator.

2) Stop of Reactor Coolant Pump (RCP)

In state C1/C2/C3a, RCPs are stopped by the “RCP ΔP low 1 and SI” signal.

3) Stop of RIS [SIS] pump(s) in RHR mode

In state C1/C2, RIS [SIS] pumps in RHR mode are stopped by the “Hot leg

ΔPsat low 2” signal.

In state C3/D, RIS [SIS] pumps in RHR mode are stopped by the “RCP [RCS] loop level low 2” signal.

4) Opening of Atmospheric Steam Dump System (VDA [ASDS])

The VDA [ASDS] valves automatically open when the secondary pressure reaches the VDA [ASDS] setpoint.

5) Start-up of Emergency Feedwater System (ASG [EFWS])

In state C1, ASG [EFWS] are actuated by the “SG level (wide range) low 2” signal.

b) FC2 safety functions (manual from the main control room)

1) Reactor coolant system boration by Emergency Boration System [EBS] (RBS [EBS])

The RBS [EBS] pumps are started by the operator before the reactor coolant system cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

2) Reactor coolant system cooldown by Steam Generators (SGs)

The cooldown is performed via the VDA [ASDS] of secondary side.

3) Reactor coolant system cooldown by RIS [SIS] in RHR mode

- If the RIS [SIS] trains in RHR mode connection conditions can be re-established

  The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

- If the connection conditions of RIS [SIS] in RHR mode cannot be re-established

  The LHSI train is actuated in SI mode. After connection of LHSI in SI mode, the connection conditions of RIS/RHR can be reached. The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

12.9.5.4.1.4 Typical Events Sequences

The analysis of SB-LOCA in state C2\C3a\C3b\D\E can be enveloped by that in state C1 for the reasons as following:

a) The higher the initial power, the more the residual heat will be generated during the transient.

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

c) The higher the initial primary average temperature, the more the initial primary heat will be.

d) The smallest numbers of available RIS [SIS] are the same in state C1\ C2\C3a\C3b\D\E.

The transient of an event can be divided into two phases: the short-term phase to the controlled state and the long-term phase to the safe state. For this event, the controlled state is reached when the primary inventory recovers; the safe state is reached when the long-term core cooling is ensured.

Therefore, only the short-term phase and long-term phase of SB-LOCA in state C1 is analysed in this subsection.

The typical event sequences in state C1 described below refers to an event sequences that is most likely to occur during transient and takes into account operator actions and safety system actions.

a) From the Initiating Event to the Controlled State

For short term phase, following the break occurring, reactor coolant system pressure and pressuriser level may decrease if the loss of coolant cannot be compensated by the Chemical and Volume Control System (RCV [CVCS]). This can cause rapid drop of the reactor coolant system pressure and pressuriser level, as well as possible core heat up. Following actions or signals will be triggered:

1) SI is triggered by the “Hot leg ΔPsat low 1” signal.

2) RCP are stopped by the “RCP ΔP low 1 and SI” signal.

3) RIS [SIS] pumps in RHR mode are stopped by the “Hot leg ΔPsat low 2” signal.

Two situations could occur: RIS/RHR in operation; RIS/RHR are stopped. In both cases, the controlled state could be reached.

1) If the RIS [SIS] pumps in RHR mode are not tripped

If the RIS [SIS] pumps in RHR mode are not stopped, the RIS [SIS] pumps in RHR mode ensure reactor coolant system heat removal. The Medium Head Safety Injection (MHSI) compensates for the break flow and the reactor coolant system coolant inventory is stabilised, enabling progression to the controlled state.

2) If the RIS [SIS] pumps in RHR mode are tripped

With the trip of the RIS [SIS] pumps in RHR mode, the reactor coolant system

temperature increases and the secondary pressure increases slowly until the VDA [ASDS] setpoint is reached. The VDA [ASDS] valves open and remove heat from the reactor coolant system. Then the heat removal is ensured by VDA [ASDS], break flow and MHSI. The coolant inventory is compensated by MHSI. Finally, the reactor coolant system coolant inventory stabilizes, and the controlled state is reached.

b) From the Controlled State to the Safe State

For long-term phase, the safe state is defined as a state at which the break flow rate is compensated by the RIS [SIS] flow rate with long-term core cooling ensured.

1) If the RIS [SIS] pumps in RHR mode are not tripped:

Considering that the RIS [SIS] trains are operating in RHR mode, the safe state is reached as long as the controlled state has been reached.

2) If the RIS [SIS] pumps in RHR mode are tripped:

In order to reach the connection conditions of RIS [SIS] in RHR mode, the sequences of actions performed by the operator are as the following:

- Primary boration by RBS [EBS] injection to maintain core sub-criticality;
- Reactor coolant system cooldown via VDA [ASDS] of secondary side;
- Connection of RIS [SIS] in RHR mode.

If the RIS [SIS] trains in RHR mode connection conditions can be re-established, long-term core cooling can be ensured by RIS [SIS] trains in RHR mode, and the safe state is reached.

If the connection conditions of RIS [SIS] in RHR mode cannot be re-established, the operator should actuate the LHSI in SI mode. After connection of LHSI in SI mode, the connection conditions of RIS/RHR can be reached. This LHSI train could be switched to RHR mode. After connection of RIS/RHR, the safe state is reached.

12.9.5.4.1.5 Analysis Assumption

a) Analysis Codes

LOCUST V1.0.2 is a system thermal-hydraulic code which is used to simulate two-fluid, non-equilibrium, and heterogeneous hydrodynamic conditions in various nuclear power plant transients. LOCUST-K V1.0.1 is a conservative analysis code that is consistent with the requirements of Appendix K in 10 CFR 50, and it is developed on the basis of LOCUST.

For this transient analysis, LOCUST-K V1.0.1 is used for the short-term analysis with bounding initial plant conditions and pessimistic capacity of safety systems. LOCUST

V1.0.2 is used for the long-term analysis with bounding initial plant conditions and pessimistic capacity of safety systems.

b) Initial Conditions

1) The initial thermal power is assumed at the beginning of state C1 (i.e. at the earliest 11.5 hours after reactor shutdown). The higher initial thermal power, the more the residual heat will be generated during the transient.

2) The initial coolant flowrate is the thermal-hydraulic design flowrate, which is considered to penalize heat removal;

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

4) The initial pressure of the pressuriser is the rated value plus the maximum uncertainty. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant.

5) The initial level of the pressuriser is the rated level at state C1 minus 8.5% based on uncertainties. The lower the initial pressuriser level, the less initial primary inventory to cooled the core.

6) The total core bypass flow rate takes the maximum value (6.5%) to minimise the flow rate passing through the core.

7) There are two trains of RIS [SIS] located on unaffected loop can be used in state C1.

c) Core-related Assumptions

In the short term analysis, Term A is calculated based on the specific neutronic data by LOCUST-K. The decay heat of actinides and fission products in Term B+C, given by LOCUST-K, meets the requirements in the Appendix K of 10 CFR 50, in which the decay heat of fission products is assumed to be 1.2 times of the value for infinite operating time in the ANS standard (October 1971).

d) Protection Signals

1) “Hot leg ΔPsat low 1” signal

The maximum positive uncertainty of the “Hot leg ΔPsat low 1” signal setpoint is taken into consideration bring into correspondence with the “Hot leg ΔPsat low 2” logically. However, the maximum delay time is taken into consideration to penalize heat removal by RIS [SIS] as much as possible.

2) “Hot leg ΔPsat low 2” signal

The maximum uncertainty and minimum delay time of the “Hot leg ΔPsat low 2” signal setpoint are taken into consideration to benefit the residual heat

be generated in early time.

3) "RCP ΔP low 1" signal

The maximum negative uncertainty and maximum delay time of the "RCP ΔP low 1"signal are taken into consideration to maximise primary heat from RCPs.

4) "SG level (wide range) low 2"

The maximum negative uncertainty and maximum delay time is taken into account to penalize heat removal by SGs.

5) VDA [ASDS] setpoint

The maximum positive uncertainty and maximum delay time is taken into account to delay the actuation of the VDA [ASDS] to maximise primary pressure, which is considered to maximise the mass flow rate at the break and minimise the MHSI flowrate.

e) System Performance

For short-term phase, FC1 safety functions are taken into consideration as following:

1) MHSI of RIS [SIS]

The RIS [SIS] is designed of 3 redundant trains (no connection between any two of trains). With the most conservative assumption, the injection flow from RIS [SIS] located on affected loop will leak from the break; one train of RIS [SIS] located on unaffected loop cannot work as single failure, only one train of RIS [SIS] will be used in this analysis.

The minimum SI flow rate is assumed, and the In-containment Refuelling Water Storage Tank (IRWST) temperature is maximised in order to minimise the ability to cool the core.

2) ASG [EFWS]

All the three trains of ASG [EFWS] are used in this analysis. The minimum feedwater flow rate and maximum feedwater temperature is assumed in order to minimise the ability to cool the core.

3) VDA [ASDS]

VDA [ASDS] consists of three independent redundant trains. All the three trains of VDA [ASDS] will be used in this analysis.

f) Single Failure Assumption

For this analysis, the most important safety system is RIS [SIS]. Hence, single failures related to RIS [SIS] are considered.

The failure of one safety injection train is assumed. As another train is assumed to be lost due to the break (located at safety injection point), only one MHSI is taken into account for the RIS [SIS].

This assumption penalizes the water inventory and heat removal from primary side. It penalizes core heat-up and limits the primary cooling.

g) Loss of Offsite Power (LOOP) Assumption

LOOP is not considered as it is assumed a consequence of turbine trip, and no turbine trip will occur in state C\D\E.

12.9.5.4.1.6 Result and Conclusions

Based on the method and assumption above, the short-term phase and long-term phase analysis results of SB-LOCA in sate C1 as following:

a) From the initiating event to the controlled state

The detailed analysis of this fault (see Reference [59]) shows that during the accident, the primary water inventory is maintained without exposing the core and the core heat is removed via the break and SI. The relevant safety acceptance criteria are thus met.

b) From the controlled state to the safe state

The analysis results of SB-LOCA in state C\D\E show that the primary coolant inventory is maintained and the core always remains covered for both short term and long term, the RIS [SIS] train in RHR mode connection conditions can be re-established for long term. As a result, the controlled state and the safe state can be reached.

c) Radiological Consequence

The radiological consequences for this event are covered by SB-LOCA in State A since the thermal state of primary coolant in state A is higher than that in state C\D\E. The source term and radiological consequence of SB-LOCA (state A) are analysed in Sub-section 12.11.4.3.

12.9.5.4.2 Small Break (in Shutdown State, RIS [SIS] Connected in RHR Mode) (One RCP or No RCP is Running)

Compared with the RCP [RCS] operating conditions, the primary initial temperature, pressure, and initial core power are lower under this condition, and the normal system protection function assumption is the same as in Sub-section 12.9.5.5.1. The accident analysis results can be covered by the analysis specified in Sub-section 12.9.5.5.1.

12.9.5.5 RHR System Piping Break inside or outside Containment (State C\D\E)

12.9.5.5.1 RHR System Piping Break inside Containment

12.9.5.5.1.1 Description

If a break occurs on the RIS [SIS] system inside containment, it leads to a loss of primary coolant inventory and a discharge of radioactive primary fluid into the containment. The studied accident is due to an isolatable break on one RIS [SIS] line during RHR mode operation, with an equivalent size smaller than or equal to DN250 (with a nominal diameter of 250 mm). The isolatable break inside containment can be located:

a) Downstream of the RIS [SIS] isolation valve which is the second closest to the RCP [RCS] on the RIS [SIS] suction line connected to an RCP [RCS] hot leg;

b) Upstream of the check valve which is the second closest to the RCP [RCS] on the RIS [SIS] injection line connected to an RCP [RCS] cold leg.

Austenitic stainless steels are used for the parts of the RCP [RCS] in contact with the primary coolant because of their high resistance to generalised corrosion at the service temperature and in conditions of cold shutdown. Precautions are taken to avoid any other localised corrosion, by conditioning of the primary coolant and appropriate chemical composition of the materials. With regards to pitting, the chloride content and oxygen content of the primary coolant is controlled to avoid this form of corrosion during service. This conditioning of the primary coolant also promotes resistance of the stainless steel to corrosion cracking.

The risk of breaks caused by corrosion on the RIS [SIS] is therefore reduced.

If a break occurs on the RIS [SIS] system inside containment, it may lead to a decrease in reactor coolant inventory, a discharge of radioactive primary fluid into the containment and potential core overheating.

The transient of an event can be divided into two phases: the short-term phase to controlled state and the long-term phase to safe state. For this event, the controlled state is reached when the primary inventory recovers; the safe state is reached when the long-term core cooling is ensured. For both phases, the analysis of RHR-LOCA in state C2\C3a\C3b\D\E can be enveloped by that in state C1 for the reasons as following:

a) The initial power in state C1 is higher, resulting in more residual heat generated during the transient.

b) The initial primary pressure is higher, resulting in higher mass flow rate at the break and the faster the loss of primary coolant.

c) The initial primary average temperature is higher, resulting in more initial stored

energy.

d) The capability of available MHSI are the same in state C1\ C2\C3a\C3b\D\E.

Therefore, only the short-term phase and long-term phase of RHR-LOCA in state C1 is analysed.

12.9.5.5.1.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

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

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

However, if the core remains covered during the transient, above criteria are considered to be met. Thus the consequences of RHR-LOCA are analysed against the following aspects:

a) Core remains covered;

b) The plant shall be brought to and maintained in controlled state;

c) The plant shall be brought to and maintained in safe state.

12.9.5.5.1.3 Main Safety Functions

In this analysis, FC1 and FC2 safety functions are listed below:

a) FC1 safety functions

1) Safety injection (SI)

In state C1/C2, SI is triggered by the “Hot leg ΔP_{sat} low 1” signal.

In state C3/D/E, SI is triggered by the “RCP [RCS] loop level low 1” signal.

2) Stop of Reactor Coolant Pumps (RCPs)

In state C1/C2/C3a, RCPs are stopped by the “RCP ΔP low 1 and SI” signal.

3) Stop of RIS [SIS] pump(s) in RHR mode

In state C1/C2, RIS [SIS] pumps in RHR mode are stopped by the "Hot leg ΔP_{sat} low 2" signal.

In state C3/D/E, RIS [SIS] pumps in RHR mode are stopped by the "RCP [RCS] loop level low 2" signal.

4) Isolation of RHR train suction line from hot leg

In state E, isolation of RHR train suction line from hot leg can also be triggered by the "Reactor pool level low 1" signal.

b) FC2 safety functions

The main operator actions encompass:

1) Reactor coolant system cooldown by Steam Generators (SGs)

The cooldown is performed via the Atmospheric Steam Dump System (VDA [ASDS]) of SGs.

2) Startup of Emergency Feedwater System (ASG [EFWS])

ASG [EFWS] is actuated to control the SGs water level.

3) Isolation of RHR train suction line from hot leg

Isolation of RHR train suction line from hot leg are performed and the break is therefore isolated.

4) Medium Head Safety Injection (MHSI) stop

The operator stops the MHSI pumps when the pressuriser level is sufficient, since the water inventory could be guaranteed due to the break isolation.

5) Reactor coolant system integrity check

The operator performs the reactor coolant system integrity check to identify which LHSI/RHR train is broken.

6) RIS [SIS] train in RHR mode re-established

Since the ruptured RHR system pipe is isolated via reactor coolant system integrity check, the RIS [SIS] train in RHR mode connection conditions can be re-established by operator via SGs.

12.9.5.5.1.4 Typical Events Sequences

a) From the initiating event to the controlled state

For short term phase, the break leads to rapid drop of the reactor coolant system pressure and pressuriser level, as well as possible core heat up. Following actions or

signals will be triggered:

1) Safety Injection (SI) is triggered by the "Hot leg ΔP_{sat} low 1" signal.

2) RCPs are stopped by the "RCP ΔP low 1 and SI" signal.

3) RIS [SIS] pump is stopped by the "Hot leg ΔP_{sat} low 2" signal.

Two situations could occur: RIS/RHRs remain in operation; RIS/RHRs are stopped. In both cases, the controlled state could be reached.

1) If the RIS [SIS] pumps in RHR mode are not tripped:

If the RIS [SIS] pumps in RHR mode are not stopped, the RIS [SIS] pumps in RHR mode ensure reactor coolant system heat removal. The MHSI compensates for the break flow and the reactor coolant system water inventory is stabilised, enabling progression to controlled state.

2) If the RIS [SIS] pumps in RHR mode are tripped:

Following the trip of the RIS [SIS] pumps, the decay heat can be removed by the break flow and the SGs, depending on the break size and the plant state. The reactor coolant system water inventory is restored and stabilised by MHSI and the controlled state is then reached.

b) From controlled state to safe state

For long-term phase, since the break can be isolated from the reactor coolant system by operator actions, the safe state is defined as a state for which the ruptured RHR train is detected through reactor coolant system integrity check and heat removal can be ensured until the RIS [SIS] trains in RHR mode can be re-established.

1) If the RIS [SIS] pumps in RHR mode are not tripped:

Considering that the RIS [SIS] trains are operating in RHR mode, the safe state may be reached as long as the controlled state has been achieved.

2) If the RIS [SIS] pumps in RHR mode are tripped:

In order to reach the connection conditions of RIS [SIS] in RHR mode, the sequences of actions performed by the operator are as the following:

- Reactor coolant system cooldown by SGs
- Startup of ASG [EFWS]
- Isolation of RHR train suction line from hot leg
- Stop of MHSI
- Reactor coolant system integrity check/ break isolation:

- The RIS [SIS] train in RHR mode connection conditions is re-established.

12.9.5.5.1.5 Analysis Assumptions

The detailed assumptions are presented in Reference [60]. The main assumptions are listed as follows:

a) Initial conditions

1) The initial thermal power is assumed to be the largest decay heat of state C1. The higher initial thermal power is, the more the residual heat will be generated during the transient;

2) The initial coolant flowrate is the thermal-hydraulic design flowrate, which is considered to penalize heat removal;

3) The hot leg temperature of the coolant is the maximum value in state C1 plus the maximum uncertainty, which is considered to maximise stored energy;

4) The initial pressure of the pressuriser is the maximum value in state C1 plus the maximum uncertainty. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant.

5) The initial level of the pressuriser is the rated level in state C1 minus maximum uncertainties. The lower the initial pressuriser level, the less initial primary inventory to cooled the core.

6) The total core bypass flow rate takes the maximum value to minimise the flow rate passing through the core.

b) Core-related assumptions

The decay heat is conservatively assumed to be constant, which equal to the initial core power.

c) LOOP assumption

Since turbine has already been stopped, Loss of Offsite Power (LOOP) is not considered in this case.

d) Single failure

For this analysis, the most important safety system is RIS [SIS]. Hence, single failures related to RIS [SIS] are considered. It is assumed that the single failure occurs on the one MHSI pump on unaffected loop.

This assumption penalizes the water inventory and heat removal from primary side. It penalizes core heat-up and limits the primary cooling.

12.9.5.5.1.6 Results and Conclusions

a) From the initiating event to the controlled state

The detailed analysis of this fault (see Reference [60]) shows that the core remains covered, so the acceptance criteria are not challenged.

b) From controlled state to safe state

The detailed analysis of this fault (see Reference [60]) shows that, the plant can be taken to safe state. The RIS [SIS] train in RHR mode connection conditions can be re-established after coolant inventory restoration. The long-term phase analysis result shows that, the core remains covered during the transient, so the acceptance criteria are not challenged.

c) Radiological Consequence

The radiological release characteristics of this accident is the same with LB-LOCA, however the latter would result a higher containment pressure, and the degree of fuel failure is worse. The radiological consequence can be bounded by the accident of large break-loss of coolant accident.

The source term and radiological consequence of LB-LOCA is analysed in Sub-section 12.11.4.8.

12.9.5.5.2 RHR System Piping Break outside Containment

12.9.5.5.2.1 Description

If a break occurs on the RIS [SIS] system outside containment, it leads to a loss of primary coolant inventory and a discharge of radioactive primary fluid into the safeguard building. The studied accident is due to an isolatable break on one RIS [SIS] line during RHR mode operation, with an equivalent size smaller than or equal to DN250 (with a nominal diameter of 250 mm). The isolatable break outside containment can be located:

a) Downstream of the RIS [SIS] isolation valve which is the second closest to the RCP [RCS] on the RIS [SIS] suction line connected to an RCP [RCS] hot leg;

b) Upstream of the check valve which is the second closest to the RCP [RCS] on the RIS [SIS] injection line connected to an RCP [RCS] cold leg.

The precautions limiting the transient are the same as for a break inside containment, described in Sub-section 12.9.5.5.1.

The transient of an event can be divided into two phases: the short-term phase to controlled state and the long-term phase to safe state. For this event, the controlled state is reached when the primary inventory recovers; the safe state is reached when the long-term core cooling is ensured. For both phases, the analysis of RHR-LOCA in

state C2\C3a\C3b\D\E can be enveloped by that in state C1 for the reasons as following:

a) The initial power in state C1 is higher, resulting in more residual heat generated during the transient.

b) The initial primary pressure is higher, resulting in higher mass flow rate at the break and the faster the loss of primary coolant.

c) The initial primary average temperature is higher, resulting in more initial stored energy.

d) The capability of available MHSI are the same in state C1\ C2\C3a\C3b\D\E.

Therefore, only the short-term phase and long-term phase of RHR-LOCA in state C1 is analysed.

When the break is located outside the containment, the release of fluid in the safeguard building could lead to the automatic isolation of RHR train suction line from hot leg either by "Safeguard building sump level high 1" signal or by "Safeguard building pressure rise high 1" signal. The automatic isolation of the RHR train on the cold leg side is done after closure of the check valves.
Even though the automatic isolation of RHR train suction line from hot leg is not triggered, the break isolation can be done by reactor coolant system integrity check.

Therefore, the core consequences of RHR-LOCA outside containment can be enveloped by that of RHR-LOCA inside containment (Sub-section 12.9.5.6.1).

12.9.5.5.2.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak Cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

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

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

However, if the core remains covered during the transient, above criteria are considered to be met. Thus the consequences of RHR-LOCA are analysed against the

following aspects:

a) Core remains covered;

b) The plant shall be brought to and maintained in controlled state;

c) The plant shall be brought to and maintained in safe state.

12.9.5.5.2.3 Main Safety Functions

In this analysis, FC1 and FC2 safety functions are listed below:

a) FC1 safety functions

1) Safety injection (SI)

In state C1/C2, SI is triggered by the "Hot leg ΔP_{sat} low 1" signal.

In state C3/D/E, SI is triggered by the "RCP [RCS] loop level low 1" signal.

2) Stop of Reactor Coolant Pumps (RCPs)

In state C1/C2/C3a, RCPs are stopped by the "RCP ΔP low 1 and SI" signal.

3) Stop of RIS [SIS] pump(s) in RHR mode

In state C1/C2, RIS [SIS] pumps in RHR mode are stopped by the "Hot leg ΔP_{sat} low 2" signal.

In state C3/D/E, RIS [SIS] pumps in RHR mode are stopped by the "RCP [RCS] loop level low 2" signal.

4) Isolation of RHR train suction line from hot leg

In state C/D/E, isolation of RHR train suction line from hot leg can be triggered either by "Safeguard building sump level high 1" signal or "Safeguard building pressure rise high 1" signal.

In state E, isolation of RHR train suction line from hot leg can also be triggered by the "Reactor pool level low 1" signal.

b) FC2 safety functions

The main operator actions encompass:

1) Reactor coolant system cooldown by Steam Generators (SGs)

The cooldown is performed via the Atmospheric Steam Dump System (VDA [ASDS]) of SGs.

2) Startup of Emergency Feedwater System (ASG [EFWS])

ASG [EFWS] is actuated to control the SGs water level.

3) Isolation of RHR train suction line from hot leg

Isolation of RHR train suction line from hot leg are performed and the break is therefore isolated.

4) Medium Head Safety Injection (MHSI) stop

The operator stops the MHSI pumps when the pressuriser level is sufficient, since the water inventory could be guaranteed due to the break isolation.

5) Reactor coolant system integrity check

The operator performs the reactor coolant system integrity check to identify which LHSI/RHR train is broken.

6) RIS [SIS] train in RHR mode re-established

Since the ruptured RHR system pipe is isolated via reactor coolant system integrity check, the RIS [SIS] train in RHR mode connection conditions can be re-established by operator via SGs.

12.9.5.5.2.4 Typical Sequence of Events

a) From the initiating event to the controlled state

For short term phase, the break leads to rapid drop of the reactor coolant system pressure and pressuriser level, as well as possible core heat up. Following actions or signals will be triggered:

1) Safety Injection (SI) is triggered by the “Hot leg ΔPsat low 1” signal.

2) RCPs are stopped by the “RCP ΔP low 1 and SI” signal.

3) RIS [SIS] pump is stopped by the “Hot leg ΔP_{sat} low 2” signal.

4) Isolation of RHR train suction line from hot leg can be triggered either by “Safeguard building sump level high 1” signal or “Safeguard building pressure rise high 1” signal.

Two situations could occur: RIS/RHRs remain in operation; RIS/RHRs are stopped. In both cases, the controlled state could be reached.

1) If the RIS [SIS] pumps in RHR mode are not tripped:

If the RIS [SIS] pumps in RHR mode are not stopped, the RIS [SIS] pumps in RHR mode ensure the reactor coolant system heat removal. The MHSI compensates for the break flow and the reactor coolant system water inventory is stabilised, enabling progression to controlled state.

2) If the RIS [SIS] pumps in RHR mode are tripped:

Following the trip of the RIS [SIS] pumps, the decay heat can be removed by the

break flow and the SGs, depending on the break size and the plant state. The reactor coolant system water inventory is restored and stabilised by MHSI and the controlled state is then reached.

b) From controlled state to safe state

For the long-term phase, since the break can be isolated from the reactor coolant system by automatic signals or operator actions, the safe state is defined as a state for which the ruptured RHR train is detected through the reactor coolant system integrity check and heat removal can be ensured until the RIS [SIS] trains in RHR mode can be re-established.

1) If the RIS [SIS] pumps in RHR mode are not tripped:

Considering that the RIS [SIS] trains are operating in RHR mode, the safe state may be reached as long as the controlled state has been achieved.

2) If the RIS [SIS] pumps in RHR mode are tripped:

In order to reach the connection conditions of RIS [SIS] in RHR mode, the sequences of actions performed by the operator are as the following:

- Reactor coolant system cooldown by SGs
- Startup of ASG [EFWS]
- Isolation of RHR train suction line from hot leg
- Stop of MHSI
- Reactor coolant system integrity check/ break isolation:

The RIS [SIS] train in RHR mode connection conditions is re-established.

12.9.5.5.2.5 Analysis Assumptions

The detailed assumptions are presented in Reference [60]. The main assumptions are listed as follows:

a) Initial conditions

1) The initial thermal power is assumed to be the largest decay heat of state C1. The higher initial thermal power is, the more the residual heat will be generated during the transient;

2) The initial coolant flowrate is the thermal-hydraulic design flowrate, which is considered to penalize heat removal;

3) The hot leg temperature of the coolant is the maximum value in state C1 plus the maximum uncertainty, which is considered to maximise stored energy;

4) The initial pressure of the pressuriser is the maximum value in state C1 plus

the maximum uncertainty. Because the higher the initial primary pressure, the more the mass flow rate at the break and the faster the loss of primary coolant.

5) The initial level of the pressuriser is the rated level in state C1 minus maximum uncertainties. The lower the initial pressuriser level, the less initial primary inventory to cool the core.

6) The total core bypass flow rate takes the maximum value to minimise the flow rate passing through the core.

b) Core-related assumptions

The decay heat is conservatively assumed to be constant, which equals to the initial core power.

c) LOOP assumption

Since turbine has already been stopped, LOOP is not considered in this case.

d) Single failure

For this analysis, the most important safety system is RIS [SIS]. Hence, single failures related to RIS [SIS] are considered. It is assumed that the single failure occurs on the one MHSI pump on unaffected loop.

This assumption penalizes the water inventory and heat removal from primary side. It penalizes core heat-up and limits the primary cooling.

12.9.5.5.2.6 Results and Conclusions

a) From the initiating event to the controlled state

Since core consequences of RHR-LOCA outside containment can be enveloped by that of RHR-LOCA inside containment (Sub-section 12.9.5.5.1), the acceptance criteria are met.

b) From the controlled state to the safe state

Since the core consequences of RHR-LOCA outside containment can be enveloped by that of RHR-LOCA inside containment (Sub-section 12.9.5.5.1), the plant can be brought to the safe state.

c) Radiological Consequence

The source term and radiological consequence of this case is analysed in Sub-section 12.11.4.10.

12.9.5.6 Inadvertent Opening of Severe Accident Dedicated Valves (One Train) (State A\B\C)

12.9.5.6.1 Inadvertent Opening of SADV in State A

12.9.5.6.1.1 Initiating Event

This event is defined as the spurious opening of the pressuriser severe accident dedicated valve (SADV) in state A (at power), without rapid reclosing due to a spurious signal or operator error.

An inadvertent opening of the dedicated depressurisation device can be initiated by:

a) A spurious opening signal of two isolation valves in series;

b) An operator error causing the manual opening of the depressurisation device.

Precautions limiting the transient occurrence:

To open the severe accident dedicated valve, two valves in series must be sequentially opened, thus limiting the scenarios and occurrence probability. The position of the SADV is accessible to the operator.

This accident can lead to a loss of reactor coolant inventory and core heat-up. The consequences of the event are considered in the plant design and can be managed with proper acceptance criteria.

The inadvertent opening of the dedicated depressurisation device in state A is classified as a DBC-4 event.

12.9.5.6.1.2 Acceptance Criteria

This accident is classified as a DBC-4 event. The safety criteria are the radiological limits for DBC-4 events.

The decoupling criteria for LOCA events:

a) The peak cladding temperature must remain lower than 1204℃;

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

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

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

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

These criteria are met if the core remains covered. Moreover, it shall be demonstrated that the plant can be brought to a safe state.

12.9.5.6.1.3 Main Safety Functions

In this event, reactor protection is provided by the following signals and actions:

a) Reactor trip is triggered after a “Pressuriser pressure low 2” signal;

b) The safety injection system is actuated by:

“Pressuriser pressure low 3” signal;

c) The RCPs are stopped by:

“RCP ΔP low 1” signal combined with the “Safety injection” signal;

d) The injection of the RIS [SIS] accumulator to the RCP [RCS] is actuated when:

The pressure of the RCP [RCS] is lower than 4.5 MPa;

e) Turbine trip is induced by:

Reactor trip;

f) The emergency feedwater system is actuated by:

“SG level (wide range) low 2” signal;

g) The main feedwater system is isolated by:

RIS [SIS] action signal or reactor trip.

12.9.5.6.1.4 Typical Events Sequence

The description presented hereafter is a typical sequence, i.e. the most likely to occur during the transient.

The sequence of events consists of two phases: the short-term phase until reaching the controlled state by use of automatic actions and the long-term phase where the plant is moved from the controlled to the safe state.

a) From the initiating event to the controlled state:

In state A, the spurious opening of the SADV induces a large pressure decrease in the RCP [RCS] and a pressuriser (PZR) level increase due to the steam released by the severe accident dedicated valve.

If the plant is initially at power, reactor trip is triggered by the “Pressuriser pressure low 2” signal or “Pressuriser level high 1” signal. The reactor trip signal automatically trips the turbine and isolates the main feedwater system full load lines.

Following turbine trip, the possible secondary side pressure increase is limited by the

steam generator (SG) relief devices: either the GCT [TBS] if available, or VDA [ASDS].

The SGs are fed by the ARE [MFFCS] through the low load lines.

Safety injection (SI) signal is actuated by the "Pressuriser pressure low 3" signal. The SI signal automatically starts the MHSI and the LHSI pumps, and initiates an MCD. The MCD consists of a controlled lowering of the GCT [TBS] (if available) or of the VDA [ASDS] pressure setpoint, with a rate corresponding to an SG cooldown of { }.

During the MCD, the RCP [RCS] pressure decreases sufficiently to allow MHSI injection into the cold legs. The released mass flowrate decreases as the PZR pressure decreases.

Further changes to the RCP [RCS] water inventory depend on the balance between the safety injection and heat removal system (RIS/RHR) injection, and the flowrate of the severe accident dedicated valve.

Before the RIS [SIS] injection is able to compensate for the flowrate of the severe accident dedicated valve, the core may be uncovered. This would result in a fuel clad temperature increase in the exposed area. The larger the area exposed, and the longer the duration, the higher the resulting clad temperatures.

The RCPs may be tripped by the "RCP ΔP low 1 over two loops and SI" signal. The RCP [RCS] inventory depletion stops when the MHSI and LHSI flowrate is sufficient to compensate for the flowrate of the severe accident dedicated valve.

The controlled state is reached following the achievement of stable heat removal conditions via the operation of MHSI and LHSI and the discharge of severe accident dedicated valve. The core is sub-critical and the reactor coolant inventory is stabilised or increasing due to RIS [SIS] injection.

b) From the controlled state to the safe state:

The safe state is defined as a state for which the flowrate of the SADV is compensated by the RIS [SIS] flowrate with long-term core cooling ensured.

The sequence of actions to be performed by the operator is as follows:

1) RCP [RCS] boration:

   The RCP [RCS] is borated sufficiently to keep the core sub-critical during the entire transient up to the safe state. Boration is performed by MHSI, or by additional boration using the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable.

2) RCP [RCS] cooldown:

The RCP [RCS] cooldown is performed via the secondary side by reducing the VDA [ASDS] opening pressure setpoint.

3) Water inventory restoration:

After reaching the switching time of the hot and cold legs, the operator switches the LHSI trains from cold leg injection to simultaneous injection to the cold leg and hot leg.

12.9.5.6.1.5 Analysis Assumptions

This transient is similar to IB-LOCA presented in Sub-section 12.9.5.2. The maximum relief capacity of one severe accident dedicated valve line is limited by the severe accident discharge nozzle on the top of the pressuriser.

The analysis performed in Sub-section 12.9.5.2, which covers a break spectrum up to 27.5 cm, located on cold leg.

The case with a surge line break analysed in Sub-section 12.9.5.2 leads to a faster decrease of RCP [RCS] water inventory than the opening of a severe accident dedicated valve line.

The consequences of the inadvertent opening of the dedicated depressurisation device in state A are thus bounded by the analysis of IB-LOCA presented in Sub-section 12.9.5.2. The acceptance criteria are thus met.

12.9.5.6.1.6 Results and Conclusions

The analysis performed shows that the transient is covered by IB-LOCA transient (see Sub-section 12.9.5.2). It demonstrates that the acceptance criteria presented in Paragraph 12.9.5.6.1.3 are met.

The radiological release characteristics of this accident is the same with LB-LOCA, however the latter would result a higher containment pressure, and the degree of fuel failure is worse. The radiological consequence can be bounded by the accident of large break-loss of coolant accident. The source term and radiological consequence of LB-LOCA is analysed in Sub-section 12.11.4.8.

12.9.5.6.2 Inadvertent Opening of SADV in State B\C

12.9.5.6.2.1 Initiating Event

The inadvertent opening of the severe accident dedicated depressurisation device in state B\C (in shutdown state) (DBC-4) is defined as the spurious opening of the pressuriser severe accident dedicated valve, without rapid reclosing due a spurious signal or operator error.

This accident can lead to a loss of reactor coolant inventory and core heat-up.

The consequences of the event are considered in the plant design and can be managed

by meeting the proper acceptance criteria.

Identification of causes:

An inadvertent opening of the dedicated depressurisation device can be initiated by:

a) A spurious opening signal of two isolation valves in series;

b) An operator error causing the manual opening of the depressurisation device.

Precautions limiting the transient occurrence:

For the SADV to open, two valves in series must be sequentially opened by the operator, thus limiting the potential scenarios and occurrence probability. The position of the SADV is accessible to the operator.

The inadvertent opening of the dedicated depressurisation device in state B\C is classified as a DBC-4 event.

12.9.5.6.2.2 Acceptance Criteria

This accident is classified as a DBC-4 event. The safety criteria are the radiological limits for DBC-4 events. The acceptance criteria for LOCA are applied.

The decoupling criteria for LOCA events:

a) The peak cladding temperature must remain lower than 1204℃;

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

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

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

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

These criteria are met if the core remains covered. Moreover, it shall be demonstrated that the plant can be brought to a safe state.

12.9.5.6.2.3 Main Safety Functions

In this event, reactor protection is provided by the following signals and actions:

a) The RCPs are tripped by:

   “ΔP low 1 over two RCPs” signal cumulated with the “Safety injection” signal;

b) The safety injection system is actuated by:

"Hot leg ΔPsat low 1" signal;

c) The emergency feedwater system is actuated by:

"SG level (wide range) low 2" signal;

d) The main feedwater system is isolated by:

1) RIS [SIS] action signal;

2) Reactor trip.

12.9.5.6.2.4 Typical Events Sequence

The description presented hereafter is a typical sequence, i.e. the most likely to occur during the transient.

The sequence of events consists of two phases: the short-term phase until reaching the controlled state through use of automatic actions and the long-term phase where the plant is operated from the controlled to the safe state.

a) From the initiating event to the controlled state:

In state B\C, the spurious opening of the severe accident dedicated valve (SADV) induces a large pressure decrease in the RCP [RCS] and a pressuriser (PZR) level increase due to the steam release by the severe accident dedicated valve.

SI signal is emitted after the "Hot leg ΔPsat low 1" signal, inducing the following actions:

1) Starting of MHSI and LHSI pumps;

2) Medium pressure rapid cooldown consisting in a controlled lowering of the GCT [TBS] (if available) or of the VDA [ASDS] setpoint;

3) Containment isolation stage: the reactor coolant pressure boundary is isolated, in particular the RCV [CVCS] letdown line and the steam generator (SG) blowdown lines are isolated.

The RCPs may be tripped by the "RCP ΔP low 1 over two loops" and "SI" signals.

As long as the RIS [SIS] flowrate does not compensate for the flowrate of the severe accident dedicated valve, RCP [RCS] coolant water inventory continues to decrease.

The flowrate of the SADV decreases as the PZR pressure decreases. The primary coolant inventory depletion stops when the RIS [SIS] flowrate compensates for the flowrate of the severe accident dedicated valve.

The controlled state is reached following achievement of stable heat removal conditions via the operation of MHSI and LHSI and the discharge of severe accident dedicated valve. The core is sub-critical and the reactor coolant inventory is stabilised

or increasing due to RIS [SIS] injection.

b) From the controlled state to the safe state:

The means to reach the safe state from the controlled state are the same as in state A (see Paragraph 12.9.5.6.1.3).

12.9.5.6.2.5 Analysis Assumptions

This transient is similar to IB-LOCA presented in Sub-section 12.9.5.2. The maximum relief capacity of one severe accident dedicated valve line is limited by the severe accident discharge nozzle on the top of the pressuriser.

The analysis performed in Sub-section 12.9.5.2, which covers a break spectrum up to 27.5 cm, located on cold leg.

The case with a surge line break analysed in Sub-section 12.9.5.2 leads to a faster decrease of RCP [RCS] water inventory than the opening of a severe accident dedicated valve line.

The consequences of the inadvertent opening of the dedicated depressurisation device in state B\C are thus bounded by the analysis of IB-LOCA presented in Sub-section 12.9.5.2. The acceptance criteria are thus met.

12.9.5.6.2.6 Results and Conclusions

The analysis performed shows that the transient is bounded by the IB-LOCA transient (see Sub-section 12.9.5.2). It demonstrates that the acceptance criteria presented in Sub-section 12.9.5.6.2.3 are met.

The radiological release characteristics of this accident is the same with LB-LOCA, however the latter would result a higher containment pressure, and the degree of fuel failure is worse. The radiological consequence can be bounded by the accident of large break-loss of coolant accident. The source term and radiological consequence of LB-LOCA is analysed in Sub-section 12.11.4.8.

12.9.6 Radiological Release of Systems or Components

12.9.6.1 Dropping of fuel assembly (State A to F)

Accidents occurring during fuel handling operations may be as follows:

a) Fuel assembly drop in the containment.

b) Fuel assembly drop in the fuel building.

The detailed analysis in terms of source terms and radiological consequences for a fuel assembly drop during fuel handling operations is provided in Sub-chapter 12.11.4.12.

12.9.6.2 Dropping of Spent Fuel Cask (State A to F)

Spent fuel cask is used to transfer spent fuel from the fuel building to the Spent Fuel Interim Storage (SFIS) facility. Dropping of spent fuel cask could occur during SFIS operation within or outside the fuel building, which may result in radioactivity release to environment and radioactivity distribution in the fuel building. The analysis in terms of source terms and radiological consequences is provided in Sub-chapter 12.11.4.13.

12.9.7 Fuel Pool Accidents

12.9.7.1 Non Isolable Small Break or Isolable RIS [SIS] Break Affecting Fuel Pool Cooling (State E)

12.9.7.1.1 Initiating Event

A piping failure may occur on an RIS [SIS] line (DN<250mm) in RHR mode or a line (DN<50mm) connected to the primary cooling system upstream of the first isolation valves. Since the transfer tube may be opened in state E, such piping failure may affect the cooling function of the SFP.

12.9.7.1.2 Acceptance Criteria

The safety criteria for the DBC accidents associated with the spent fuel storage pool are as follows and are also described in sub-chapter 12.5.9.1.

a) Permanent maintenance of sub-criticality;

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

12.9.7.1.3 Main Safety functions

For this event, the following plant safety functions can mitigate the event:

a) Every PTR [FPCTS] train is designed to remove decay heat from the SFP.

b) Isolation of the RIS/RHR line following the signal of “the reactor pool level low 1” of 16.4m.

c) Isolation of the PTR [FPCTS] trains following the signal “Spent fuel pool water level low 4”.

12.9.7.1.4 Typical Events Sequence

a) For non-isolable break (<50mm) on a line connected to the primary cooling system:

   1) transfer tube open

   In this case, the reactor pool, the reactor internals storage compartment, transfer compartment and the spent fuel pool are connected. Since the break in this situation is non-isolatable, the resulting drainage leak cannot be passively stopped manually or automatically. When the water level in the reactor pool drops to +16.4m, the RIS [SIS] line isolation signal is triggered. When the SFP water level drops to +16.0m, the isolation signal of the PTR [FPCTS] trains is triggered. The SFP temperature begins to rise without the PTR [FPCTS] cooling train. When the water level in the pools drops to +15.89m, the operator will manually start the MHSI to fill the pools and thus to restore the water level. After confirming the steady SFP water level is above the water level required

for restarting PTR [FPCTS] trains, the operator restarts one PTR [FPCTS] train. The temperature of the SFP will stop rising.

During the transient, the water loss is eventually collected in the IRWST due to its lower position in the containment.

Water makeup is performed with the MHSI pumps in recirculation mode between the IRWST and the primary cooling system.

Before starting the MHSI pumps for injection, it is necessary to drain the IVR (In-Vessel Retention) tank in the IRWST to ensure a sufficient IRWST water level for the MHSI pumps.

Related floor drainage/discharge lines are automatically isolated to prevent any loss of water outside the reactor building.

2) transfer tube closed

In this case, the reactor pool and the spent fuel pool are not connected. The break has no effect to the spent fuel pool. The SFP water level and temperature are stabilised.

b) For RIS/RHR lines isolatable break (<250mm)

1) transfer tube open:

In this case, the reactor pool, the reactor internals storage compartment, transfer compartment and the spent fuel pool are connected. The break in the RIS [SIS] line leads to drainage of the pools. When the water level in the reactor pool drops to 16.4m, the RIS [SIS] line isolation signal is triggered. The leak through RIS [SIS] suction line is automatically isolated by closing motorised valves. The drainage through RIS [SIS] discharge line is automatically prevented by the check valves.

The result shows that the water level is stabilised at 16.07m, and the isolation signal of the PTR [FPCTS] trains is not triggered. The SFP water level and temperature are stabilised.

2) transfer tube closed:

In this case, when the water level in the reactor pool drops to 16.4m, the RIS [SIS] line isolation signal is triggered. The leak through RIS [SIS] suction line is automatically isolated by closing motorised valves. The drainage through RIS [SIS] discharge line is automatically prevented by the check valves.

Since the transfer tube is closed, the reactor pool and the spent fuel pool are not connected. The break has no effect to the spent fuel pool. The SFP water level and temperature are stabilised.

12.9.7.1.5 Analysis Assumptions

Main assumptions adopted in the analysis are listed as follows:

a) The decay heat of the SFP in State E is conservatively assumed as 12.53MW.

b) The initial water temperature is 50℃, which can cover all normal operating conditions.

c) The initial water volume of the SFP is 1265.8m^3 corresponding to the water level of 16.9m.

d) One PTR cooling train is considered unavailable due to maintenance on the supporting systems of the PTR [FPCTS] train.

e) The most pessimistic Single Failure Criterion (SFC), one PTR [FPCTS] cooling train is unavailable, is considered in the analysis.

f) The isolation signal of the RIS [SIS] line will be triggered when the water level of the reactor pool drops to +16.4m.

   90s is considered for the RIS [SIS] line isolation signal time delay and valve isolation action.

g) The isolation signal of the PTR [FPCTS] train will be triggered when the water level of the SFP drops to +16.0m.

h) The break is conservatively assumed to be located in the lowest position of the corresponding pipeline, to maximize the leak flowrate.

i) The water heating is considered to be only localised in the SFP compartment, and the water is homogeneously heated in the SFP compartment.

j) The SFP and the PTR pipes are considered as adiabatic.

12.9.7.1.6 Results and Conclusions

The detailed analysis is presented in the Reference [61]. The analysis demonstrated that the temperature of the SFP will not exceed the saturation temperature. The fuel assemblies remain covered during the entire transient. The sub-criticality of the fuel assemblies is ensured by the design of spent fuel storage rack which is analysed in detail in Reference [48].

All acceptance criteria are met in this accident.

In terms of radiological consequence, since no boiling occurs in the accident and fuel assemblies are always covered in the SFP, there is radioactivity release.

12.9.8 Loss of Support Systems

12.9.8.1 Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinets Rooms

of Safeguard Building Division B (State C)

12.9.8.1.1 Description

This event is the representative of the following event which causes similar transient impact on the reactor core (Reference [100]):

a) Loss of LHB [EPDS(NI-10kV)].

This event leads to loss of one RIS-RHR train in operation (train B assumed) superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]) and loss of RCP [RCS] pumps (i.e. pump shutdown). Besides, the additional impact on other key safety functions is loss of division B and channel II (see Sub-chapter 12.8.8.1.1 for details).

Compared with loss of RRI [CCWS] or SEC [ESWS] Train A (State C\D\E) event analysed in Sub-chapter 12.8.8.2, the transient impact and consequence of this event are very similar. The DBC events that cause similar transient impact are the events in Sub-chapter 12.7.2.5, 12.7.5.1 and 12.8.5.4, which are the same as that listed in Sub-chapter 12.8.8.2.1.

12.9.8.1.2 Acceptance Criteria

The acceptance criteria are the same as that presented in Sub-chapter 12.8.8.2.2.

12.9.8.1.3 Main Safety Functions

The main safety functions required are the same as that presented in Sub-chapter 12.8.8.2.3.

12.9.8.1.4 Typical Events Sequences

The typical events sequences are the same as that described in Sub-chapter 12.8.8.2.4.

12.9.8.1.5 Results and Conclusions

As the analysis scope of Sub-chapter 12.7.2.5, 12.7.5.1 and 12.8.5.4 covers the state C and the initiating event, transient evolution and consequence of the event analysed in Sub-chapter 12.8.8.2 are highly similar to this event, it is justified that the analysis result of the event in Sub-chapter 12.8.8.2 remains applicable to this event. Therefore, all the acceptance criteria are met.

In this accident, there is no radioactivity release to the environment and the RPT-4 BSO is met.

12.10 Demonstration of Diverse Protection Lines

Diverse protection lines are provided for frequent faults. As part of design basis analysis, transient analyses are performed to demonstrate the functional adequacy of diverse protection lines.

This sub-chapter summarises the transient analyses for demonstrating the functional adequacy of diverse protection line. The conditions applied to the transient analyses are based on the bounding case selection results [62]. The summary of diverse protection lines demonstration is presented in Reference [63]. This sub-chapter describes the transient analysis of all diverse protection lines except for the following cases which are described in Sub-chapter 13.4.5:

a) ATWS by Rods Failure - Loss of Main Feedwater

b) ATWS by Rods Failure - Loss of Offsite Power

c) ATWS by Rods Failure - Small Break - Loss of Coolant Accident (SB-LOCA)

d) ATWS by Rods Failure - Spurious Pressuriser Spraying

e) SB-LOCA with Total Loss of Medium Head Safety Injection (MHSI)

f) Small Break - Loss of Coolant Accident (SB-LOCA) with Failure of Medium Pressure Rapid Cooldown (MCD)

g) Total Loss of Feedwater (TLOFW) (Loss of Normal Feedwater Flow with Mechanical Failure of ASG [EFWS])

h) Loss of RHR or Failure of Recovery of RHR after LOOP Accident (State C/D) (Loss of One Cooling Train of the Safety Injection System (RIS [SIS]) in Residual Heat Removal Mode (RHR) State (C\D) with Mechanical Failure of Continued Operation of the RHR trains)

i) SBO (LOOP with Failure of EDG)

j) SBO for Spent Fuel Pool (Long Term Loss of Offsite Power (>2 hours) Affecting Fuel Pool Cooling with Failure of EDG)

Different from DBC analysis, the analysis rules for diverse protection line demonstration are listed as follows:

a) Key initial parameters, main system parameters and time delay are considered with conservative assumptions;

b) Single failure is not considered;

c) Equipment that is not qualified for specific accident conditions is assumed to fail unless its continued operation results in more unfavourable conditions;

d) The time interval between detection of the abnormal event or accident and the required action is sufficiently long, and adequate procedures (such as

administrative, operational and emergency procedures) is specified to ensure the performance of such actions;

e) Preventive maintenance is not taken into account in diverse line analysis.

Additionally, LOOP is not taken into account except for the cases where LOOP is an initiating event.

12.10.1 ATWS by Rods Failure - Forced Reduction in Reactor Coolant Flow (3 pumps)

12.10.1.1 Description

This section describes the accident analysis of forced reduction in reactor coolant flow (3 pumps) & reactor trip failure caused by mechanical blockage of rods.

12.10.1.2 Acceptance Criteria

The acceptance criteria for this event are decoupling criteria of DBC-4 accidents. The following decoupling criteria are used in the DBC-4 analyses:

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

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

c) The peak cladding temperature must remain less than 1482 ℃.

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. If the minimum DNBR remains above the design limit { }, the criteria are met. Besides, the highest pressure of primary circuit should be under 130% design pressure (22.37 MPa abs.) to ensure the primary side remains intact.

12.10.1.3 Main Safety Functions

The main reactor protections are listed below:

a) Reactor trip is triggered by the “Low RCP pump speed” signal automatically (FC1).

b) The reactor trip signal triggers the turbine trip automatically (FC1).

c) The reactor trip signal triggers the ARE [MFFCS] full load lines of the SG isolation automatically. And the ARE [MFFCS] low load lines are assumed unavailable. The SGs are fed with water by the ARE [MFFCS] system through the low load lines (FC1).

d) The “high rod position” (at least 2 control rods cannot be inserted) combined with reactor trip signal triggers the Anticipated Transient without Scram (ATWS) signal automatically (FC2).

e) Three trains of the ASG [EFWS] are actuated by “SG level (wide range) low 2”

signal automatically (FC1).

f) The ATWS signal initiates three trains of the RBS [EBS] automatically (FC2).

12.10.1.4 Typical Sequence of events

The causes of the ATWS may be:

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

b) Shutdown rod failure due to mechanical blockage of rods.

The forced reduction in reactor coolant flow - ATWS transient caused by mechanical blockage of rods is analysed.

The forced reduction in reactor coolant flow may be caused by a simultaneous fault in the power supplies to all the reactor coolant pumps. A fast decrease in the off-site grid supply frequency can lead to a reversal of motor torque and thus to decrease the reactor coolant pumps speed, which rapidly reduces the coolant flow.

The reactor trip signal is emitted on “Low RCP pump speed” signal. However, although the reactor trip signal has been emitted, the control rods are still at high positions due to mechanical blockage. Therefore, the reactor trip is not realised. Then the turbine trips automatically. After that, the ARE [MFFCS] full load lines are automatically closed, and the ARE [MFFCS] low load lines are assumed unavailable. The coolant flow rate decreases and temperature rises may lead to a decrease in the DNB margin. Finally, the core is cooled through natural circulation flow.

The “high rod position” combined with reactor trip 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. The VDA [ASDS] ensures the removal of the secondary heat. When the SG level decreases to the “SG level (wide range) low 2”, the ASG [EFWS] is started up to supply water to the SG. The EDG come into service following the failure of the off-site grid to support the operation of the main systems related to the automatic protection functions.

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

The decrease in reactor coolant flow causes a rapid increase in coolant temperature and pressure, potentially resulting in the DNB and subsequent fuel damage.

12.10.1.5 Results and Conclusions

The minimum DNBR of 1.46 in the forced reduction in reactor coolant flow - ATWS accident is greater than the limit {

}. It is confirmed that the peak primary pressure is 18.4 MPa abs., which does not exceed the maximum allowable pressure of 22.37 MPa abs. There are enough margins due to the PSVs operation, although the nominal value minus the maximum uncertainty is used to minimize the DNBR. And the inherent safety of nuclear plant ensures the acceptance criteria concerning DNBR are satisfied. Therefore, this fault does not challenge the integrity of the RCP [RCS]. It is concluded that the acceptance criteria are met. The detailed results are presented in Reference [64].

In the long term, the residual heat is removed by the VDA [ASDS] of all SGs with the feedwater supplied by the ASG [EFWS]. The RBS [EBS] boron injection ensures that the core remains subcritical. The safe state is reached after the RHR is connected.

12.10.2 Small Break LOCA with Failure of Reactor Trip Sensor

12.10.2.1 Description

SB-LOCA with failure of reactor trip sensor (failure of pressuriser pressure sensors) at state A, including a break in the Emergency Boration System (RBS [EBS]) injection line, is studied. It means those signals related to the pressuriser pressure are invalid. As far as SB-LOCA is concerned, two important signals needed for reactor protection, “Pressuriser pressure low 2” signal and “Pressuriser pressure low 3” signal in RPS [PS] system, are considered to be invalid. Diversity in sensors is implemented. Hot leg pressure related signals would provide protection in this situation.

12.10.2.2 Acceptance Criteria

The analyses should meet the following acceptance criteria:

a) The peak cladding temperature must remain lower than 1204 ℃;
b) The maximum cladding oxidation must remain lower than 17% of the cladding thickness;
c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding had reacted;
d) The ability to cool the core shall be maintained, i.e. calculated changes in core geometry shall be such that the core remains amenable to cooling;

However, if no significant core heat up would occur during the transient, above criteria are considered to be met. Thus the consequences of SB-LOCA are analysed against the following aspects:

a) Core remains covered;

b) The plant shall be brought to and maintained in controlled state;

c) The plant shall be brought to and maintained in safe state.

12.10.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions are required:

a) Reactor trip

In state A, reactor trip is triggered by the “Hot leg pressure low 1” signal.

b) Turbine trip

The reactor trip signal triggers the turbine trip.

c) The reactor coolant pumps trip

The Reactor Coolant Pumps (RCP) trip is triggered by the “RCP ΔP low 1 and SI” signal.

d) ARE [MFFCS] full load lines isolation

Following the reactor trip signal, ARE [MFFCS] full load lines of all steam generators are isolated.

e) Safety Injection (SI)

SI is actuated by the “Hot leg pressure low 3” signal.

f) Emergency Feedwater System (ASG [EFWS]) start up

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

g) ASG [EFWS] isolation

ASG [EFWS] in one certain loop is isolated by the “SG level (wide range) high 1” signal of corresponding Steam Generator (SG).

h) Opening of Atmospheric Steam Dump System (VDA [ASDS])

The VDA [ASDS] valves automatically open when the secondary pressure reaches the VDA [ASDS] setpoint.

i) Medium Pressure Rapid Cooldown (MCD)

Following the SI signal, MCD is initiated to cool the primary circuit with a rate of { }.

In order to reach the safe state, the following manual safety functions are required:

a) Reactor coolant system boration

The Emergency Boration System (RBS [EBS]) pumps are started by the operator before the reactor coolant system cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

b) Reactor coolant system cooldown by SGs

The cooldown is performed via the VDA [ASDS] of SGs. The cooling rate is { } with at least two RBS trains in operation and { } if only one RBS train is available.

c) Main Steam Isolation Valve (MSIV) closure

MSIV closure is manually initiated when one SG claimed unavailable. All the main steam lines are then isolated.

d) Reactor coolant system depressurization

During the reactor coolant system depressurization, the accumulators are isolated when the reactor coolant system pressure decreases below 2.0 MPa abs.

The Medium Head Safety Injection (MHSI) pumps are stopped when the reactor coolant system level is sufficient and the hot leg temperature is lower than { }.

For a very small break, if necessary, reactor coolant depressurization can be realized by pressuriser spray or opening of the pressurizer safety valves.

Reactor coolant system is then depressurized until the injection pressure of Low Head Safety Injection (LHSI) is reached.

e) Safety Injection System (RIS [SIS]) in Residual Heat Removal (RHR) mode connection

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling.

12.10.2.4 Typical Sequence of events

a) From the initiating event to controlled state (short term)

Loss of Coolant Accident (LOCA) could lead to a loss of primary coolant inventory and primary depressurization.

The SB-LOCA with failure of pressurizer pressure sensors results in a loss of primary coolant, a potential decrease in reactor coolant system pressure and radioactive release to the environment. This accident may lead to a decrease in reactor coolant inventory and potential core overheating. The SB-LOCA with failure of pressurizer pressure sensors accident is mainly a gravity-driven accident, in which the reactor coolant system discharges slowly with the evident formation of mixing layers throughout the reactor coolant system. These mixing layers change over time, depending on the transient of two phase mass and energy mutual transfer. The first heat-up results from the core level decrease and the formation of a loop seal, and can be mitigated by loop seal clearance during the accident. The second heat-up is due to the boiling and evaporation of the core coolant. During this event, the flow from the MHSI, accumulators and LHSI enter

the core and cool the fuel cladding to prevent further temperature increase, and guarantees the core coolant inventory.

Reactor trip is triggered by the “Hot leg pressure low 1” signal. Following the reactor trip, turbine trip occurs and Main Feedwater Flow Control System (ARE [MFFCS]) full load lines for all SGs are isolated. After reactor trip and turbine trip, the secondary pressure increases rapidly until that the setpoint of VDA [ASDS] is reached.

Because of the continuous break flow to the containment and the decrease of decay heat after reactor trip, the SI signal is triggered by the “Hot leg pressure low 3” signal. Medium Pressure Rapid Cooldown (MCD) is initiated in all SGs following the SI signal. The MCD is carried out by reducing the VDA [ASDS] setpoint, cooling down the reactor coolant system with a rate of{ }. When the MCD completes, the secondary pressure is reduced to 6.0 MPa abs. Following the SI signal, the Medium Head Safety Injection (MHSI) and the LHSI pumps are actuated. The Safety Injection System (RIS [SIS]) starts injecting when the reactor coolant system pressure is below the pump injection head. Then RIS [SIS] injection flow will compensate for the break flow.

After reactor trip and safety injection, the residual heat is mainly removed by the break flow, the RIS [SIS] and the secondary side. The controlled state is achieved when:

1) The primary residual heat can be continuously removed via the break and the plant safety systems including RIS [SIS] and VDA [ASDS];

2) Core sub-criticality is ensured;

3) Core coolant inventory stabilises or increases via the Safety Injection (SI).

b) From controlled state to safe state (long term)

The safe state is defined as a state at which the break flow rate is compensated by the RIS [SIS] flow rate with long-term core cooling ensured. The following actions need to be performed (by operators) in order to reach the safe state:

1) Reactor coolant boration

During the reactor coolant system cooldown, to ensure the core sub-criticality, the operator uses RBS [EBS] to compensate the reactivity insertion resulting from the reactor coolant system cooldown.

2) Reactor coolant cooldown

The cooldown, to achieve suitable connecting conditions for the RIS [SIS] in RHR mode, is performed for the units via the secondary side by reducing the VDA [ASDS] setpoint.

3) Primary depressurization

   In order to achieve connection conditions of the RIS [SIS] train in RHR mode, the operator stops MHSI pumps to depressurize primary circuit.

4) Connection of RIS [SIS] in RHR mode.

   The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long-term cooling

12.10.2.5 Results and Conclusion

The analysis result on SB-LOCA with failure of pressurizer pressure sensors shows that the core remains covered from initiating event to safe state. In addition, the RIS [SIS] in RHR mode connection conditions can be reached. As a result, the relevant acceptance criteria described in 12.10.2.2 are met. The detailed results are presented in Reference [65].

In terms of radiological consequence, it is represented by “small break LOCA” fault. Since the core remains covered during the transient, there is no challenge of fuel integrity. The releasing pathway is the same as “small break LOCA”. Therefore, the radiological consequence for this fault can be represented by “small break LOCA”.

12.10.3 ATWS by Rods Failure - Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup

12.10.3.1 Description

This section provides the diverse protection demonstration of uncontrolled RCCA bank withdrawal at a subcritical or low power startup condition with ATWS.

12.10.3.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

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

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

c) The peak cladding temperature must remain lower than 1482℃;

In addition, the highest pressure of primary circuit should be under 130% design pressure (22.37MPa abs) to ensure the primary integrity.

12.10.3.3 Main Safety Functions

The following control and protection systems are considered in the event:

a) Reactor trip signal

Reactor trip is triggered by the “high neutron flux (power range, low setpoint)” signal automatically.

b) “ATWS” signal

The high rod position combined with reactor trip signal triggers the “ATWS” signal.

c) Reactor coolant pumps stop

The “Steam Generator (SG) level (narrow range) low 1” signal combined with the “ATWS” signal triggers the reactor coolant pumps to stop automatically.

d) ASG [EFWS] operation

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

e) Pressuriser Safety Valve (PSV) open and close

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

f) VDA [ASDS] open and close

The VDA [ASDS] opens and closes automatically when the pressure reaches the setpoint to limit the secondary pressure.

g) RBS [EBS] operation

The "ATWS" signal initiates three trains of the RBS [EBS] automatically. The RBS [EBS] is one of the key systems to mitigate the accident, which belongs to DEC-A features.

12.10.3.4 Typical Sequence of events

In RCCA bank withdrawal at a subcritical or low power startup condition, the insertion of positive reactivity results in an increase in the core power. Thus it triggers the reactor trip on "high neutron flux (power range, low setpoint)" signal. However, the reactor does not shutdown as the RCCAs fail to drop.

Once it is detected that the rods are still at high positions, the ATWS signal is triggered. The RBS [EBS] is initiated automatically by ATWS signal. The pumps of RCP [RCS] are tripped on ATWS signal combined with the "SG level (narrow range) low 1" signal.

The steam is discharged either by the GCT [TBS] or the 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 the 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, thus slowing down the increasing rate of primary pressure and temperature.

The ASG [EFWS] is initiated by "SG level (wide range) low 2" signal. The RBS [EBS] boron injection ensures that the core remains subcritical in the long term. Then, the SG inventory recovers, and thus the primary temperature and pressure also begin to drop.

12.10.3.5 Analysis Assumptions

The detailed assumptions are presented in Reference [30]. The main assumptions of DNB analysis are listed as follows:

a) Initial Conditions

1) G1, G2, N1, N2 and R control rod banks are fully inserted;

2) Critical core;

3) The unit is initially operated under 10^{-13} FP;

4) Initial reactor coolant average temperature is at its nominal value plus uncertainty (298.5℃) to penalise DNBR;

5) Initial pressuriser pressure is at its nominal value minus uncertainty (15.25MPa) to penalise DNBR;

6) Initial reactor coolant flowrate is equal to the thermal design flow (24000m^3/h/loop) considering 10% pipe plugging of SGs, so as to penalise the heat removal.

b) Core-related Assumptions

1) Neutronic kinetics parameter

The delayed neutron fraction and the prompt neutron lifetime used in the analysis are set to the maximum envelope values, i.e. 750pcm and 31μs respectively, to ensure the maximum energy in the fuel pellet.

2) Doppler effect

The Doppler feedback is set at its calculated enveloped absolute value of BCX in the first cycle to increase the peak nuclear power.

3) Reactivity insertion rate

The differential worth of the two most valued RCCA banks withdrawn with the maximum rate (72steps/minute) is calculated at BCX. The result is used for the nuclear transient calculation.

The axial power distribution greatly tilting towards the core bottom is selected, maximizing the differential worth of the withdrawn RCCA as well as the peak power factor.

4) Nuclear enthalpy rise hot channel factor $F_{\Delta H}$

Between the full insertion and full withdrawal of the RCCA bank, the most penalising position during the bank withdrawal is used in the FΔH calculation. During the RCCA bank withdrawal, the FΔH is assumed to remain unchanged, equalling to the most penalising value.

c) Reactor Protection

1) Reactor trip is triggered on “high neutron flux (power range, low setpoint)” signal;

2) ATWS signal is actuated by the “high rod position signal (at least 2 control rods cannot be inserted) combined with reactor trip signal;

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

4) RBS [EBS] is actuated by the the ATWS signal;

5) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

6) VDA [ASDS] is actuated by the “SG pressure high 1” signal;

7) PSVs are opened when the pressuriser pressure reaches the setpoint.

d) Control Systems

The normal control systems which have negative effects on the transient are considered in the analysis. The pressuriser spray is taken into account to penalise the primary pressure.

The main assumptions of fuel temperature case are the same with DNB case except the followings:

a) Initial reactor coolant average temperature is at its nominal value minus uncertainty (291.5℃) according to the sensitivity analysis;

b) Initial pressuriser pressure is at its nominal value plus uncertainty (15.75MPa) according to the sensitivity analysis;

c) The heat flux hot channel factor

The heat flux hot channel factor F_Q used in the hotspot thermal transient analysis is a product of the radial peaking factor F_{xy} and the axial peaking factor F_z. The F_{xy} is assumed to remain unchanged during the whole control rod withdrawal period, equaling to the maximum value; the F_z is also assumed to remain unchanged and be set to the maximum value during the transient.

12.10.3.6 Results and Conclusions

The calculation result of DNBR case shows that the minimum DNBR is 1.51 which is greater than the design limit 1.36 (W3 correlation, deterministic method). Thus the acceptance criterion for this event is met.

The calculation result of fuel temperature case shows that the peak pellet center temperature is 2510℃ which is lower than the fuel design limit { }℃. Thus the acceptance criterion for this event is met.

The fault analysis shows that the protection system provides sufficient protection for the reactor. All the acceptance criteria are met. The detailed results are presented in Reference [66].

In terms of radiological consequence, this fault is represented by “Small Break – Loss of Coolant Accident (State A)” fault considering that fuel integrity is maintained and primary integrity is temporarily breached by opening of PSV during this transient. The radiological consequence of “Small Break – Loss of Coolant Accident (State A)” fault is analysed quantitatively, which can represent this kind of accidents with VDA [ASDS] releasing pathway and potential containment releasing pathway.

12.10.4 RCCA Bank Withdrawal at Power with Failure of Primary Protection Sensor for RT

12.10.4.1 Description

According to the analysis of RCCA withdrawal at power, the primary protection line of reactor trip is “high neutron flux” signal or “overtemperature ΔT” signal. The sensors for the two signals are different, thus, with the failure of primary protection sensors for one of the two signals, the other signal can be used as the diverse line. However, “high neutron flux” signal is mainly triggered in high reactivity insertion rate case and “overtemperature ΔT” signal is mainly triggered in the low reactivity insertion rate case. As the consequence of high reactivity insertion rate case is worse than the low reactivity case, the failure of sensors for “high neutron flux” signal is considered in the study.

12.10.4.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

a) The amount of fuel rods experiencing DNB must remain lower than 10%;

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

c) The peak cladding temperature must remain lower than 1482℃.

In addition, the highest pressure of primary circuit should be under 130% design pressure (22.37MPa abs) to ensure the primary side remains intact.

12.10.4.3 Main Safety Functions

The following control and protection systems are considered in the event:

a) Reactor trip Signal

Reactor trip is triggered by the “Overpower ΔT” signal automatically.

b) Turbine trip

The reactor trip signal triggers the turbine trip automatically.

c) Main Feedwater Flow Control System (ARE [MFFCS]) operation

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

d) Pressuriser spray valve open and close

The Pressuriser (PZR) spray valve open and close automatically to limit the primary circuit pressure.

e) Atmospheric Steam Dump System (VDA [ASDS]) open and close

12.10.4.4 Typical Sequence of events

The induced reactivity insertion results in an increase in the core heat flux. Before the secondary circuit pressure reaches the setpoint of the relief valve or safety valve, the heat removed from the SGs lags behind the increase of core power. The pressure and temperature of primary and secondary circuit increase until RT. Before reactor trip, the pressurizer spray and PSVs may be opened to limit the RCP [RCS] pressure and the VDA [ASDS] may be opened to limit the secondary circuit pressure.

After reactor trip, the RCCA banks drop into the core and the core power decreases dramatically. Turbine trip and the Main Feedwater Flow Control System (ARE [MFFCS]) full load isolation are initiated by the reactor trip signal. The secondary circuit pressure is limited by the VDA [ASDS] if the Turbine Bypass System (GCT [TBS]) is unavailable.

Finally, the controlled state is reached. The residual heat is removed by the VDA [ASDS] of all steam generators.

12.10.4.5 Analysis Assumptions

The detailed assumptions are presented in Reference [67]. The main assumptions are listed as follows:

a) Initial Conditions

1) The initial power is assumed at full power plus uncertainty (102%FP) to maximise primary heat;

2) Initial reactor coolant average temperature is assumed at its nominal value plus uncertainty (309.5℃) to minimise the DNBR;

3) Initial pressuriser pressure is assumed at its nominal value minus uncertainty (15.25MPa) to minimise the DNBR;

4) Initial reactor coolant flowrate is assumed to be the thermal design flow (24000m^3/h/loop), considering 10% tube plugging of SGs, so as to penalise the heat removal.

b) Core-related Assumptions

1) The moderator density coefficient is set at its minimum absolute value to maximise the nuclear power.

2) The Doppler power coefficient, which tends to limit the nuclear power increase, is set at its minimum absolute value without consideration of the uncertainty.

3) The Doppler temperature coefficient, which induces a negative reactivity insertion when the fuel temperature increases, is set at its minimum absolute value.

4) The maximum bounded worth of R bank is respectively calculated at BCX, MOC and EOC for all cycles, besides, R bank withdrawn with the maximum rate (72 step/minute) is considered for the transient calculation.

c) Reactor Protections

1) Reactor trip is triggered on "Overpower ΔT" signal. The setpoint is assumed to be the rated value plus uncertainties. A conservative delay between setpoint actuation and the beginning of rod drop is considered;

2) PSVs are assumed to be available, so as to limit the RCP [RCS] pressure increase and therefore penalise the DNBR calculation;

3) If reactor trip occurs,

- Turbine trip;
- ARE [MFFCS] full load lines are isolated;
- The RCP [RCS] heat is removed by VDA [ASDS], and the GCT [TBS] is assumed to be unavailable.
- The SGs are fed by the ARE [MFFCS] low load line.

d) Control Systems

PZR spray is assumed to be available, so as to limit the RCP [RCS] pressure increase and therefore penalise the DNBR calculation.

12.10.4.6 Results and Conclusion

The calculation results show that:

a) The most penalizing transient occurs at EOC.

b) The amount of fuel rods experiencing DNB is 0.65%, which is less than 10%, so the criterion for DNB is met.

c) The maximum fuel pellet temperature is 2557.9℃, which is lower than { }℃, so the fuel pellet melting at the hot spot is 0% and the criterion for fuel pellet melting is met.

d) The peak cladding temperature is 926.5℃, which is lower than 1482℃, so the criterion for peak cladding temperature is met.

e) Based on the analysis result, the peak primary pressure is 16.07 MPa abs, thus the criterion of overpressure is not challenged.

The fault analysis shows that the protection system provides sufficient protection for the reactor. All the acceptance criteria are met. The detailed results are presented in Reference [67].

The analysis is based on conservative assumptions and models, which follows good

practice. The results prove that all the acceptance criteria for this fault are met. Besides, FC3 and non-classified mitigation measures are not taken into account in the analysis, which could contribute to fault mitigation.

In terms of radiological consequence, this fault is represented by “Spectrum of RCCA Ejection Accident” fault considering that DNB occurs and primary integrity is temporarily breached by potential opening of PSV during this transient. The radiological consequence of “Spectrum of RCCA Ejection Accident” fault is analysed quantitatively, which can represent this kind of accidents with VDA [ASDS] releasing pathway and potential containment releasing pathway.

12.10.5 ATWS by Rods Failure - RCCA Bank Withdrawal at Power

12.10.5.1 Description

This subchapter provides the diverse protection demonstration of RCCA bank withdrawal at power with ATWS.

12.10.5.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

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

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

c) The peak cladding temperature must remain lower than 1482℃;

In addition, the highest pressure of primary circuit should be under130% design pressure (22.37MPa abs) to ensure the primary integrity.

12.10.5.3 Main Safety Functions

The following control and protection systems are considered in the event:

a) Reactor trip signal

Reactor trip is triggered by the “high neutron flux (power range, high setpoint)” or “overtemperature ΔT” signal automatically.

b) “ATWS” signal

The high rod position combined with reactor trip signal triggers the “ATWS” signal.

c) Turbine trip

The reactor trip signal triggers the turbine trip.

d) Reactor coolant pumps stop

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

e) ASG [EFWS] operation

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

f) ARE [MFFCS] operation

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

g) Pressuriser Safety Valve (PSV) open and close

The PSVs open and close automatically when the pressure reaches the setpoint to

limit the primary pressure automatically.

h) VDA [ASDS] open and close

The VDA [ASDS] opens and closes automatically when the pressure reaches the setpoint to limit the secondary pressure.

i) RBS [EBS] operation

The “ATWS” signal initiates three trains of the RBS [EBS] automatically.

12.10.5.4 Typical Sequence of events

In ATWS by RCCA bank withdrawal at power event, the insertion of positive reactivity results in an increase in the core power. The heat extraction from the SG lags behind the core power generation. The pressure and temperature of primary and secondary circuit keep increasing and thus it triggers the reactor trip on “high neutron flux (power range, high setpoint)” signal, “overtemperature ΔT” or “high neutron flux (intermediate range)”. However, the reactor does not shutdown as the RCCAs fail to drop. This accident leads to a significant increase in the primary pressure and temperature.

The turbine trip and ARE [MFFCS] full load isolation are actuated by reactor trip signal. Once it is detected that the rods are still at high positions, the ATWS signal is triggered. The pumps of RCP [RCS] 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 trip, the steam is discharged either by the GCT [TBS] or the 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 the PSV. 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 also begin to drop. The RBS [EBS] boron injection ensures that the core remains subcritical in the long term.

12.10.5.5 Analysis Assumptions

The detailed assumptions are presented in Reference [68]. The main assumptions are listed as follows:

a) Initial Conditions

1) The initial power is assumed at full power plus uncertainty (102%FP) to maximise primary heat;

2) Initial reactor coolant average temperature is assumed at its nominal value plus uncertainty (309.5℃) to minimise the DNBR;

3) Initial pressuriser pressure is assumed at its nominal value minus uncertainty (15.25MPa) to minimise the DNBR;

4) Initial reactor coolant flowrate is assumed to be the thermal design flow (24000m^3/h/loop), considering 10% tube plugging of SGs, so as to penalise the heat removal.

b) Core-related Assumptions

1) The moderator temperature coefficient, is set at -21.2 pcm/℃ at the beginning of the transient, which envelopes 99% of the whole nuclear plant life time.

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

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

4) The reactivity insertion rates (0.1pcm/s ~ 45pcm/s) assumed in the analysis envelope all possible conditions. The maximum positive reactivity insertion rate analysed is greater than that for the simultaneous withdrawal at maximum speed (72 steps/min) of the two control banks having the maximum combined worth and the maximum overlap.

c) Reactor Protections

1) Reactor trip is triggered by the high neutron flux (power range, high setpoint) signal;

2) ATWS signal is actuated by the high rod position combined with reactor trip signal;

3) The reactor trip signal triggers the turbine trip automatically;

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

5) RBS [EBS] is actuated by the the ATWS signal;

6) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

7) VDA [ASDS] is actuated by the “SG pressure high 1” signal;

8) PSVs are opened when the pressuriser pressure reaches the setpoint.

d) Control Systems

The normal control systems which have negative effects on the transient are considered in the analysis.

1) The pressuriser spray is taken into account to penalise the primary pressure.

2) The GCT [TBS] is taken into account to penalise the increase of primary coolant temperature.

12.10.5.6 Results and Conclusions

The calculation result shows that the amount of fuel rods experiencing DNB is 1.0% which is lower than the design limit 10%. The maximum fuel center temperature is 2517℃ and the maximum melt portion of fuel pellet is 0%, which is lower than the design limit 10%. The maximum cladding temperature is 1263℃, which is lower than the design limit 1482℃. Based on the analysis result, the peak primary pressure is 20.9 MPa abs. Thus the criterion of overpressure is not challenged.

The fault analysis shows that the protection system provides sufficient protection for the reactor. All the acceptance criteria are met. The detailed results are presented in Reference [68].

In terms of radiological consequence, this fault is represented by “Spectrum of RCCA Ejection Accident” fault considering that DNB occurs and primary integrity is temporarily breached by opening of PSV during this transient. The radiological consequence of “Spectrum of RCCA Ejection Accident” fault is analysed quantitatively, which can represent this kind of accidents with VDA [ASDS] releasing pathway and potential containment releasing pathway.

12.10.6 ATWS by Rods Failure - RCCA Misalignment up to Rod Drop

In case of mechanical ATWS, the negative reactivity would be introduced by neutronic negative feedback and high concentrated boron injection. Primary pressure could be limited by PSVs. As the initiating event of this accident is RCCA misalignment up to rod drop, this accident is less severe than other reactivity insertion accident with mechanical ATWS, for instance, RCCA bank withdrawal accidents.

12.10.7 ATWS by Rods Failure - Uncontrolled Single RCCA Withdrawal

12.10.7.1 Description

This section describes the accident analysis of uncontrolled withdrawal of a single control rod under full power reactor operation combined with ATWS by mechanical blockage of rods.

12.10.7.2 Acceptance Criteria

The fuel integrity and integrity of RCP [RCS] might be challenged in this fault. The following acceptance criteria are used for this fault:

In terms of fuel integrity, the following acceptance criteria are used for this fault:

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

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

c) The peak cladding temperature must remain lower than 1482℃.

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. The acceptance criteria to be considered for this event are as follows:

a) The minimum DNBR shall be greater than { };

b) The peak cladding temperature must remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

In terms of integrity of RCP [RCS], the acceptance criteria for DBC-4 are applied to ensure the integrity of pressure boundary for RCP [RCS] system. Therefore, the pressure at the most loaded point shall not exceed 130% design pressure (22.37MPa abs) is defined as the decoupling criteria.

12.10.7.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions are required:

a) Reactor trip is triggered by the “Overtemperature ΔT” signal and other reactor trip signals automatically. The “rod position signal (at least 2 control rods cannot be inserted)” combined with reactor trip signal triggers the “ATWS” signal automatically;

b) The “ATWS” signal initiates the RBS [EBS] automatically;

c) Turbine trip on “RT” signal;

d) ARE [MFFCS] full load lines are isolated on reactor trip signal automatically;

e) VDA [ASDS] is opened by the “SG pressure high 1” signal;

f) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

g) PSV opening when primary pressure reaches the setpoints.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

If the ASGs [EFWS] are not actuated automatically, the operator will start the ASGs [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASGs [EFWS].

b) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

c) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rate is { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

d) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by PZR normal spray or opening the PSV when the PZR normal spray is unavailable.

e) Accumulators isolation

The accumulators are isolated to avoid the injection of accumulator water.

f) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.10.7.4 Typical Sequence of events

A typical event sequence, where automatic actions and manual actions are presented, can be divided into the following two stages:

a) From initiating event to controlled state

The uncontrolled withdrawal of a single control rod causes an insertion of reactivity, resulting in an increase in the core power, coolant temperature and hot channel factor. Around the withdrawal position, the local power peak may lead to a low DNBR and potentially leading to fuel cladding failure.

After the withdrawal of a single control rod, reactor trip signal is emitted on “Overtemperature △T” signal. However, although the reactor trip signal has been

emitted, the control rods are still at high positions due to mechanical blockage; therefore the reactor trip is not realized. The high rod position combined with reactor trip signal lead to the triggering of the “ATWS” signal, the “ATWS” signal initiates the RBS [EBS] operation. Then the turbine trips automatically. After that, ARE [MFFCS] full load lines are automatically closed. When the SG level decreases to the “SG level (narrow range) low 1”, the “ATWS” signal and “SG level (narrow range) low 1” signal cause the RCP [RCS] pumps to trip. When the SG level decreases to the “SG level (wide range) low 2”, the ASG [EFWS] is started up to supply water to the SG. Once the primary and secondary pressure increase to the setpoint of PSV and VDA [ASDS], the opening of the PSV and VDA [ASDS] would limit the primary pressure rise and ensure the removal of the secondary heat. Then, the decay heat can be continuously removed.

b) From controlled state to safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration via the RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation via the normal or auxiliary pressuriser spray and the PSVs can be used when the pressuriser sprays are unavailable.

12.10.7.5 Results and Conclusions

The calculation results show that:

a) The minimum DNBR is greater than the design limit { };

b) The maximum fuel cladding temperature is less than 1482℃;

c) The maximum fuel temperature is lower than the fuel melting temperature limit { }℃. Thus the amount of fuel melting at hot spot is 0 %.

And the maximum pressure of the RCP [RCS] is lower than 130% RCP [RCS] design pressure. All acceptance criteria are thus met. The detailed results are presented in Reference [69].

For this accident, no DNB occurs and the limit of fuel pellet temperature and cladding temperature are not challenged, and the integrity of the pressure boundary for RCP [RCS] system is ensured during the transient.

In terms of radiological consequence, it is represented by “Turbine Trip” fault. Since there is no challenge of fuel integrity and primary circuit integrity, the radiological consequence is very limited. Turbine trip is analysed quantitatively in terms of radiological consequence, which can represent this kind of accidents with a VDA [ASDS] releasing pathway.

12.10.8 RCV [CVCS] Malfunction that Results in a Decrease in Boron Concentration in the Reactor Coolant with Failure of Isolation Valve

This section describes the accident analysis of RCV [CVCS], REA [RBWMS] and TEP [CSTS] malfunction that result in a decrease in boron concentration in the reactor coolant combined with failure of isolation valve. Due to loss of primary protection line, the dilution source cannot be isolated automatically. A diverse protection line is designed to isolate RCV[CVCS] charging line by operator via closing RCV8211VP- or RCV6512/6314VP-, isolate RCP[RCS] seal injection line by operator via closing RCV8311VP- and stop the charging pumps manually in the main control room. For boron dilution events at power operation conditions in manual control mode, calculation results for all fuel cycles analysed show that after reactor trip the operator has enough time to isolate dilution source manually before the core reaches criticality, which have been analysed in Sub-chapter 12.7.4.5.2. Thus, the following two cases are analysed for justification.

12.10.8.1 RCV [CVCS] Malfunction that Results in a Decrease in Boron Concentration in the Reactor Coolant with Failure of Isolation Valve（State A: Power Operation: Automatic Control）

12.10.8.1.1 Description

This section provides the diverse protection demonstration of the RCV [CVCS] boron dilution events with failure of isolation valve at power operation in automatic control mode.

12.10.8.1.2 Acceptance Criteria

The acceptance criteria for this event are decoupling criteria of DBC-4 accidents. The following decoupling criteria are used in the DBC-4 analyses:

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

b) The fuel pellet melting at the hot spot must not exceed 10 % by volume, i.e. considering a cross section of the hottest fuel rod at the elevation of the power peak, less than 10 % of this area is allowed to reach the melting temperature.

c) For cases not involving the rapid transient of oxidation of the cladding, the peak cladding temperature must remain lower than 1482 ℃.

12.10.8.1.3 Main Safety Functions

a) Reactor trip

   Reactor trip is triggered by the “Overtemperature ΔT” or “Overpower ΔT” signal.

b) Dilution source isolation

   The RCV [CVCS] charging line is isolated by operator via closing RCV8211VP-

or RCV6512/6314VP-, and the RCP [RCS] seal injection line is isolated by operator via closing RCV8311VP-.

c) ASG [EFWS] start-up

ASG [EFWS] is actuated either by the “Steam generator level (wide range) low 2” signal.

c) RBS [EBS]

The RBS [EBS] pumps are started by the operator before the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

d) Controlled cooldown

The cooldown is performed via the VDA [ASDS] of SGs by the operator.

12.10.8.1.4 Typical Sequence of events

a) From the initiating event to controlled state

Boron dilution results in positive reactivity insertion. At the beginning of this event, Bank R insertion gradually compensates for positive reactivity insertion. When R bank inserts to “Bank R positon low 4”, the reactor power level and the average coolant temperature increase slowly with positive reactivity insertion. The reactor is protected by Overtemperature ΔT protection channel or Overpower ΔT protection channel. After reactor trip, the operator shall perform manual dilution source isolation (isolation of RCV [CVCS] charging line and RCP [RCS] seal injection line manually in the main control room) at 30 minutes and the controlled state is reached.

b) From Controlled State to Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurization according to specific rules:

1) Reactor coolant boration via the RBS [EBS].

2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

3) Reactor coolant depressurization via the normal or auxiliary pressurizer spray, and the PSV can be used when the pressurizer sprays are unavailable.

12.10.8.1.5 Results and Conclusions

For RCV [CVCS] boron dilution events at power operation conditions in automatic control mode, calculation results for all fuel cycles analyzed show that after reactor trip the operator has enough time to isolate dilution source manually before the core reaches criticality.

For DNB case, the minimum DNBR is greater than the design limit of { }. The detailed results are presented in Reference [70].

12.10.8.2 RCV [CVCS] Malfunction that Results in a Decrease in Boron Concentration in the Reactor Coolant with Failure of Isolation Valve (State A\B\C: Shutdown conditions)

12.10.8.2.1 Description

This section provides the diverse protection demonstration of the RCV [CVCS] boron dilution events with failure of isolation valve at shutdown condition.

12.10.8.2.2 Acceptance Criteria

Analysis for this event use the same criteria descripted in Sub-chapter 12.10.8.1.2.

12.10.8.2.3 Main Safety Functions

a) Reactor trip

   Reactor trip is triggered by the “high neutron flux (source range)” signal.

b) Dilution source isolation

   At the beginning of this event, the boron dilution results in a potential increase neutron flux. When the neutron flux reaches the setpoint, the “high neutron flux at shutdown” alarm (3Φ alarm) informs the operator that the dilution may happen. The RCV [CVCS] charging line is isolated by operator via closing RCV8211VP- or RCV6512/6314VP-, and the RCP [RCS] seal injection line is isolated by operator via closing RCV8311VP-.

c) ASG [EFWS] start-up

   ASG [EFWS] is actuated either by the “Steam generator level (wide range) low 2” signal.

e) RBS [EBS]

   The RBS [EBS] pumps are started by the operator before the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

f) Controlled cooldown

The cooldown is performed via the VDA [ASDS] of SGs by the operator.

12.10.8.2.4 Typical Sequence of events

a) From the initiating event to controlled state

As positive reactivity being inserted, the neutron flux increases and triggers the “high neutron flux at shutdown” alarm (3Φ alarm) informing the operator of the dilution. The neutron flux keeps increasing until “high neutron flux (source range)” signal triggers RT.

After reactor trip, the operator performs manual dilution source isolation (isolation of RCV [CVCS] charging line RCP [RCS] seal injection line manually in the main control room) and the controlled state is reached.

Under this state, the residual heat is removed by the VDA [ASDS] or RHR, and the feedwater is supplied by the ASG [EFWS]. Boric acid can be injected manually via RBS [EBS] following requirement of Operating Technical Specification (OTS).

b) From Controlled State to Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurization according to specific rules:

1) Reactor coolant boration via the RBS [EBS].
2) Reactor coolant cooldown via the secondary circuit using the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS]. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted.

12.10.8.2.5 Results and Conclusions

For each condition, the operator has at least 70 minutes of grace period before the core reaches criticality. The detailed results are presented in Reference [70].

12.10.9 RCCA Bank Withdrawal at Power with Mechanical Failure of ASG [EFWS]

For reactivity insertion faults, the primary heat-up will vaporise the secondary water. The low load lines of main feedwater still work. Hence, the failure of ASG [EFWS] would not lead to severe consequences and the most challenging fault for loss of ASG [EFWS] is: Total Loss of Feedwater, which is shown in Chapter13. With loss of ASG [EFWS], the heat removal would be performed by primary side with feed and bleed.

12.10.10 Uncontrolled Single RCCA Withdrawal with Mechanical Failure of ASG [EFWS]

The analysis is same as RCCA Bank Withdrawal at Power with Mechanical Failure of ASG [EFWS]. With the loss of ASG [EFWS], the heat removal would be performed by primary side with feed and bleed.

12.10.11 Isolatable Piping Failure on a System Connected to the Spent Fuel Pool with Fail to Isolate PTR [FPCTS] trains

The PTR [FPCTS] isolation valves are implemented and common cause failure is considered to be avoided [71].

12.10.12 Isolatable Piping Failure on a System Connected to the Spent Fuel Pool with Fail to Restart PTR [FPCTS] trains

Isolatable Piping Failure on a System Connected to the Spent Fuel Pool with Fail to Restart PTR [FPCTS] trains accident would lead to the loss of three PTR [FPCTS] trains, and water makeup by ASP could be used to maintain the spent fuel pool cooling. ASP [SPHRS] is upgraded to category 2 [63] and the water makeup by ASP [SPHRS] could be used to maintain the spent fuel pool cooling for this accident [72].

12.10.13 Inadvertent Closure of All Main Steam Isolation Valves with PSVs Fail to Open

12.10.13.1 Description

This fault is defined as the inadvertent closure of all main steam isolation valves (MSIVs) with all pressuriser safety valves (PSVs) fail to open at the initial moment, which leads to a decrease in heat removal by the secondary system and an increase of the primary pressure. This fault may cause the occurrence of departure from nucleate boiling (DNB), make the fuel cladding failure, and challenge the integrity of pressure boundary for RCP [RCS].

12.10.13.2 Acceptance Criteria

The fuel integrity and integrity of RCP [RCS] might be challenged in this fault. The following acceptance criteria are used for this accident:

a) In terms of fuel integrity, the acceptance criteria for DBC-4 are applied:
   1) The amount of fuel rods experiencing DNB must remain lower than 10%.
   2) The fuel pellet melting at the hot spot must not exceed 10% by volume.
   3) The peak cladding temperature must remain lower than 1482℃.

b) In terms of integrity of RCP [RCS], the acceptance criteria for DBC-4 are applied to ensure the integrity of pressure boundary for RCP [RCS] system. Therefore, the pressure at the most loaded point shall not exceed 130% design pressure (22.37MPa abs) is defined as the decoupling criteria.

12.10.13.3 Main Safety Functions

The following plant safety functions are used to mitigate the event from the initiating events to the controlled state:

a) Reactor trip is actuated on “SG pressure high 1” signal or “Pressuriser pressure high 2” signal;

b) Turbine trips on “RT” signal;

c) VDA [ASDS] is opened by the “SG pressure high 1” signal;

d) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

   If the ASG [EFWS] are not actuated automatically, the operator will start the ASG [EFWS] manually. The SG levels are also controlled by operator with adjusting the flowrate of the ASG [EFWS].

b) Startup/Isolation of RBS [EBS]

The RBS [EBS] pumps are started by the operator at the beginning of the RCP [RCS] cooldown. The RBS [EBS] injection is stopped when the boron concentration of primary cold shutdown state is reached.

c) Startup of cooldown via VDA [ASDS]

The cooldown is performed via the VDA [ASDS] of available SGs. The cooling rates are { } with at least two RBS [EBS] trains in operation and { } if only one RBS [EBS] train is available.

d) RCP [RCS] depressurisation

The RCP [RCS] depressurisation is realized by Pressuriser (PZR) normal spray when the PZR normal spray or the PSVs are unavailable.

e) Accumulators isolation

The accumulators are isolated when the RCP [RCS] pressure is lower than 7.0MPa abs.

f) Connection of RIS [SIS] in RHR mode

The connection of the RIS [SIS] in RHR mode guarantees a continuous heat removal and core long term cooling.

12.10.13.4 Typical Sequence of events

For this accident, the typical events sequence can be divided into the following two stages:

a) From the initiating event to the controlled state

During the transient, the primary pressure and secondary pressure increase gradually, reactor trip can be triggered by the “SG pressure high 1” signal or “Pressuriser pressure high 2” signal.

After reactor trip, residual heat is removed by the VDA [ASDS] of all available SGs. If ARE [MFFCS] is not available, the feedwater supply is ensured by ASG [EFWS]. Then the RCP [RCS] will remain stable and the controlled state is reached.

b) From the controlled state to the safe state

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration is performed via the chemical and volume control system RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit uses the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS] train. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation is performed by the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.10.13.5 Results and Conclusions

The calculation results show that the minimum DNBR is greater than the design limit and the maximum pressure of the RCP [RCS] is lower than 130% RCP [RCS] design pressure. All the acceptance criteria are met. Detailed analysis results can be found in Reference [73].

For this accident, no DNB occurs and the limit of fuel pellet temperature and cladding temperature are not challenged, and the integrity of the pressure boundary for RCP [RCS] system is ensured during the transient.

In terms of radiological consequence, it is represented by “Turbine Trip” fault. Since there is no challenge of fuel integrity and primary circuit integrity, the radiological consequence is very limited. Turbine trip is analysed quantitatively in terms of radiological consequence, which can represent this kind of accidents with a VDA [ASDS] releasing pathway.

12.10.14 Containment Isolation

Containment isolation is performed by isolation valves and mainly influences the confinement of radiological substances in case of accidents. There are two redundant valves for containment isolation, one inside the containment and one outside the containment. The containment isolation valves or components are diversified to avoid common cause failure [74].

12.10.15 MSIV Fail to Close

Each loop of secondary locates one MSIV. The redundant drive solenoid valves improve the reliability of closing MSIV. Concerning the isolation of affected SG in SGTR (one tube) event, the component flashboard is decided to be diversified [75].

12.10.16 Isolatable Piping Failure on a System Connected to the Spent Fuel Pool with Fail to Stop PTR [FPCTS] trains

Isolatable piping failure on a system connected to the spent fuel pool with failure to stop PTR [FPCTS] trains mainly focuses on the extra functions of providing mechanical supporting for the performance of safety functions. If the PTR trains were

unable to be stopped during the accident, the low pressure at the inlet of the PTR pumps would cause cavitation, leading to the damage of the pumps. In this case, spent fuel pool might not be cooled by PTR [FPCTS] and water makeup by ASP [SPHRS] could be used to maintain the spent fuel pool cooling. The analysis would be bounded by Isolatable Piping Failure on a System Connected to the Spent Fuel Pool with Fail to Restart PTR [FPCTS] trains.

12.10.17 ATWS by Rods Failure - Spurious Pressuriser Heater Operation

12.10.17.1 Description

This subchapter provides the diverse protection demonstration of spurious pressuriser heating with ATWS.

12.10.17.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

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

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

c) The peak cladding temperature must remain lower than 1482℃;

For this accident, the acceptance criteria of no DNB and no fuel melting are conservatively applied. If the minimum DNBR remains above the design limit { }, the criteria are met. In addition, the highest pressure of primary circuit should be under 130% design pressure (22.37MPa abs) to ensure the primary integrity.

12.10.17.3 Main Safety Functions

The following control and protection systems are considered in the event:

a) Reactor trip signal

Reactor trip is triggered by the “Pressuriser pressure high 2” signal automatically.

b) “ATWS” signal

The high rod position combined with reactor trip signal triggers the “ATWS” signal.

c) Turbine trip

The reactor trip signal triggers the turbine trip.

d) Reactor coolant pumps stop

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

e) ASG [EFWS] operation

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

f) ARE [MFFCS] operation

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

g) Pressuriser Safety Valve (PSV) open and close

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

h) VDA [ASDS] open and close

The VDA [ASDS] opens and closes automatically when the pressure reaches the setpoint to limit the secondary pressure.

i) RBS [EBS] operation

The “ATWS” signal initiates three trains of the RBS [EBS] automatically.

12.10.17.4 Typical Sequence of Events

In ATWS by the spurious pressuriser heating event, the pressure of primary circuit keeps increasing and thus it triggers the reactor trip on “Pressuriser pressure high 2” signal. However, the reactor does not shutdown as the RCCAs fail to drop. This accident leads to a significant increase in the primary pressure and temperature.

The turbine trip and ARE [MFFCS] full load isolation are actuated by reactor trip signal. Once it is detected that the rods are still at high positions, the ATWS signal is triggered. The pumps of RCP [RCS] 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 trip, the steam is discharged either by the GCT [TBS] or the 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 the PSV. 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 also begin to drop. The RBS [EBS] boron injection ensures that the core remains subcritical in the long term.

12.10.17.5 Analysis Assumptions

The detailed assumptions are presented in Reference [76]. The main assumptions are listed as follows:

a) Initial Conditions

1) The initial power is assumed at full power plus uncertainty (102%FP) to maximise primary heat;

2) Initial reactor coolant average temperature is assumed at its nominal value plus uncertainty (309.5℃) to minimise the DNBR;

3) Initial pressuriser pressure is assumed at its nominal value minus uncertainty (15.25MPa) to minimise the DNBR;

4) Initial reactor coolant flowrate is assumed to be the thermal design flow (24000m^3/h/loop), considering 10% tube plugging of SGs, so as to penalise the heat removal.

b) Core-related Assumptions

1) The core power decreases due to the negative feedback effect of the reactor coolant before the RBS [EBS] boron injection. The moderator temperature coefficient is the most sensitive value in the analysis. The Beginning of Cycle, Equilibrium Xenon (BCX) of the first cycle is considered in the analysis, because the moderator temperature coefficient is the minimum (absolute value) in all cycles.

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

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

c) Reactor Protections

1) Reactor trip is triggered by the “Pressuriser pressure high 2” signal;

2) ATWS signal is actuated by the “High rod position” (at least 2 control rods cannot be inserted) combined with reactor trip signal;

3) The reactor trip signal triggers the turbine trip automatically;

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

5) RBS [EBS] is actuated by the the ATWS signal;

6) ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

7) VDA [ASDS] is actuated by the “SG pressure high 1” signal;

8) PSVs are opened when the pressuriser pressure reaches the setpoint.

d) System Performance

RBS [EBS] is actuated by the ATWS signal. The RBS [EBS] boron injection ensures that the core remains subcritical in the long term. The minimum flowrate of RBS [EBS] is assumed.

12.10.17.6 Results and Conclusions

The calculation result shows that the minimum DNBR of spurious pressuriser heating with ATWS event is { }, which is greater than the limit { }. It also confirms that the peak primary pressure is 17.98 MPa abs, which is far from the maximum allowable pressure (22.37 MPa abs) with a large margin, and will not challenge this criterion.

The fault analysis shows that the protection system provides sufficient protection for the reactor. All the acceptance criteria are met. The detailed results are presented in Reference [76].

In terms of radiological consequence, this fault is represented by “Small Break - Loss of Coolant Accident (State A)” fault considering that fuel integrity is maintained and primary integrity is temporarily breached by opening of PSV during this transient. The radiological consequence of “Small Break - Loss of Coolant Accident (State A)” fault is analysed quantitatively, which can represent this kind of accidents with potential containment and VDA [ASDS] releasing pathway.

12.10.18 Conclusions

The validity of diverse protection lines provided in UK HPR1000 Fault Schedule is proved by the diverse line analyses. This is demonstrated in three ways:

a) Optioneering is performed to solve diversity findings;

b) Transient analyses show that the diverse protection lines limit consequences and satisfy the acceptance criteria;

c) Assessment on radiological consequences shows that radiological consequences of diverse sequences can be represented by design basis conditions.

Justification/optioneering is performed to solve the identified shortfalls. The analyses for the bounding cases show that all acceptance criteria are met, which means the acceptance criteria are met and overpressure is prevented. The safe state is achieved for all the bounding cases.

For the radiological consequences, qualitative judgment is given for each bounding case. The diverse sequences can be represented by one of the following faults:

a) Small Break - Loss of Coolant Accident (State A);

b) Spectrum of RCCA Ejection Accident;

c) Dropping of Fuel Assembly;

d) Turbine Trip.

The radiological consequences of these faults are within the limits of basic safety level of Radiation Protection Target 4.

12.11 Radiological Consequences of Design Basis Accident

12.11.1 Safety Requirements

12.11.1.1 Safety Objectives

The nuclear safety objective of the UK HPR1000 is as follows, which is also defined in PCSR Chapter 4: The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defenses to fulfill the fundamental safety functions, reducing the nuclear safety risks to a level that is ALARP.

The safety objectives for DBCs radiological consequence analysis is to verify that the plant systems are appropriately designed and operated from the point of view of radiological release. It also aims to show that the doses to the public and on-site workers following a discharge of radioactivity of the plant does not exceed the radiological consequence acceptance criteria.

12.11.1.2 Design Requirements

In order to judge the adequacy of radiological hazard control for DBC accidents, radiation protection targets are set in Reference [4]. This reference gives a set of targets for the effective dose received by any person from a DBC fault sequence and which are set in terms of a Basic Safety Level (BSL) and a Basic Safety Objective (BSO). The BSLs should be met in the first place, especially the mandatory legal limits. The region under BSO represents the broadly acceptable region. For the UK HPR1000 nuclear power plant, the maximum effective dose received by any person arising from the DBCs should meet the requirement of these targets.

12.11.2 General Statements and Assumptions

The purpose of this section is to present the main assumptions and inputs to radiological consequence evaluation of the DBCs, including:

a) The activity inventory;

b) The activity release, including release fraction, timing of release phases, radionuclide composition and the chemical form of radioactivity release;

c) Radionuclides released into the environment;

d) Radionuclide release transfer in the Environment;

e) Off-site dose calculations;

f) On-site dose calculation (MCR);

g) On-site dose calculation (other than MCR)

12.11.2.1 Activity Inventory

When the accident involves fuel failure, radioactivity may be released from the fuel, primary coolant or secondary coolant.

a) Core Inventory

When the integrity of fuel rods fails, the radioactivity in the fuel of the reactor core is released to the primary coolant, then to the containment or secondary side. Conservative reactor core activity inventory is considered for the source term calculation.

b) Primary Coolant Activity

The primary coolant source term for the UK HPR1000 is presented in *Primary Source Term Calculation Report* (see Reference [77]). The phenomenon of iodine spiking, which will cause the radioactive iodine concentration in the primary coolant to increase significantly, is considered in the source term analysis.

c) Secondary Coolant Activity

Under normal operating conditions, the secondary system is mostly free of radioactivity because of the leak-tight steam generator tubes. However, limited primary-to-secondary leaks through the SG tubes are considered in the analysis during normal plant operation. To calculate the initial secondary coolant activity in the accidental transient, the primary-to-secondary leak, decay of nuclides and the purification of the blowdown system of the secondary system are all taken into consideration. The SG primary-to-secondary leakage is continuously monitored and limited to reduce the transient consequences. The maximum admissible leak rate and the minimum SG blowdown flowrate are used to calculate the initial secondary coolant activity.

12.11.2.2 Activity Release

12.11.2.2.1 Activity Release Following Fuel Failure

a) Release fraction

Based on the thermal-hydraulic transient analysis results, the radioactive release fractions from the fuel are conservatively considered for the design basis accidents.

For the DBC LOCAs, the estimated release fractions for a fuel gap release are as follows [78]:

- Noble Gases: 5%,
- Halogens: 5%,
- Alkali Metals: 5%.

For an RCCA ejection accident, the gap release fractions are 10% for noble gases and iodines, 12% for Alkali Metals [78].

For other non-LOCA events, the estimated core inventory fractions for gap release are assumed to be 8% for I-131, 10% for Kr-85, 5% for other noble gases, 5% for other halogens and 12% for alkali metals [78].

b) Timing of Release Phases

Generally, radioactivity release for the fuel failure occurs at the point of fuel failure. For DBC LOCAs, the onset of the radioactivity release from fuel failure is conservatively considered as 30 seconds after the initiation of the accident. For non-LOCA DBCs in which fuel damage occurs, the radioactivity release from the fuel gap and fuel pellet is assumed to occur instantaneously at the onset of the fuel damage.

c) Radionuclide Composition

The elements in each radionuclide group considered in the radiological consequence analysis are listed in T-12.11-1.

T-12.11-1 Elements in Each Radionuclide Group Discussed in the Radiological Consequence Analysis

Radionuclide group	Nuclide elements
Noble gases	Kr, Xe
Halogens	I, Br
Alkali metals	Cs, Rb
Tellurium group	Te, Sb, Se, Ba, Sr
Noble metals	Ru, Rh, Pd, Mo, Tc, Co
Lanthanides	La, Zr, Nd, Eu, Nb, Pm, Pr, Sm, Y, Cm, Am,Ce
Cerium	Pu, Np

d) Chemical form

The iodine released from the RCP [RCS] to the containment in the postulated accident is assumed to be in various chemical forms, of which 95% is cesium iodine, 4.85% is elemental iodine, and 0.15% is organic iodine [78]. The fission products released into the containment are all assumed to be in particulate form, except for elemental iodine, organic iodine and noble gases. During the radioactivity transporting process, the chemical form may be changed and will be analysed according to the specific accident.

12.11.2.2.2 Activity Release Following the Discharge of Liquid

Liquids discharged to the containment or peripheral buildings will partially flash into

the atmosphere. For noble gases, 100% of the noble gases in the discharged liquids are released into the ambient atmosphere instantaneously.

For iodine and other solids in the discharged liquids, the release fraction to the atmosphere is determined by flash fraction and partition coefficient[79]. The flash fraction of the discharged liquid is calculated assuming that the discharge is a constant enthalpy process.

12.11.2.2.3 Activity Release Following the Moisture Carryover from the Steam Generator

Radioactive release to the environment through the Steam Generator is determined by SG tube status. Two cases are considered:

a) Radioactivity release to the secondary system through operational SG leakage;

b) Radioactivity release to the secondary system following SGTR.

For the first case, four following representative DBCs are considered:

1) Turbine Trip;

2) RCCA Ejection Accident;

3) Steam System Piping Large Break;

4) Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break.

For the second case, two following representative DBCs are considered:

1) Steam Generator Tube Rupture (One Tube);

2) SG Tube Rupture (Two Tubes in One SG).

a) Activity Carryover in the case of operational leakage

In accidents with operational leakage in the SG, the primary coolant containing radionuclides passes from the primary side to the secondary side, due to the pressure difference between two circuits. The leak results in a build-up and an increase in radioactivity concentration of the secondary coolant during the transients.

The reactor coolant leaking into the steam generators is assumed to mix with the secondary water. As steam is released, a portion of the iodine and alkali metals in the coolant is released. Release from the secondary coolant is limited by the assumed SG moisture carryover. The noble gas activity entering the secondary side is assumed to be released to the environment directly. For the iodine and alkali metals, it is assumed that the leakage from the primary circuit to the secondary circuit enters into the liquid phase and mixes with the water, and which is then carried by secondary circuit steam and discharged into the environment. The release fraction is determined by the steam

flowrate and carryover factors. The carryover factors are assumed to be 1% for iodines and 0.25% for alkali metals [79].

b) Activity Carryover in case of SGTR accident

In an SGTR accident, two different situations could arise, depending on whether the tube break is submerged. In either case, noble gases are conservatively assumed to be immediately transported to the main steam, released to the environment without reduction or mitigation. Due to its volatility, elemental iodine that enters SGa will all release to the environment through open VDA [ASDS]. For particulate iodine and alkali metals, following assumptions are used.

1) If the tube is submerged, the primary-to-secondary leakage can be assumed to mix with the secondary water. Particulate iodine and alkali metals in the bulk water are carried by steam and then discharged into the environment. The partition factors are 0.0025 for particulate iodine and for alkali metals [79].

2) If the tube is uncovered, a portion of break flow flashes into steam, the radioactivity carried in the flashed coolant is directly released to the environment without mitigation. The radioactivity in the remaining coolant mixes homogeneously with the secondary water. The flash portion of the break flow is calculated according to the thermodynamic conditions of the primary coolant and the secondary side.

12.11.2.3 Radionuclides Released into the Environment

12.11.2.3.1 Containment Leakage Rate

The containment is the third safety barrier of a nuclear power plant for preventing the release of radioactive material to the environment. It normally contains very small leaks originating from the manufacturing and construction processes. Appropriate leakage and strength tests, which are to be performed in the course of commissioning of the plant as well as at regular intervals during in-service inspections, would ensure that the realistic leak rate is lower than the limiting value in the Operation Technical Specification. The containment leakage rate considered is as follows:

a) 0-24h: peak pressure technical specification leak rate (0.3%/d) specified in the OTS;

b) >24h: reduced to 50% of the technical specification leak rate (namely 0.15%/d) [79].

In accidental conditions, the containment and system design can ensure that the peak containment pressure is lower than the design criteria of the containment. The above leakage rate adopted in the radiological consequence analysis is conservative.

For the overall containment leakages, it is assumed that:

a) 40% of the overall leak rate are collected and filtered in the annulus;

b) 60% of the overall leak rate are collected and filtered in surrounding buildings.

These assumptions are:

a) Initially based on experience feedback from nuclear power plants (type B/C containment leak tightness periodic tests);

b) Consistent with the Standard in Reference [80]: the global leakage through containment penetrations shall not be above 60% of the overall containment leak rate.

12.11.2.3.2 Ventilation System

During power operation, there is no sweeping ventilation of the containment atmosphere, and all the containment isolation valves are closed. However, when access to the service area is necessary, the low-capacity circuit of the Containment Sweeping and Blowdown Ventilation System (EBA [CSBVS]) is started for the purpose of sweeping, several days before and throughout access, in order to ensure a level of atmospheric contamination compatible with the staff access.

It is conservatively assumed that the EBA [CSBVS] low-capacity circuit is operating at its maximum flowrate. At the start of the accident, containment isolation is initiated by the reactor protection system. All containment isolation valves of the low-capacity EBA [CSBVS] circuit are closed.

The extracted air is released at the stack after being filtered by one of the EBA [CSBVS] filtration trains. However, the retention effects of the EBA [CSBVS] filters are conservatively not taken into account for this analysis.

During normal operation, the normal-operational train of the Annulus Ventilation System (EDE [AVS]) operates continuously to create and maintain a sub-atmospheric pressure in the annulus. The exhaust air is discharged via filters to the vent stack. In the analysis, these filters are not taken into account.

During an accident, the annulus is maintained at sub-atmospheric pressure in order to collect the inner containment leakages including those collected by the containment leakage rate and monitoring system. During the accident, the EDE [AVS] switches automatically to the safety trains to process leakages from the reactor building containment. The normal-operational train is automatically isolated by motorised isolation dampers on the containment isolation signal. The fan on the safety train and the electric heater are started, thus maintaining the required sub-atmospheric pressure in the annulus. The leakage from the containment is mixed and diluted in the annulus before release via the EDE [AVS]. The maximum EDE [AVS] flowrate is considered in the accident.

The activity inside the annulus is assumed to be homogeneously distributed and to be

discharged into the environment via the stack through accident filters at the ventilation rate of the EDE [AVS]. The filter efficiencies are postulated as follows:

1) Noble Gases: 0.0%,

2) Organic Iodine: 99.0%,

3) Elemental Iodine: 99.0%, and

4) Aerosols: 99.9%.

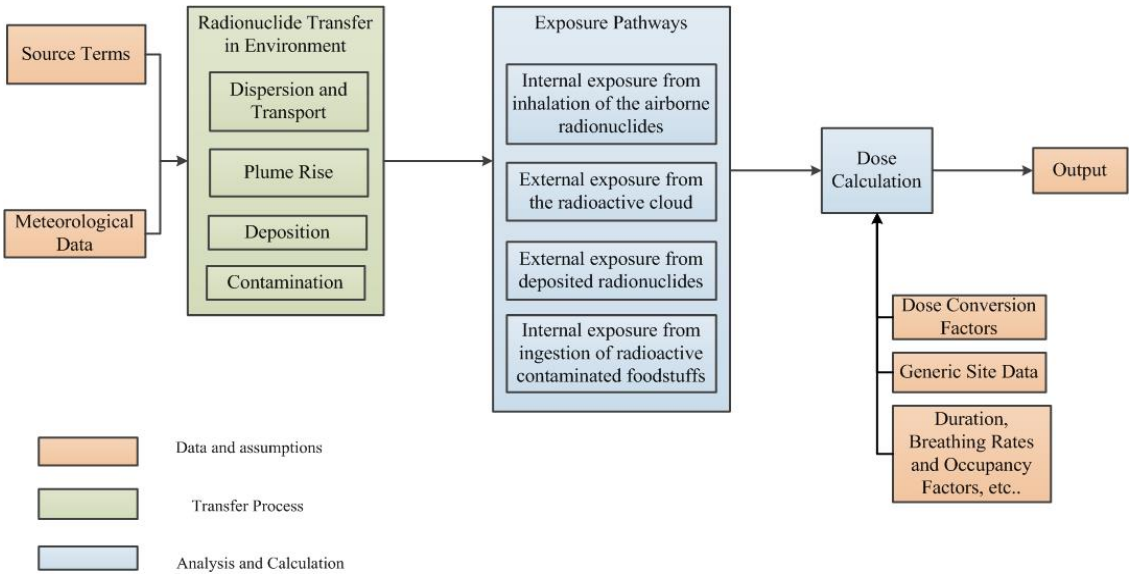
These values are conservative, and the actual filtration efficiencies are higher.

12.11.2.4 Radionuclides Released Transfer in the Environment

a) Atmospheric Dispersion Assessment for Public

For UK HPR1000, the methodology for off-site dose evaluation is developed based on UK context and RGPs to fill the gaps between the practice for Hua-long Pressurized Reactor under construction at Fangchenggang nuclear power plant unit 3 (HPR1000 (FCG3)) and requirements of the UK context. To assess the radiological consequence for DBAs against the off-site radiation protection targets for a design basis fault sequence, the conservative deterministic method is adopted. And the methodology is developed and brief introduced in *Off-site Radiological Consequences Analysis Methodology for DBC Accidents of UK HPR1000*, Reference [81].

Radiological materials are potentially released to atmosphere from the on-site facilities in accidents and transported in the environment through dispersion and deposition process. These may cause potential effective doses to the off-site persons from several different exposure pathways. The analysis process is presented in F-12.11-1.



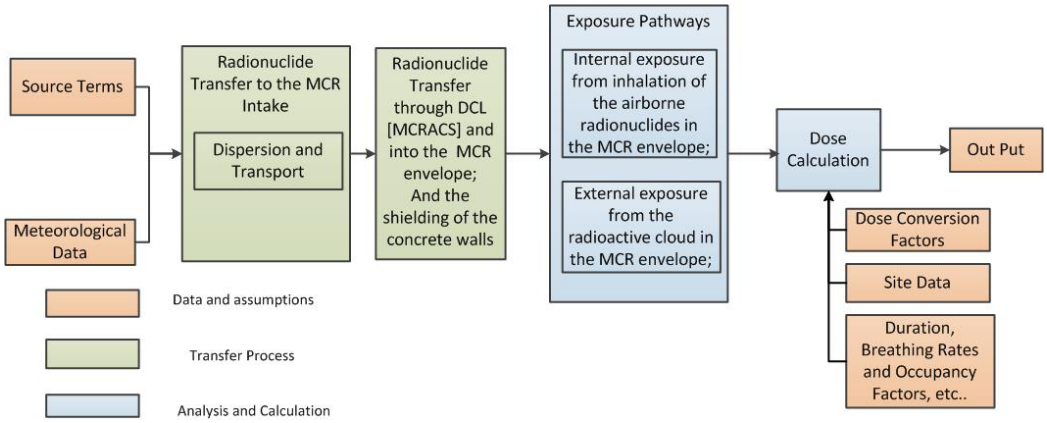
F-12.11-1 Off-site Radiological Consequences Analysis Scheme

As the transfer progress, radionuclides released to atmosphere are dispersed and transferred to the vicinity, and finally deposited on the ground or other surfaces. For off-site dose calculation, the UK Atmospheric Dispersion Modelling Liaison Committee provides the guidance of atmospheric dispersion and a list of available software which including the Atmospheric Dispersion Modelling System (ADMS) range of software. The ADMS Version 5.0 is a practical, short-range dispersion model that simulates a wide range of buoyant and passive release to the atmosphere either individually or in combination. The basic dispersion model is Gaussian model. It is included in the list of available software which is collated by the National Radiological Protection Board (NRPB) which became part of Public Health England, based on the agreement at the Atmospheric Dispersion Modelling Liaison Committee meeting. For UK HPR1000, the atmospheric dispersion model ADMS Version 5 is used to calculate activity concentrations in air per unit discharge, deposition rate per unit discharge and the cloud gamma doses for the nuclides shown in the gaseous source term. There are partial amount of radioactive material which is deposited on plants and animals and transferred into foodstuffs which may be consumed by the local public. For UK HPR1000, the atmospheric dispersion model ADMS Version 5 is used to calculate activity concentrations in air per unit discharge and deposition rate per unit discharge for the nuclides shown in the gaseous source term.

The meteorological data of generic site is assumed and built up which is typical value set out in relevant context. Generic site environmental parameters are used for calculating the atmospheric and ground concentrations of radioactive material.

b) Atmospheric Dispersion Assessment for MCR

For the radiological consequences analysis for the worker in the main control room, there is no gap were identified between the methodology used for HPR1000 (FCG3) (Reference [81]), and requirements of the UK context. The methodology used for UK HPR1000is detailed recorded in *On-site (MCR) Radiological Consequences analysis for Representative DBC Accidents of UK HPR1000*, Reference [82], and progress of the radiological consequences analysis for the MCR worker is presented as F-12.11-2.



F-12.11-2 Radiological Consequences Analysis Scheme for the Worker in the MCR

The radiological material released after the postulated accident disperses to the MCR intakes, and enters the MCR envelope after the filtration of the Main Control Room Air Conditioning System (DCL [MCRACS]). The radionuclides concentration at the intake of the DCL [MCRACS] is evaluated. The basic model is a straight-line Gaussian model that assumes the release rate is constant for the entire period release. The ground-level, vent, and elevated releases can be evaluated. Building wake effects are considered in the evaluation of relative concentrations from ground-level releases. The diffusion coefficients in this model consider both low-wind speed meander and wake effects. The hourly meteorological data are adopted. It combines the hourly averages to estimate concentrations for periods ranging in duration from 2 hours to 30 days. The relative concentrations for five periods used in the MCR habitability assessments are calculated from the 95th percentile relative concentration.

12.11.2.5 Off-site Dose Calculations

As the dose analysis progress in Figure F-12.11-1, to calculate the effective dose for off-site public, following an accidental release of radionuclides to atmosphere, exposure pathways are included as follows:

a) Internal exposure from inhalation of the airborne radionuclides,

b) External exposure from the radioactive cloud,

c) External exposure from deposited radionuclides,

d) Internal exposure from ingestion of radioactive contaminated foodstuffs.

It is necessary to take the age group of the exposed population into account for assessing the exposure of the general public. Although the breathing and ingestion rates of infants and children are lower than the rates of adult, the dose coefficients for infants and children are generally greater than those for adults. Therefore, infants and children may receive higher individual doses from a source of exposure than adults. Adults, children and infants are adopted to cover all age groups of the hypothetical person. These persons are conservatively assumed to reside at, and source their food from 500m downwind of the radioactivity release point. And the exposure and integration periods for long-term exposure pathways are assumed as the 50 years for adult and the 70 years for child and infant; the exposure and integration periods for long-term exposure pathways are assumed as the duration of accidental release. The habits data of these persons, including the breathing rates, food consumptions, and occupancy data adopt the UK generic data.

The detailed methods, parameters and values of inputs (expect the source terms) are also listed in Reference [81].

12.11.2.6 On-site dose calculation (MCR)

Following the progress shown in F-12.11-2, in the compartment dose assessment

models, the MCR envelope is simulated as a finite-size compartment. Relevant physical processes are considered, including shield, fresh air filtration, recirculation filtration, leakage, deposition, decay and etc. The released radiological materials are transported to the intake of compartments as the air disperses. The MCR does not intake radioactivity directly from other buildings. The integrated activity in MCR over the emergency response period is calculated.

The parameters of DCL [MCRACS], such as filter efficiency, filtered fresh air volume and filtered recirculation volume, and the parameters of MCR, such as the free volume of MCR are the inputs of calculated integrated activity in MCR.

To calculate the effective dose for worker in MCR, following an accidental release of radionuclides to atmosphere, exposure pathways are included as follows:

a) Internal exposure from inhalation of the airborne radionuclides,

b) External exposure from the internal radioactive cloud,

Based on the finite size of a compartment, the internal cloud shine doses in a compartment caused by the radioactive cloud will be less than the doses caused by immersion in a finite cloud shine. The internal cloud shine doses are calculated using Murphy's method, which models the compartment as a hemisphere.

The detailed model, parameters and values of inputs (expect the source terms) are listed in Reference [82].

12.11.2.7 On-site dose calculation (other than MCR)

Based on the categories of workers, the assumptions for the worker dose assessment during fault and accident conditions are as follows:

a) Accident intervention workers are participated in the accident mitigation operations. Accident intervention workers include MCR workers and local accident intervention workers. The MCR workers do the operations in MCR and the local accident intervention workers need to access to site and carry out local operations. The exposure duration of local accident intervention workers depends on the operation time and the time spent on the way to and from the operation location. The detailed assumptions for operation time calculation for local accident intervention workers are described in DBC Operator Distribution Report, Reference [83].

b) For the accidentally involved workers and the other workers, dose is dependent on the radioactive release of the accident and the time of the person discovers the accident and evacuates. For workers in the release room, considering that these areas usually are designed with radiation monitoring, and the corresponding alarm signal will be triggered after the accident, workers could be immediately aware of the accident. So the exposure time is assumed to be 10 min, which is a good practice. In addition, alarming Electronic Personal Dosimeter (EPD) wore by worker could help

to increase the likelihood of early evacuations. For workers not in the release room, corresponding alarm signal of radiation monitoring, alarming EPDs, emergency signal of buildings etc. could help to make the workers aware of the accident and 1 hour is assumed for discovering and evacuation, which is a good practice.

c) The accessibility of areas which accidentally involved workers and other workers to be presented are needed to be assessed. If the radiation zone of areas where accident occurs is the red zone or the orange zone during normal operation conditions, the workers are not supposed to be inside the areas when accident occurs.

12.11.3 Radiological Consequence Evaluation Process

To assess the radiological consequences for DBCs against the on-site and off-site radiation protection targets for a design basis fault sequence, source terms are analysed firstly based on the thermal-hydraulic analysis, then on-site and off-site radiological consequences analysis are carried out. Conservative deterministic methods are used. Physical processes and phenomena are analysed with conservative, bounding assumptions.

12.11.3.1 Source term evaluation

The work stream for source term analysis is as follows:

a) Illustrate the activity source and source term release paths for each DBC scenario.

b) Identify the key inputs, assumptions and models which have a nuclear safety significance and impact on the radiological consequences analysis for DBC. An appropriate and prudent safety margin is considered to compensate for uncertainties in facility parameters, accident progression, and radioactive material transport.

c) Provide appropriate and proportionate evidence to support the assumptions made and models used, which will be presented on a case-by-case basis.

d) Solve the radioactivity balance equations considering the source of release, activity transport and retention mechanisms and get the source term results.

Source term results including the quantity of radioactivity, duration of release, rate of release, physical and chemical characteristics of the radionuclides released and height of release point combined with the frequency of the initiating event are used as inputs for dose evaluation to the on-site and off-site persons.

12.11.3.2 Dose evaluation to persons on the site (MCR)

Following the MCR worker radiological consequences analysis progress shown in Figure F-12.11-2, the steps include:

a) Calculating the air concentration per unit discharge for different time intervals;

b) Calculating the effective doses of MCR worker based on the representative DBC accidents;

c) Comparing the effective dose with the requirements of Radiation Protection Target 4 to get conclusion.

Detailed progress and results of radiological consequences analysis is presented in Reference [82].

12.11.3.3 Dose evaluation to persons on the site (other than MCR)

The on-site radiological consequence evaluation of the UK HPR1000 includes the following steps:

a) Determining the design basis accident lists for the analysis of the Radiation Protection Target 4;

b) Identifying the types of operations of the workers under the design basis accidents and grouping the workers;

c) Calculating the exposure dose of workers under each design basis accident;

d) Comparing the largest exposure dose with the requirements of Radiation Protection Target 4 to get conclusion and further finish ALARP demonstration.

Detailed methodology of on-site worker dose assessment is presented in Reference [84].

12.11.3.4 Dose evaluation to persons off the site

Following the off-site radiological consequences analysis progress shown in Figure F-12.11-1, the steps include

a) Calculating the air concentration per unit discharge for different time intervals and deposition rates per unit discharge for different time intervals;

b) Calculating the effective doses of each age group for the representative DBC accidents;

c) Comparing the largest effective dose among age groups with the requirements of Radiation Protection Target 4 to get conclusion.

Detailed progress of off-site radiological consequences analysis is presented in *Off-site Radiological Consequences analysis for Representative DBC Accidents of UK HPR1000,* Reference [85].

12.11.4 Analysis for Radiological Representative DBC Accidents

The radiological release following Design Basis Conditions (DBC) should meet the Radiation Protection Target (RPT) 4. For certain types of DBCs, the radiological release characteristics are quite similar, including condition of the fuel integrity,

primary circuit boundary integrity and potential release paths or locations. In addition, the radiological consequences of some DBCs can be bounded by other DBCs. Thus, it is not necessary to calculate the radiological releases of all DBCs.

Radiological representative faults are identified and listed in the following table from radioactivity release aspect for each type of accidents with the same radiological activity release characteristics after qualitative analysis. Radiological consequence of these radiological representative DBCs are quantitatively analysed in this section. The description and justification on "radiological bounding fault" are described in each DBC transient analysis section from Sub-chapter 12.7 to Sub-chapter 12.9.

It should be noted that, “Large Break Loss of Coolant Accident (LB-LOCA) (up to Double-ended Guillotine Rupture)” is a special fault for the radiological consequence analysis, although it is not included in the DBC-4 list.

T-12.11-2 Radiological Representative DBC List

Design Basis Fault Sequence Frequency	DBC Category	NO.	Title of Radiological Representative DBC
$>1 \times 10^{-3}$	DBC-2	1	Turbine Trip
	DBC-3	2	SG Tube Rupture (SGTR) (One Tube)
	DBC-3	3	Small Break (Loss of Coolant Accident) (SB-LOCA)
1×10^{-3} -1×10^{-4}	DBC-3	4	Rupture of a Line Carrying Primary Coolant outside Containment
	DBC-3	5	Volume Control Tank Break
1×10^{-4} - 1×10^{-5}	DBC-4	6	Spectrum of RCCA Ejection Accident
	DBC-4	7	Steam System Piping Large Break
	DBC-4	8	Large Break Loss of Coolant Accident (LB-LOCA) (up to Double-ended Guillotine Rupture)
	DBC-4	9	SG Tube Rupture (SGTR) (Two Tubes in One SG)
	DBC-4	10	RHR System Piping Break inside (outside) Containment (≤DN 250)
	DBC-4	11	Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break
	DBC-4	12	Dropping of Fuel Assembly
	DBC-4	13	Dropping of Spent Fuel Cask

12.11.4.1 Turbine Trip

12.11.4.1.1 Description

The turbine trip accident results in the loss of steam flow rate, leading to the reduction of secondary circuit heat removal ability. In chapter 12.7.2, the transient thermal-hydraulic characteristics of the accident have been analysed.

During the transient, the contaminated primary coolant is transferred into the secondary side through primary-to-secondary leakage, causing an increase in the activity concentration of the secondary circuit. During the primary circuit cooldown, the contaminated steam is released to the environment through the atmospheric steam dump system (VDA [ASDS]). The radionuclides are released directly to the environment through VDA, causing radiological consequences to the people off the site. In addition, the contaminated steam in the steam lines may cause a radiation on the workers that working near the steam pipelines. When the RIS [SIS] train is connected to the primary system in RHR mode to remove the decay heat, the radionuclides release through the VDA [ASDS] is terminated.

12.11.4.1.2 Main Safety Functions

In Reference [18], the main safety functions for reactor core protection are described. There are no additional safety functions for radiological release mitigation claimed.

12.11.4.1.3 Source Term

12.11.4.1.3.1 Radioactivity Released into the Environment

When the accident occurs, the loss of steam flow rate leads to the reduction of secondary circuit heat removal ability, resulting in the increase of primary temperature and pressure. The thermal-hydraulic analysis results show that the fuel rods do not experience DNB, and that the maximum fuel pellet temperature is lower than the melting temperature. A concurrent iodine spiking model is used in the analysis. The primary coolant activity during the transient is determined assuming that the iodine release rate from the fuel rods increase to a value 500 times of the equilibrium release rate during normal operation.

During the transient, radionuclides carried in the primary coolant transfer to the secondary side through primary-to-secondary leakage, increasing the activity of secondary water.

When the VDA [ASDS] is automatically put into operation to remove the decay heat, radionuclides in the secondary side are released to the environment through VDA [ASDS]. During the process, the temperature and pressure continue to decrease.

When the primary coolant conditions satisfy the operation conditions of RHR system, the RIS [SIS] train is connected to the primary system in RHR mode. The VDA [ASDS] is isolated and radiological release through VDA [ASDS] is terminated.

12.11.4.1.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the main steam pipelines. The radionuclides are released into the secondary side through the primary-to-secondary leakage, causing an activity increase of the secondary circuit.

Noble gases released from the primary system are homogeneously distributed in the steam pipelines.

Iodine and alkali metals leaked from the primary system are mixed homogeneously with the secondary water. The concentrations of iodine and alkali metals in the vapor are determined by the partition factors. The partition factors of iodine and alkali metals are 0.01 and 0.0025, respectively.

The activity increase in the steam pipelines causes a radiation on the workers working near the steam pipelines.

Main assumptions and parameters used in the source term calculation are presented in Reference[86]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.1.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 8.55E-03mSv, 1.61E-02mSv, and 6.62E-02mSv, respectively. The off-site doses are between the RPT-4 BSO and BSL for frequent faults (BSO: 0.01mSv, BSL: 1mSv).

The maximum dose to workers on-site is 3.84E-04mSv. The on-site doses are far below the RPT-4 BSO of 0.1mSv.

12.11.4.2 Steam Generator Tube Rupture (One Tube)

12.11.4.2.1 Description

This accident is initiated by the double-ended guillotine rupture of one tube of a steam generator (SG) in full power operation condition.

During the transient, the contaminated primary coolant is released into the secondary side of SGa through the break, causing an increase in the activity concentration of the secondary circuit. When the MCD is initiated to cooldown the primary circuit, the contaminated steam is released to the environment through the VDA [ASDA].

The break mass flowrate and steam release mass flowrate are calculated through the thermal hydraulic analysis of this accident (see Sub-chapter 12.8.5.2). Regarding to the transient cases with the operator action time assumptions which are common practice for design basis analysis, and supplementary transient case with the operator actions timelines based on human reliability analysis, source terms are carried out. They are noted as “SGTR (one tube) without operator action time” and “SGTR (one tube) with operator action time”, respectively.

12.11.4.2.2 Main Safety Functions

In reference [45], the main safety functions for SGTR mitigation are described from core protection and thermal-hydraulic aspects. There are no additional safety functions for radiological release mitigation claimed.

12.11.4.2.3 Source Term

In this section, the source terms of SGTR (one tube) are analysed.

12.11.4.2.3.1 Radioactivity Released into the Environment

When the accident occurs, the contaminated primary coolant is released into the secondary side of SGa through the break, increasing the activity of secondary water. More realistic initial primary coolant activity 5GBq/t DEI is used in source term evaluation based on Reference [43].

The accident causes the primary pressure to decrease. An alarm is actuated on “high activity detection in the KRT [PRMS]” signal by the activity increase of the secondary circuit and the SGTR accident is detected.

When MCD is actuated to cooldown the primary circuit, the radionuclides carried in the steam are released to the environment through VDA [ASDS] of SGa and unaffected SGs.

The isolation of SGa is executed by operators. The SGa isolation actions include the isolation of ARE [MFFCS] and ASG [EFWS], closure of MSIV and an increase in the VDA [ASDS] setpoint. The primary system cooldown and depressurization are performed via the VDA [ASDS] of the unaffected SGs. The radionuclides in the

unaffected SGs, which are released through primary-to-secondary leakage, continue releasing to the environment through VDA [ASDS].

When the VDA [ASDS] of SGa is opened again for primary system depressurization, radionuclides in the SGa are released to the environment. The steam release through the VDA [ASDS] is terminated when the RIS [SIS] trains are connected to the primary system in RHR mode and the residual heat of the core can be removed by RIS [SIS] trains.

12.11.4.2.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the main steam pipelines. The radionuclides are released into the secondary side through the break or primary-to-secondary leakage, causing an activity increase of the secondary circuit. The activity increase causes radiation exposure to the workers working near the steam pipelines.

During the transient, radionuclides in the primary coolant transfer to secondary side through primary-to-secondary leakage or the break in the tube.

Noble gases enter the steam pipelines directly. Similar to noble gases, the elemental iodine released to secondary side is assumed to directly enter the steam pipelines. When the tube is submerged, particulate iodine and alkali metals mix with the secondary water and are carried to the steam pipelines by steam generated. When the tube is uncovered, a portion of particulate iodine and alkali metals are flashed into steam and enter the steam pipelines directly. Remaining particulate iodine and alkali metals in the break flow mix with secondary water, and are carried to the steam pipelines by the steam generated.

Main assumptions and parameters used in the source term calculation are presented in Reference [87]. The results are used as input data for the evaluation of radiological consequences of any person off site and any worker on site.

12.11.4.2.4 Dose Evaluation

For SGTR (one tube) without operator action time, the off-site effective doses of adult, child and infant are 4.24E-02mSv, 8.29E-02mSv, and 3.43E-01mSv, respectively. For SGTR (one tube) with operator action time, the off-site effective doses of adult, child and infant are 6.92E-02mSv, 1.36 E-01mSv, and 5.65E-01mSv, respectively. These off-site doses are all between the RPT-4 BSO and BSL for frequent faults (BSO: 0.01mSv, BSL: 1mSv).

The maximum dose to workers on-site is 2.36E-01mSv. On-site doses to workers are between the RPT-4 BSO and BSL for frequent faults (BSO: 0.1mSv, BSL: 20mSv) and is close to RPT-4 BSO.

12.11.4.3 Small Break - Loss of Coolant Accident (State A)

12.11.4.3.1 Description

A Small Break Loss of Coolant Accident (SB-LOCA) is defined as an accident in which a small break with equivalent diameter not larger than 5.0 cm occurs on the pipes of the reactor coolant system or on the upstream line of the second isolation valve connected to it. This accident lead to pressuriser level decrease and primary depressurization with a possible core heat-up due to lack of cooling. The transient thermal-hydraulic characteristics of the accident have been analysed in Sub-chapter 12.8.5.3.

In this section, the source term and dose calculation of SB-LOCA accident are analysed.

12.11.4.3.2 Main Safety Functions

In this section, the main safety functions for radiological release mitigation are claimed.

a) Containment Isolation

Containment isolation is triggered either by ‘Containment Pressure High 1’ signal or by ‘SI’ signal.

b) Isolation of the Regular Trains of Ventilation Systems

The containment isolation causes the isolation of following ventilation systems:

1) Low-capacity EBA [CSBVS] circuits of the containment;
2) Regular trains of EDE [AVS] of the annulus;
3) Regular trains of DWL [SBCAVS] of safeguard buildings;
4) DWK [FBVS] of fuel building.

c) Operation of the Safety Trains of Ventilation Systems

When the regular trains of ventilation systems are isolated, the safety trains are automatically put into operation:

1) One of the safety trains of EDE [AVS] is automatically put into operation, when the regular trains of EDE [AVS] are isolated;
2) One of the low-capacity DWK [FBVS] circuits is automatically put into operation for the ventilation of fuel building during the transient, when the DWK [FBVS] is isolated;
3) One of the safety trains of DWL [SBCAVS] is automatically put into operation, when the regular trains of DWL [SBCAVS] are isolated.

The design of the safety trains of EDE [AVS] and DWL [SBCAVS], and the low-capacity EBA [CSBVS] circuits has considered the single failure criteria. When one of the safety trains fails to start up, the backup train will be put into operation automatically.

12.11.4.3.3 Source Term

12.11.4.3.3.1 Radioactivity Released into the Environment

The analysis of LOCA source terms is based on the Appendix A of Reference [79], considering specific conditions and system designs.

a) Release of Radioactivity to Containment

In the blowdown phase, it is conservatively assumed that all of primary coolant is released to containment where airborne radionuclides are uniformly mixed with air inside containment.

The thermal-hydraulic analysis results of SB-LOCA show that the core always remains covered. So there is no fuel cladding failed during the accident.

b) Release of Radioactivity into Environment

The EBA [CSBVS] low-capacity circuit is operating at its maximum flowrate before the accident. All containment isolation valves of the low-capacity EBA [CSBVS] circuit are closed 20 s after the accident.

Before the accident, for the annulus, the normal-operational train of EDE [AVS] operates continuously at its maximum flowrate, for the peripheral building, the normal-operational train fuel building and safeguard building is in operation. During the accident, the EDE [AVS] switches automatically to the safety trains and also the safety train for peripheral buildings. The accident filters in the safety trains of annulus and peripheral buildings are taken into account after five minutes and after thirty minutes, respectively.

The other removal processes (such as deposition, sedimentation, wall condensation, etc.) are not taken into account. The impact of containment sprinkler system on containment depressurization and airborne radioactive material is not considered.

When the containment pressure has significantly decreased, the leak from inner containment to the containment annulus and peripheral buildings and that of from the containment annulus to the environment is gradually terminated. It is conservatively assumed that the leak from the containment and the ventilation of the containment annulus and peripheral buildings can last for 30 days after the accident.

12.11.4.3.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

During the accident, the radionuclides release into the annulus and surrounding buildings through containment leakage. The radionuclides may cause radiation

exposure to the workers working in the containment, annulus, surrounding buildings and near the steam pipelines.

Possible distributions of radionuclides inside the containment include:

a) Radionuclides suspended in the containment atmosphere;

b) Radionuclides deposited on the surfaces inside the containment;

c) Radionuclides in the IRWST Coolant.

Possible distributions of radionuclides inside the annulus and surrounding buildings include:

a) Radionuclides suspended in the building atmosphere;

b) Radionuclides deposited on the surfaces inside the buildings;

Main assumptions and parameters used in the source term calculation are presented in Reference[88]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.3.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 1.12E-01mSv, 1.62E-01mSv, and 5.93E-01mSv, respectively. The off-site doses are between the RPT-4 BSO and BSL for frequent faults (BSO: 0.01mSv, BSL: 1mSv).

The maximum dose to workers on-site is 1.48mSv. On-site doses to workers are between the RPT-4 BSO and BSL for frequent faults (BSO: 0.1mSv, BSL: 20mSv).

12.11.4.4 Rupture of a Line Carrying Primary Coolant Outside Containment

12.11.4.4.1 Description

Rupture of a line carrying primary coolant outside containment may result from the failure of:

a) The Chemical and Volume Control System (RCV [CVCS]), including the RCV [CVCS] connecting lines;

b) The Nuclear Sampling System (REN [NSS]).

Rupture of a line carrying primary coolant outside containment induces a loss of primary coolant, potential decrease in RCP [RCS] pressure (if the loss flowrate cannot be compensated by the RCV [CVCS]) and radioactive release to the environment. This accident may lead to a decrease in reactor coolant inventory and potential core overheating.

The rupture of a line carrying primary coolant outside containment is classified as an DBC-3 event, the thermal-hydraulic consequences are covered by the small break loss of coolant accident, which is presented in Sub-section 12.8.5.3. Following this accident, there is no fuel failure.

Considering the low temperature of the flow and restricted flowrate, a rupture in the RCV [CVCS] discharge line is not analysed. However, the postulated sample line break is analysed, assuming that the failure of the sample line occurs downstream of the containment penetration.

12.11.4.4.2 Main Safety Functions

In chapter 12.8.5.1, the main safety functions for reactor core protection of rupture of a line carrying primary coolant outside containment are described. In this section, the main safety functions for radiological release mitigation are claimed.

a) Isolation of break line

For pipe failure within RCV [CVCS] outside containment, the RCV [CVCS] letdown line is isolated when the ‘pressuriser level low 1’ and reactor trip signals occur.

For pipe failure within REN [NSS] outside containment, the REN [NSS] line is isolated by the operator when the ‘Activity High’ signal is detected by the plant radiation monitoring system.

12.11.4.4.3 Source Term

12.11.4.4.3.1 Radioactivity Released into the Environment

It is assumed that sampling is being performed before the accident during normal operation. The break is located just downstream of the containment penetration. An iodine spike occurs at the beginning of the accident, and a factor of 500 is considered

for the release rate from the fuel.

A constant leak flowrate is considered during the transient.

The noble gases contained in the break flow are assumed to be released into the auxiliary building and then to the environment.

The fraction of iodine and caesium available for release to the environment is assumed to be equal to the coolant flash fraction. The flash fraction is determined by assuming the discharge is a constant enthalpy process. Retention within the auxiliary building is not considered.

The line is isolated 60 min after the accident (30 min for signal actuation and 30 min for manual operator action).

12.11.4.4.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the RCV [CVCS] and REN [NSS] pipelines. When the accident occurs, the radionuclides released into the surrounding buildings may cause radiation exposure to the workers. Furthermore, the radioactivity concentrations in the RCV [CVCS] and REN [NSS] pipelines may cause a radiation on the workers near the pipelines.

Thus, the radioactivity distributions for radiation exposure to the workers on site to be evaluated are listed as below:

a) Radionuclides inside the surrounding buildings;

b) Radionuclides inside the RCV [CVCS] and REN [NSS] pipelines.

Main assumptions and parameters used in the source term calculation are presented in Reference [89]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.4.4 Dose Evaluation

The off-site effective doses of adult, child and infant 1.37E-01mSv, 2.95E-01mSv, and 1.27mSv, respectively. The off-site doses are between the RPT-4 BSO and BSL for DBC-3 infrequent faults (BSO: 0.01mSv, BSL: 10mSv).

The maximum dose to workers on-site is 3.50E+01mSv. On-site doses to workers are between the RPT-4 BSO and BSL for DBC-3 infrequent faults (BSO: 0.1mSv , BSL: 200mSv).

12.11.4.5 Volume Control Tank Break

12.11.4.5.1 Description

Volume control tank is located in the fuel building, downstream the RCV [CVCS] purification unit. Volume control tank break accident will result in leakage of the primary coolant in the fuel building.

If volume control tank fails structurally, the radionuclides in the volume control tank will be released into the fuel building. Moreover, until the operator isolates the RCV [CVCS] letdown line, a certain amount of liquids will also be released continuously. The radioactivity released includes:

a) Radioactivity from the gaseous phase of the tank;

b) Radioactivity from the liquid phase of the tank;

c) Radioactivity contained in liquids released from the letdown line before isolation.

12.11.4.5.2 Main Safety Functions

The main safety function for radiological release mitigation in this accident is the "isolation of RCV [CVCS] letdown line". The RCV [CVCS] letdown line is isolated when the 'pressuriser level low 1' and reactor trip signals occur.

12.11.4.5.3 Source Term

12.11.4.5.3.1 Radioactivity Released into the Environment

When the accident occurs, the radionuclides in the primary coolant are released into the fuel building through the break. The radionuclides in the building atmosphere are then released into the environment through leakage and ventilation.

12.11.4.5.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working in the fuel building. When the accident occurs, the radionuclides released into the fuel building may cause a radiation on these workers.

Possible distributions of radionuclides inside the fuel building include:

a) Radionuclides suspended in the building atmosphere;

b) Radionuclides deposited on the surfaces inside the buildings.

Main assumptions and parameters used in the source term calculation are presented in Reference [90]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.5.4 Dose Evaluation

The off-site effective dose of adult, child and infant are 1.67E-02mSv, 1.68E-02mSv,

and 4.93E-02mSv, respectively. The off-site doses are between the RPT-4 BSO and BSL for DBC-3 infrequent faults (BSO: 0.01mSv, BSL: 10mSv) and is close to BSO.

The maximum dose to workers on-site is 5.34mSv. On-site doses to workers are between the RPT-4 BSO and BSL for DBC-3 infrequent faults (BSO: 0.1mSv, BSL: 200mSv).

12.11.4.6 RCCA Ejection Accident

12.11.4.6.1 Description

The RCCA ejection accident is defined as the scenario where an RCCA is vertically ejected from the reactor core due to the mechanical failure of the RCCA drive mechanism housing at the top of the Reactor Pressure Vessel (RPV).

This accident leads to a rapid reactivity transient by inducing an uncontrolled positive reactivity to the core, followed by a nuclear power excursion and a power distribution disturbance. The accident may result in the failure of the fuels. The transient thermal-hydraulic characteristics of the accident have been analysed in Sub-chapter 12.9.4.1.

In this section, the source terms and radiological consequence of RCCA ejection accident are analysed.

12.11.4.6.2 Main Safety Functions

In Sub-chapter 12.9.4.1, the main safety functions for reactor core protection are described. In this section, the main safety functions for radiological release mitigation are claimed.

a) Containment Isolation

Containment isolation is triggered either by ‘Containment Pressure High 1’ signal or by ‘SI’ signal.

b) Isolation of the Regular Trains of Ventilation Systems

The containment isolation causes the isolation of following ventilation systems:

1) Low-capacity EBA [CSBVS] circuits of the containment;

2) Regular trains of EDE [AVS] of the annulus;

3) Regular trains of DWL [SBCAVS] of safeguard buildings;

4) DWK [FBVS] of fuel building.

c) Operation of the Safety Trains of Ventilation Systems

When the regular trains of ventilation systems are isolated, the safety trains are automatically put into operation:

1) One of the safety trains of EDE [AVS] is automatically put into operation, when the regular trains of EDE [AVS] are isolated;

2) One of the low-capacity EBA [CSBVS] circuits is automatically put into operation, when the DWK [FBVS] is isolated;

3) One of the safety trains of DWL [SBCAVS] is automatically put into

operation, when the regular trains of DWL [SBCAVS] are isolated.

The design of the safety trains of EDE [AVS] and DWL [SBCAVS], and the low-capacity EBA [CSBVS] circuits has considered the single failure criteria. When one of the safety trains fails to start up, the backup train will automatically put into operation.

12.11.4.6.3 Source Term

RCCA ejection accident may result in the failure of the fuels. The radionuclides in the defective fuels are released into the primary coolant. The potential radioactivity release paths to the environment include:

a) Containment Release Path;

b) Secondary Release Path.

Considering that radiological release may cause radiation exposure to the workers on the site, the potential radioactivity distributions during the transient are described.

The calculation of source terms in this section is based on the assumptions given by Appendix F in Reference [79].

12.11.4.6.3.1 Radioactivity Released into the Environment

When the accident occurs, with the assumed control rod ejection, radionuclides in the damaged fuel assemblies are released into the primary coolant, resulting in a rapid increase in primary coolant activity.

It is assumed that 10% of the fuel rod cladding is ruptured and 10% of fuel pellets within the damaged fuel rods melt.

There are 2 pathways for the release of radionuclides into the environment:

1) Release from Containment

An RCCA ejection accident may cause a break at the top of RPV, from which the radionuclide in primary coolant and damaged fuels may be released into containment atmosphere. The radionuclides from the inner containment leak to the annulus and peripheral buildings (radioactive materials may be released into environment from the inner containment through the ventilation before the isolation of the containment). The radionuclides in the annulus and peripheral buildings are released into the environment via ventilation system and filters.

The EBA [CSBVS] low-capacity circuit is operating at its maximum flowrate before the accident. All containment isolation valves of the low-capacity EBA [CSBVS] circuit are closed 20 s after the accident.

Before the accident, for the annulus, the normal-operational train of EDE [AVS] operates continuously at its maximum flowrate, for the peripheral building, the

normal-operational train fuel building and safeguard building is in operation. During the accident, the EDE [AVS] switches automatically to the safety trains and also the safety train for peripheral buildings. The accident filters in the safety trains of annulus and peripheral buildings are taken into account after five minutes and after thirty minutes, respectively.

The other removal processes (such as deposition, sedimentation, wall condensation, etc.) are not taken into account. The impact of containment sprinkler system on containment depressurization and airborne radioactive material is not considered.

When the containment pressure has significantly decreased, the leak from inner containment to the containment annulus and peripheral buildings and that of from the containment annulus to the environment is gradually terminated. It is conservatively assumed that the leak from the containment and the ventilation of the containment annulus and peripheral buildings can last for 30 days after the accident.

2) Release from Secondary Circuit

Before RHR is connected and operational, the residual heat of the reactor core is removed by the secondary circuit. Due to a potential leak from the SG heat transfer tube, the radioactivity of the secondary coolant gradually increases.

It is assumed that this accident occurs simultaneously with LOOP as well as failure of steam discharge condenser, so the residual heat of reactor core is removed by the secondary circuit through the VDA [ASDS]. Due to primary-to-secondary leakage, the radioactivity in secondary circuit increases and is released into the environment through the VDA [ASDS].

When calculating the secondary circuit release, the release to the containment is not considered. The fraction releases from the fuel gaps are given in Sub-chapter 12.11.2.2. It is assumed that all noble gases and 50% of iodines and alkali metals in the damaged fuel rods are available for release to the primary coolant. For iodine and alkali metals release through VDA [ASDS], it is determined by the steam flowrate through VDA [ASDS] and the associated carryover factors. The carryover factor of water in steam for iodine is assumed to be 1% and the entrainment factor of water in steam for cesium is assumed to be 0.25%.

12.11.4.6.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the airlock of the containment, in the fuel building or safeguard building, or near the main steam pipelines. When the accident occurs, the radionuclides released may cause radiation exposure to these workers. Thus, when evaluating the accident radiation exposure to the workers on the site, it is necessary to consider all potential radioactivity distributions during the accident.

When RCCA ejection accident occurs, the radioactivity distributions need to be

considered are listed as below:

1) Radionuclides inside the containment;

2) Radionuclides inside the annulus and surrounding buildings, including fuel building and safeguard buildings;

3) Radionuclides inside the steam pipelines.

Main assumptions and parameters used in the source term calculation are presented in Reference [91]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.6.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 2.27E+01mSv, 2.68E+01mSv, and 8.69E+01mSv, respectively. These off-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO:0.01mSv, BSL:100mSv).

The maximum dose to workers on-site is 3.35E+02mSv. On-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.7 Steam System Piping Large Break

12.11.4.7.1 Description

The steam system piping large break is defined as the large break of steam systems and its connecting lines. The steam system piping break induces an initial increase in the steam flow which then decreases during the accident as the steam pressure falls.

The transient thermal-hydraulic characteristics of the accident have been analysed in sub-chapter 12.9.1.1. The results show that the fuel cladding failure would not happen in the case of a main steam line break accident, the mass and energy release to the containment or environment can be limited.

In this section, the source term and radiological consequence of steam system piping large break are analysed.

12.11.4.7.2 Main Safety Functions

In chapter 12.9.1.1, the main safety functions for reactor core protection are described. There are no additional safety functions for radiological release mitigation claimed.

12.11.4.7.3 Source Terms

For this accident, the radioactivity release to the environment through the secondary system, which includes two parts, radioactivity released to the environment through steam piping break, and radioactivity released to the environment through VDA [ASDS]. Considering that radiological release may cause a radiation on the workers on the site, the potential radioactivity distributions during the transient are described.

The source term analysis method is based on Appendix C of Reference [79].

12.11.4.7.3.1 Radioactivity Released into the Environment

When an MSLB happens, all the water in the affected SG is released as steam into environment and the initial radioactive materials in the affected SG are released into environment. It is conservatively supposed that the initial water inventory of the affected steam generator is 100,000 kg which can bound all operation conditions.

Assuming the steam generator of the affected reactor coolant loop is free from heat removal, the RIS [SIS]/RHR connection is finished after 8 hours of the accident. Assuming conservatively that the core decay heat, primary/secondary circuit sensible heat, metal storage heat, and heat produced by pumps within the eight hours after the accident are all carried out by two unaffected SG. Due to the primary-to-secondary leakage, the radioactivity of the secondary side increases and radioactive material is released into the environment through the VDA [ASDS].

It is assumed that a power transient takes place before the piping break and the primary coolant activity increases to the transient value.

The VDA [ASDS] will continue releasing steam to remove heat until the primary circuit reaches the condition that is suitable for RHR connection. About 824,000kg of steam is released to the environment through other unaffected two steam generators in this period.

12.11.4.7.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the airlock of the containment, in the fuel building or safeguard building, or near the main steam pipelines. When the accident occurs, the radionuclides released may cause radiation exposure to these workers. Thus, when evaluating the accident radiation on the workers on the site, it is necessary to consider all potential radioactivity distributions during the accident.

Radiation exposure to the workers can be caused by radioactivity release following piping break and by radioactivity in the steam pipelines considering that the steam system piping break may occur in the containment or the safeguard building. For a piping break occurs in the containment, the radioactivity can transfer from containment leakage to the annulus and surrounding buildings, which includes the fuel building and safeguard building.

Thus, the radioactivity distributions which need to be considered are summarised as below:

a) Radioactivity Distributions following Piping Break inside the Containment

- Radionuclides inside the containment;
- Radionuclides inside the annulus and surrounding buildings;

b) Radioactivity Distributions following Piping Break inside the Safeguard Building

c) Radioactivity in the Steam Pipelines

Main assumptions and parameters used in the source term calculation are presented in Reference [92]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.7.4 Dose evaluation

The off-site effective doses of adult, child and infant are 8.28E-02mSv, 1.19E-01mSv, and 4.36E-01mSv, respectively. These off-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.01mSv, BSL: 100mSv).

The maximum dose to workers on-site is 1.28E+01mSv. On-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.8 Large Break Loss of Coolant Accident (LB-LOCA) (up to Double-ended Guillotine Rupture)

12.11.4.8.1 Description

Large Break Loss of Coolant Accident (LB-LOCA) (up to Double-ended Guillotine Rupture) is defined as an accident in which a large break (equivalent diameter over 27.5 cm, up to double-ended) occurs on the pipes of the Reactor Coolant System (RCP [RCS]) or on the lines connecting RCP [RCS] and the second isolation valve.

A LB-LOCA induces a rapid loss of primary coolant. It results in an abrupt decrease of RCP [RCS] pressure and Pressuriser level with a significant core heat-up due to limited heat removal capacity under accident condition. The accident may result in fuel damage. The transient thermal-hydraulic characteristics of the accident have been analysed in reference [93].

In this section, the source term and radiological consequence of LB-LOCA accident are analysed.

12.11.4.8.2 Main Safety Functions

The main safety functions for radiological release mitigation are claimed as follows,

a) Containment isolation

Containment isolation is triggered either by ‘Containment Pressure High 1’ signal or by ‘SI’ signal.

b) Isolation of the regular trains of ventilation systems

The containment isolation causes the isolation of following ventilation systems:

1) Low-capacity EBA [CSBVS] circuits of the containment;
2) Regular trains of EDE [AVS] of the annulus;
3) Regular trains of DWL [SBCAVS] of safeguard buildings;
4) DWK [FBVS] of fuel building.

c) Operation of the safety trains of ventilation systems

When the regular trains of ventilation systems are isolated, the safety trains are automatically put into operation:

1) One of the safety trains of EDE [AVS] is automatically put into operation, when the regular trains of EDE [AVS] are isolated;
2) One of the low-capacity EBA [CSBVS] circuits is automatically put into operation for the ventilation of fuel building during the transient, when the DWK [FBVS] is isolated;

3) One of the safety trains of DWL [SBCAVS] is automatically put into operation, when the regular trains of DWL [SBCAVS] are isolated.

The design of the safety trains of EDE [AVS] and DWL [SBCAVS], and the low-capacity EBA [CSBVS] circuits has considered the single failure criteria. When one of the safety trains fails to start up, the backup train will be put into operation automatically.

12.11.4.8.3 Source Term

12.11.4.8.3.1 Radioactivity Released into the Environment

The analysis of LOCA source terms is based on the Appendix A of Reference [79], considering specific conditions and system designs.

a) Release of Radioactivity to Containment

In the blowdown phase, it is conservatively assumed that all of primary coolant is released to containment where airborne radionuclides are uniformly mixed with air inside containment.

The cladding damage stage begins 30s after the accident. It is assumed that radionuclides in the fuel gaps are released to containment immediately and uniformly mixed with atmosphere. The fractions of core fission products released into containment are given in Sub-chapter 12.11.2.

b) Release of Radioactivity into Environment

The EBA [CSBVS] low-capacity circuit is operating at its maximum flowrate before the accident. All containment isolation valves of the low-capacity EBA [CSBVS] circuit are closed 20 s after the accident.

Before the accident, for the annulus, the normal-operational train of EDE [AVS] operates continuously at its maximum flowrate, for the peripheral building, the normal-operational train fuel building and safeguard building is in operation. During the accident, the EDE [AVS] switches automatically to the safety trains and also the safety train for peripheral buildings. The accident filters in the safety trains of annulus and peripheral buildings are taken into account after five minutes and after thirty minutes, respectively.

The other removal processes (such as deposition, sedimentation, wall condensation, etc.) are not taken into account. The impact of containment sprinkler system on containment depressurization and airborne radioactive material is not considered.

When the containment pressure has significantly decreased, the leak from inner containment to the containment annulus and peripheral buildings and that of from the containment annulus to the environment is gradually terminated. It is conservatively assumed that the leak from the containment and the ventilation of the containment

annulus and peripheral buildings can last for 30 days after the accident.

12.11.4.8.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the airlock of the containment, in the fuel building or safeguard building. When the accident occurs, the radionuclides released may cause radiation exposure to these workers. Thus, when evaluating the accident radiation on the workers on the site, it is necessary to consider all potential radioactivity distributions during the accident.

When LB-LOCA occurs, the radioactivity distributions need to be considered are listed as below:

a) Radionuclides inside the containment;

The possible distributions of radionuclides inside the containment are:

1) Radionuclides suspended in the containment atmosphere;
2) Radionuclides deposited on the surfaces inside the containment;
3) Radionuclides resolved in the In-containment Refuelling Water Storage Tank (IRWST) coolant.

b) Radionuclides inside the annulus and surrounding buildings, including fuel building and safeguard buildings.

Possible distributions of radionuclides inside the annulus and surrounding buildings include:

1) Radionuclides suspended in the building atmosphere;
2) Radionuclides deposited on the surfaces inside the buildings.

Main assumptions and parameters used in the source term calculation are presented in Reference [93]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.8.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 1.13E+01mSv, 9.66mSv, and 2.26E+01mSv, respectively. These off-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.01mSv, BSL: 100mSv).

The maximum dose to workers on-site is 1.13E+02mSv. On-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.9 SG Tube Rupture (Two Tubes in One SG)

In SG Tube Rupture (Two Tubes in One SG), guillotine break occurs on 2 tubes inside an SG, which is a DBC-4 accident. Radioactive nuclides in primary circuit are released to the secondary circuit and then to the environment. The methodology and assumptions are exactly the same as those used for an SGTR. The source term calculation is presented in Reference [94]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

The off-site effective doses of adult, child and infant are 4.70E-02mSv, 9.19E-02mSv, and 3.80E-01mSv, respectively. These off-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.01mSv, BSL: 100mSv).

The maximum dose to workers on-site is 6.04E-01mSv. On-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.10 Residual Heat Removal System Break Outside Containment

12.11.4.10.1 Description

An RHR system piping break outside containment is defined as an accident in which an isolatable break with an equivalent diameter smaller than or equal to DN250 (with a nominal diameter of 250 mm) on one Safety Injection System (RIS [SIS]) line outside containment under RHR mode, induces loss of coolant inventory and Reactor Coolant System (RCP [RCS]) pressure decrease, thereby leading to a possible core heat-up. The transient thermal-hydraulic characteristics of the accident have been analysed in sub-chapter 12.9.5.5.

In this section, the source term and dose calculation of RHR system piping break outside containment accident are analysed.

12.11.4.10.2 Main Safety Functions

The RIS [SIS] lines are automatically isolated to limit the coolant leak into the safeguard building by the "safeguard building sump level high 1" signal or "safeguard building pressure rise high 1" signal.

12.11.4.10.3 Source Term

12.11.4.10.3.1 Radioactivity Released to the Environment

The analysis of RHR system piping break outside containment accident source terms is based on the Appendix A of Reference [79], considering specific conditions and system designs.

Before the accident occurs, Safeguard Building Controlled Area Ventilation System (DWL [SBCAVS]) is operating. When the RHR break occurs, the radionuclides in the primary coolant are released into the safeguard building through the break. And then the radionuclides in the safeguard building atmosphere will be released into the environment through the DWL [SBCAVS] after filtration, which may cause a radiation on people off site.

12.11.4.10.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

During the accident, the radionuclides release into the safeguard buildings through the break. The radionuclides may cause radiation exposure to the workers in the safeguard buildings and near the RIS [RHR] Pipelines.

Possible distributions of radionuclides inside the safeguard buildings include:

a) Radionuclides suspended in the safeguard buildings atmosphere;

b) Radionuclides deposited on the surfaces inside the safeguard buildings.

Main assumptions and parameters used in the source term calculation and source term results are presented in Reference [95]. The results are used as input data for the

evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.10.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 3.51E-01mSv, 4.90E-01mSv, and 1.76mSv, respectively. These off-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO:0.01mSv, BSL:100mSv).

The maximum dose to workers on-site is 1.04E+02mSv. On-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.11 Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break

12.11.4.11.1 Description

Reactor coolant pump seizure (locked rotor) or reactor coolant pump shaft break is defined as a seizure or a shaft break of the rotor for the reactor coolant pump under normal operation. A seized rotor or shaft break is due to mechanical failure. The result of a reactor coolant pump shaft break is bounded by a locked rotor, as the coolant flow reduction rate is lower for the former. Therefore, only the locked rotor is considered.

During the transient, the core flow reduction causes a rapid increase in reactor coolant temperature. This increase may result in fuel rods experiencing DNB, and subsequent fuel damage. The transient thermal-hydraulic characteristics of the accident have been analysed in Sub-chapter 12.9.3.1.

In this section, the source term and radiological consequence of a locked rotor accident are analysed.

12.11.4.11.2 Main Safety Functions

In Sub-chapter 12.9.3.1, the main safety functions for reactor core protection are described. There are no additional safety functions for radiological release mitigation claimed.

12.11.4.11.3 Source Term

A locked rotor accident may result in the failure of the fuel rods. The radionuclides in the defective fuel rods are released into the primary coolant. The potential radioactivity release path to the environment only includes secondary release path.

Considering that radiological release may cause radiation exposure to the workers on the site, the potential radioactivity distributions during the transient are described.

The source term analysis method is mainly based on Reference [79] which supports the development of the assumptions for evaluating the radiological consequences of a PWR locked rotor accident.

12.11.4.11.3.1 Radioactivity Released into the Environment

In the analysis, 10% of fuel cladding is assumed to be ruptured. As a non-LOCA event, the fraction of the fission product inventories in the fuel gaps are described in Sub-chapter 12.11.2.2. The radioactivity will be released into the reactor coolant. This is assumed to occur instantaneously and homogeneously throughout the primary coolant and dramatically increases the activity of the primary circuit.

Assuming that the steam dump condenser fails, residual heat is removed by the ASG [EFWS] and VDA [ASDS]. Considering the primary-to-secondary leakage,

radioactivity in the secondary side will increase and the radiological material will be released to the environment through VDA [ASDS]. It is assumed that noble gases released from the primary system are released into the environment without mitigation. Iodine and alkali metals released from the primary system are mixed homogeneously in the water of SGs. The releases into the environment of iodine and alkali metals are determined by steam flow rate and partition factors. The partition factors of iodine and alkali metals are 0.01 and 0.0025, respectively.

Steam from the secondary side will continue to be discharged until the RCP [RCS] reaches the temperature and pressure value for connection of the RIS [SIS] in RHR mode. Assuming the steam generator of the affected reactor coolant loop is free from heat removal, the RIS/RHR connection is finished after 8 hours of the accident.

12.11.4.11.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Before the accident occurs, workers may be working near the main steam pipelines. When the accident occurs, the radionuclides released may cause radiation exposure to these workers. When a locked rotor accident occurs, the radionuclides inside the steam pipelines need to be considered.

It is assumed that 10% of the fuel claddings are ruptured at the beginning of the accident and released to the primary coolant. The radionuclides in the primary coolant are then released into the secondary coolant through the possible primary-to-secondary leakage in the Steam Generators (SGs) which will lead the radioactivity concentrations in the steam pipelines increasing to a relatively high level. It is considered that the noble gases released from the primary system are homogeneously distributed in the steam pipelines. The iodine and alkali metals are mixed homogeneously with the secondary water. The concentration of iodine and alkali metals in the vapour are determined by the partition factors. The partition factors of iodine and alkali metals are 0.01 and 0.0025, respectively.

Main assumptions and parameters used in the source term calculation are presented in Reference [96]. The results are used as input data for the evaluation of radiological consequences of any person off the site and any worker on the site.

12.11.4.11.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 2.46mSv, 3.78mSv, and 1.43E+01mSv, respectively. These off-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.01mSv, BSL: 100mSv).

The maximum dose to workers on-site is 8.34E-01mSv. On-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.12 Dropping of fuel assembly

12.11.4.12.1 Description

The accident of dropping of fuel assembly (FA) may occur during fuel handling operations, which include the following operations:

a) Receipt, inspection and storage of new fuel assemblies in fuel building;

b) Fuel loading and unloading;

c) Spent fuel delivery in fuel building.

When the accident occurs, the cladding of the dropped FA may fails, which will cause the radioactivity in the fuel cladding gap to be released to the fuel pool. Noble gases and volatile iodine will escape from the fuel dropped pool to the atmosphere of fuel operating room. The escaped iodine and noble gases will be released to the environment through the building ventilation system.

In this section, the source terms of dropping of FA accident are analysed. For off-site source term evaluation, dropping of FA in the fuel building is considered. If a FA drops in the fuel pool in the containment, because of the large free volume of the containment, the containment accidental ventilation rate is lower than that of the fuel building. The radioactivity released to the environment from the containment can be bounded by that of the fuel building accident. For on-site source term evaluation, FA drop in the fuel pool of the containment and of the fuel building are all considered.

12.11.4.12.2 Main Safety Functions

The main safety functions for radiological release mitigation for dropping of FA in the containment and in the fuel building are claimed as follows,

a) Dropping of FA in the Containment

1) Isolation of the high-capacity EBA[CSBVS] circuit

The high-capacity EBA [CSBVS] circuit is isolated by “Radioactivity high level” in the containment.

2) Operation of the low-capacity EBA[CSBVS] circuit

The low-capacity circuit exhaust ventilation system maintains the reactor building negative pressure to limit the release of radioactivity to the environment.

b) Dropping of FA in the Fuel Building

1) Isolation of the regular trains of fuel handling hall ventilation systems.

Regular trains of DWK [FBVS] of fuel handling hall are isolated by “Radioactivity high level” in the fuel handling hall.

2) Operation of the safety trains of fuel handling hall ventilation systems.

When the regular trains of fuel handling hall ventilation systems are isolated, the safety trains are automatically put into operation: One of the safety trains of DWL [SBCAVS] is automatically put into operation, when the regular trains of DWK [FBVS] are isolated.

The design of the safety trains of DWL [SBCAVS] has considered the single failure criteria. When one of the safety trains fails to start up, the backup train will automatically put into operation.

12.11.4.12.3 Source Term

12.11.4.12.3.1 Radioactivity Released to the Environment

It is assumed that the accident occurs 100 hours after reactor shutdown, which is the shortest time for spent fuel being transported to the fuel storage area. When the accident occurs, dropping of the FA in the fuel building is considered. Cladding of fuel rods may be breached. It is conservatively assumed that all of the fuel rods within one fuel assembly during handling are breached.

The fission products inventory in the breached fuel cladding gap is totally released immediately. The noble gases released will escape from the pool to the fuel handling hall. Because of the water solubility and decomposition, the large proportion of iodine will be trapped in the water. All the Alkalis are also assumed to be trapped in water. The escaped iodine and noble gases will be released to the environment through the fuel building ventilation system.

During normal operation, the regular trains of Fuel Building Ventilation System (DWK [FBVS]) are operating continuously. The radionuclides in the fuel building are released into the atmosphere via the DWK [FBVS] ventilation systems through the stack.

When the ‘radioactivity high level in the fuel handling hall’ signal is triggered, DWK [FBVS] is automatically isolated. The safety train of DWL [SBCAVS] is put into operation automatically after the isolation of the regular trains of DWK [FBVS]. When the safety trains of DWL [SBCAVS] circuit is operating, the radionuclides in the fuel building is filtered before venting into the atmosphere.

12.11.4.12.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Considering that radiological release may cause radiation exposure to the workers on the site, in this chapter, the potential radioactivity distributions during the transient are described.

Before the accident occurs, workers may be working in the containment or in the fuel building. When the accident occurs, the radionuclides released may cause radiation exposure to these workers on site. Thus, when evaluating the accident radiation

exposure to the workers on the site, it is necessary to consider all potential radioactivity distributions during the accident.

a) Radioactivity distributions in the containment

When dropping of FA occurs in the reactor building, the radioactivity distributions needed to be considered are listed as below:

1) Radionuclides inside the containment;

2) Radionuclides resolved in the fuel dropped pool.

FA may drop in the reactor cavity pool, the core internal pool or the reactor building transfer pit during loading and unloading operation. So for dropping of fuel assembly under these three cases, the following distributions of radionuclides are considered:

- Radionuclides resolved in the reactor cavity pool;
- Radionuclides resolved in the core internal pool;
- Radionuclides resolved in the reactor building transfer pit.

b) Radioactivity distributions in the fuel building

When dropping of FA occurs in the fuel building, the radioactivity distributions needed to be considered are listed as below:

1) Radionuclides inside the fuel handling hall;

2) Radionuclides resolved in the fuel dropped pool.

FA may drop in the fuel building transfer pit, SFP during loading and unloading operations. So for dropping of assembly under these two cases, the following distributions of radionuclides are considered:

- Radionuclides resolved in the fuel building transfer pit;
- Radionuclides resolved in the SFP.

Main assumptions and parameters used in the source term calculation are presented in Reference [97]. The results are used as input data for dose evaluation of any person off the site and any worker on the site.

12.11.4.12.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 1.01mSv, 2.23mSv, and 9.62mSv, respectively. These off-site doses are all between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.01mSv, BSL: 100mSv).

The maximum dose to workers on-site is 3.15E+02mSv. On-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.11.4.13 Dropping of Spent Fuel Cask

12.11.4.13.1 Description

Dropping of spent fuel cask could occur during SFIS operations within or outside the fuel building. If the accident happened during transportation outside the fuel building, the cask will only be slightly above the ground and the drop height will not exceed the drop withstand capability of the cask. So it will not damage the integrity of the cask. Only accidents which happens inside the fuel building is considered.

There are 3 following spent fuel cask delivery processes inside the fuel building,

a) Lifting of the spent fuel cask from the loading pit to the cask stand;

b) Lifting of the spent fuel cask from cask stand onto the transit platform;

c) Lifting of the spent fuel cask from the transit platform onto the transport vehicle.

Impact limiters are placed on the lifting route of spent fuel cask, including loading pit, cask stand, transit platform and hoisting pit. For delivery process b) and c), the fuel cask is fully sealed. The impact limiters on the surface of cask stand, underneath the transit platform and hoisting pit are able to reduce the impact on the spent fuel transfer cask to the allowable limit. The cask integrity can be assured.

For the delivery process a), the cask is not fully sealed. The canister inner cover is placed on the canister in the spent fuel cask before the lifting. This inner cover is about 3-5 tons and is located inside the spent fuel transfer cask (the edge of transfer cask is higher than the upper surface of inner cover). During normal operation, the inner cover is very unlikely to slip from the spent fuel transfer cask. However, a very extreme condition is taken into account conservatively that the spent fuel cask drops into the loading pit from the maximum height during the transfer a), the fuel claddings of all fuel assemblies stored in the cask are considered to be damaged, and the cask inner cover is removed for dropping. Under this extreme condition, the radiological consequences to persons on-site and off-site are evaluated.

12.11.4.13.2 Main Safety Functions

The main safety functions for radiological release mitigation for dropping of spent fuel cask are claimed as follows,

a) Isolation of the regular trains of Fuel Building Ventilation Systems (DWK [FBVS])

Regular trains of DWK [FBVS] of fuel handling hall are isolated by “Radioactivity high level” in the fuel handling hall.

b) Operation of the safety trains of fuel building ventilation systems.

When the regular trains of fuel building ventilation systems are isolated, the safety

trains are automatically put into operation: One of the safety trains of Safeguard Building Controlled Area Ventilation System (DWL [SBCAVS]) is automatically put into operation, when the regular trains of DWK [FBVS] are isolated.

The design of the safety trains of DWL [SBCAVS] has considered the single failure criterion. When one of the safety trains fails to start up, the backup train will automatically put into operation.

12.11.4.13.3 Source Term

12.11.4.13.3.1 Radioactivity Released to the Environment

When the accident occurs, the cladding of fuel rods may be breached. The fission products inventory in the breached fuel cladding gap is totally released immediately. The noble gases released will escape from the pool to the fuel handling hall. Because of the loading pit water solubility and decomposition, the large proportion of iodine will be trapped in the water. All the alkali metals are also assumed to be trapped in the loading pit water. The escaped iodine and noble gases are considered to be released to the environment directly.

12.11.4.13.3.2 Radioactivity Distributions for Radiation Evaluation of Workers

Considering that radiological release may cause radiation exposure to the workers on the site, in this chapter, the potential radioactivity distributions during the transient are described.

Before the accident occurs, workers may be working in the fuel building. When the accident occurs, the radionuclides released may cause radiation exposure to these workers on site. The radioactivity distributions needed to be considered are listed as below:

a) Radionuclides inside the fuel handling hall;

b) Radionuclides resolved in the loading pit.

Main assumptions and parameters used in the source term calculation are presented in Reference [98]. The results are used as input data for dose evaluation of any person off the site and any worker on the site.

12.11.4.13.4 Dose Evaluation

The off-site effective doses of adult, child and infant are 1.89E-02mSv, 2.81E-02mSv, and 3.40E-02mSv, respectively. These off-site doses far below RPT-4 BSL and is near BSO (BSO: 0.01mSv, BSL: 100mSv).

The maximum dose to workers on-site is 2.15E+02mSv. On-site doses are between the RPT-4 BSO and BSL for DBC-4 faults (BSO: 0.1mSv, BSL: 500mSv).

12.12 Specific Studies

For specific studies, the safety analysis rules are the same with DEC-A which is described in Reference [4], Section 7.2.3.

Analyses for specific studies from spurious I&C actuation are presented in *Analysis for Spurious I&C Actuation Events*, Reference [99]. Analyses for specific studies from loss of support system are presented in *Analysis for Loss of Support System Events*, Reference [100]. Analysis for *Double-ended Guillotine Failure of Largest RCS Pipe* is presented in *Large Break - Loss of Coolant Accident (up to double-ended break)*, Reference [101]. For *Main Steam Line Large Break (Pipe with HIC classification)*, the transient analysis is bounded by that of DBC-4 event: *Steam System Piping Large Break*.

12.12.1 Spurious I&C Actuation

12.12.1.1 Spurious Actuation of One or More ASG [EFWS] Trains (State A\B)

12.12.1.1.1 Description

This event leads to the increase in SG feedwater flowrate and thus the increase in heat removal by the secondary system. During power operation, the increase in heat removal causes core power increase due to the moderator temperature feedback or by the RCP [RCS] average coolant temperature control. In the zero power state, the increase in heat removal causes a return to power due to the moderator temperature feedback. Therefore, this event may lead to the risk of DNB (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC event causing similar initiating event and transient evolution is “Increase in Feedwater Flow due to Feedwater System Malfunctions” (Sub-chapter 12.7.1.1), which includes the case of spurious actuation of 1 or 3 ASG [EFWS] trains.

Similar to Sub-chapter 12.7.1.1, the coolant temperature and core power at full power level are higher than those conditions at other power levels in state A. Therefore, full power case can cover any cases of other power levels. The coolant temperature in hot shutdown state is higher than other shutdown states in state A and state B, so the core is more easily to return criticality and the DNB risk is more onerous. Thus the bounding case is spurious actuation of 1 or 3 of ASG [EFWS] trains at full power operation or hot shutdown state.

12.12.1.1.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.1.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Event occurred at full power operation

1) Reactor trip is actuated by the “SG level (narrow range) high 1” signal;

2) Turbine trip is actuated by reactor trip signal;

3) The ARE [MFFCS] full load isolation is actuated by “SG level (narrow range) high 1” or reactor trip signal;

4) The ARE [MFFCS] low load isolation is actuated by “SG level (wide range) high 0” and reactor trip signal;

5) The MSSVs open automatically when SG pressure reaches the setpoint.

b) Event occurred at hot shutdown state

1) The ARE [MFFCS] full load isolation is actuated by “SG level (narrow range) high 1” or reactor trip signal;

2) The ARE [MFFCS] low load isolation is actuated by “SG level (wide range) high 0” and reactor trip signal;

3) The main steam isolation valves are closed by “SG pressure low 1” signal;

4) The Safety Injection System (RIS [SIS]) is actuated by “Hot leg pressure low 3” signal.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSV can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The affected ASG [EFWS] can be isolated by the operator via local manual actions.

12.12.1.1.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

During power operation, the increase in feedwater flowrate leads to decrease of primary coolant temperature and increase of reactor power. Reactor trip is automatically triggered by “SG level (narrow range) high 1” signal of KDS [DAS], which subsequently actuates the turbine trip. The isolation of the full load lines of ARE [MFFCS] is actuated by “SG level (narrow range) high 1” signal or reactor trip signal. If the SG level reaches the setpoint of “SG level (wide range) high 0”, the low load lines of ARE [MFFCS] are isolated.

In hot shutdown state, the increase in feedwater flowrate leads to decrease of primary coolant temperature and the core shutdown margin, and then the core may return to criticality. The isolation of the full load lines of ARE [MFFCS] is actuated by “SG level (narrow range) high 1” signal or reactor trip signal. If the SG level reaches the setpoint of “SG level (wide range) high 0” after reactor trip, the low load lines of ARE [MFFCS] are isolated. The Main Steam Isolation Valves (MSIVs) can be closed by KDS [DAS] to isolate the main steam lines if the setpoint of “SG pressure low 1” is reached.

The affected ASG [EFWS] can be isolated by the operator via local manual actions. Later on, the controlled state is reached. Under this state, the residual heat is removed by MSSVs. And the feedwater is supplied by the ASG [EFWS].

b) From the Controlled State to the Safe State

The safe state is defined as a state where at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. To reach the safe state, operators perform primary cooldown and depressurisation according to specific rules:

1) Reactor coolant boration is performed via the chemical and volume control system RCV [CVCS], or via the RBS [EBS] if the RCV [CVCS] is unavailable;

2) Reactor coolant cooldown via the secondary circuit uses the ASG [EFWS] and VDA [ASDS] by means of reducing the VDA [ASDS] opening pressure setpoint. The cooldown rate depends on the number of available RBS [EBS] train. ASG [EFWS] tank capacity is designed to ensure that the RIS [SIS] can be connected in RHR mode before the ASG [EFWS] tank inventory is exhausted;

3) Reactor coolant depressurisation is performed by the normal or auxiliary pressuriser spray, and the PSVs can be used when the pressuriser sprays are unavailable.

12.12.1.1.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to that of the DBC event analysed in Sub-chapter 12.7.1.1. Compared with the DBC event, automatic reactor trip signal of this event may be a little later because the increase of feedwater flowrate assumed in the DBC event is larger. Considering the safety margin shown in Sub-chapter 12.7.1.1, it is justified that the DNBR limit will not be exceeded and the fuel melt temperature limit is not challenged for this event.

12.12.1.2 Spurious Actuation of One or More ASP [SPHRS] Trains (State A\B\C\D\E\F)

12.12.1.2.1 Description

This event leads to a minor increase in steam flowrate which causes a power mismatch between reactor power and steam flow demand. The overcooling of primary side caused by the excessive increase in secondary steam flow leads to a core power increase, by the moderator reactivity feedback, or by the RCP [RCS] core average temperature control. Thus this event may lead to the risk of DNB (Reference [99]).

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC event causing similar initiating event and transient evolution is “Excessive Increase in Secondary Steam Flow” (Sub-chapter 12.7.1.2), which includes the case of spurious actuation of ASP [SPHRS].

Similar to Sub-chapter 12.7.1.2, the bounding case is spurious actuation of 3 ASP [SPHRS] rains at power operation.

12.12.1.2.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.2.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on “High neutron flux (power range, low setpoint & high setpoint)” signal;

b) Turbine trip is actuated by reactor trip signal;

c) ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) The MSSVs open automatically when SG pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSV can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The ASP [SPHRS] can be isolated by the operator via local manual actions.

12.12.1.2.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

The reactor power increases to automatically trigger reactor trip by “High neutron flux (power range, low setpoint & high setpoint)” signal from KDS [DAS] or stabilise at a higher power level without triggering RT.

If reactor trip is not triggered, the operator can identify the alarm of high core power and perform appropriate measures to isolate ASP [SPHRS] via local manual actions.

If reactor trip is triggered, turbine trip and isolation of the ARE [MFFCS] full load lines are actuated. The plant stabilises in the hot shutdown state.

b) From the Controlled State to the Safe State

The ASP [SPHRS] can be isolated by the operator via local manual actions. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.2.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to that of the DBC event analysed in Sub-chapter 12.7.1.2. Compared with the DBC event, automatic reactor trip signal of this event is a little later because the increase of steam flowrate assumed in the DBC event is larger. Considering the safety margin shown in Sub-chapter 12.7.1.2, it is justified that the DNBR limit will not be exceeded and the fuel melt temperature limit is not challenged for this event.

12.12.1.3 Spurious Actuation of the GCT [TBS] MCD Function and RIS [SIS] Injection Function with Large Miniflow Line Closed (State A\B)

12.12.1.3.1 Description

In state A, the RCP [RCS] pressure is higher than the MHSI injection header, so there is no injection of MHSI flow into RCP [RCS] actually.

In state B, the RCP [RCS] pressure may be higher or lower than the MHSI injection header. When the RCP [RCS] pressure is lower than the MHSI injection header, this event leads to injection of MHSI flow into RCP [RCS].

The main consequence is actuation of GCT MCD that leads to an increase in steam flowrate and thus over-coolingfor the primary system which is similar to the event in Sub-chapter 12.12.1.2 (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC events causing over-cooling consequence are “Excessive Increase in Secondary Steam Flow” (Sub-chapter 12.7.1.2) and/or “Steam System Piping Large Break” (Sub-chapter 12.9.1.1).

Similar to Sub-chapter 12.7.1.2 and 12.9.1.1 the bounding case is spurious actuation of GCT [TBS] MCD function and RIS [SIS] injection function at power operation or zero power.

12.12.1.3.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.3.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS

[DAS] are required:

a) Reactor trip is actuated on “High neutron flux (power range, low setpoint & high setpoint)” or “SG level (narrow range) low 1” or “pressuriser pressure low 2” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS].

12.12.1.3.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

1) Power operation

The GCT [TBS] MCD by PSAS is terminated when the secondary system pressure reaches the setpoint (6.0 MPa). The primary side temperature and pressure decreases while the reactor power increases until reactor trip is automatically triggered by “High neutron flux (power range, low setpoint & high setpoint)” or “SG level (narrow range) low 1” or “pressuriser pressure low 2” signal from KDS [DAS].

After reactor trip, the automatic protection actions are actuated to mitigate the event and the reactor can reach the controlled state.

The primary system pressure may not fall below the MHSI injection header so there is no injection of MHSI flow into RCP [RCS]. If the primary system pressure falls below the MHSI injection header, the injection of MHSI flow can maintain the primary system at the MHSI injection pressure. The secondary system pressure is stable at the end of MCD.

2) Hot shutdown state

It is anticipated that there is no risk of DNB because the cooldown by the GCT [TBS] MCD is terminated when the secondary system pressure reaches 6.0 MPa and the Doppler Effect can limit the power excursion. The controlled state can be reached.

b) From the Controlled State to the Safe State

The GCT [TBS] can be isolated by the operator via local manual actions. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.3.5 Analysis Result

The transient evolution and main safety functions of this event are similar to those of the DBC events in Sub-chapter 12.7.1.2 and 12.9.1.1. The discharge size of GCT [TBS] valves is within the range of break size in Sub-chapter 12.9.1.1. Considering the safety margin shown in Sub-chapter 12.7.1.2 and 12.9.1.1, it is justified that the DNBR limit will not be exceeded and the fuel melt temperature limit is not challenged for this event.

12.12.1.4 Spurious Opening of One or More VDA [ASDS] Trains (State A\B\C\D\E\F)

12.12.1.4.1 Description

This event leads to an increase in steam flowrate and thus over-cooling for the primary system which is similar to Sub-chapter 12.12.1.2 (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC event causing similar initiating event and transient evolution is “Steam System Piping Large Break” (Sub-chapter 12.9.1.1).

Similar to Sub-chapter 12.9.1.1, the bounding case is spurious opening of one or more VDA [ASDS] trains at full power or zero power.

12.12.1.4.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.4.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on “High neutron flux (power range, low setpoint & high setpoint)” or “pressuriser pressure low 2” or “SG pressure low 1” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ARE [MFFCS] low load isolation is actuated by “SG pressure low 2” signal;

e) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

f) The MSSVs open automatically when SG pressure reaches the setpoint.

g) The RIS [SIS] is actuated by the “Hot leg pressure low 3” signal.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The affected VDA [ASDS] can be isolated by the operator via local manual actions.

12.12.1.4.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

1) Event occurred at power operation

Initially, this event leads to decrease of secondary system pressure and increase of core power due to the negative moderator temperature coefficient. reactor trip might be automatically triggered by “High neutron flux (power range, low setpoint & high setpoint)” or “pressuriser pressure low 2” or “SG pressure low 1” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS]. If the setpoint of “SG pressure low 1” is reached, the isolation of all main steam lines is automatically actuated by KDS [DAS]. Furthermore, if the setpoint of “SG pressure low 2” is reached, the isolation of the low load line of ARE [MFFCS] is actuated by KDS [DAS].

The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory. The MSSV of the unaffected SG will open automatically if the secondary pressure

exceeds its setpoint. Thereafter, the controlled state is reached.

If the discharge size is not large enough, reactor trip might not be triggered, and the core power will remain at a higher level matching the secondary side. The operator can identify the alarm of high core power and perform appropriate actions to bring the reactor to the controlled state.

2) Event occurred at zero power state

Initially, this event leads to decrease of secondary system pressure. reactor trip might be automatically triggered by “pressuriser pressure low 2” or “SG pressure low 1” signal of KDS [DAS]. If the setpoint of “SG pressure low 1” is reached, the isolation of all main steam lines is automatically actuated by KDS [DAS]. After that, only the affected SG continues to depressurize. Furthermore, if the setpoint of “SG pressure low 2” is reached, the isolation of the low load line of ARE [MFFCS] is actuated by KDS [DAS]. The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory.

The RCP [RCS] cooldown induces positive reactivity in the core, and the reactor may return to criticality. However, the Doppler Effect may limit the power excursion.

If the setpoint of “Hot leg pressure low 3” Safety Injection (SI) signal is reached, the RIS [SIS] is automatically actuated by KDS [DAS] to compensate the reactivity insertion and maintain the core sub-critical. The controlled state can be reached.

b) From the Controlled State to the Safe State

The affected VDA [ASDS] can be isolated by the operator via local manual actions. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.4.5 Analysis Result

The transient evolution and main safety functions of this event are similar to those of the DBC event in Sub-chapter 12.9.1.1. The discharge size of one, two or three VDA [ASDS] trains is within the break spectrum ranged from DN50 (corresponding to nominal diameter 50 mm) to double ended guillotine break analysed in Sub-chapter 12.9.1.1. Considering the safety margin shown in Sub-chapter 12.9.1.1, it is justified that no DNB occurs and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this event.

12.12.1.5 Spurious Isolation of All Main Feedwater (State A\B)

12.12.1.5.1 Description

This event leads to loss of main feedwater flow and thus the decrease in heat removal by the secondary system. During power operation, the decrease in heat removal causes the increase in primary coolant temperature and inadequate cooling of fuel cladding. Therefore, this event may lead to the risk of DNB (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DEC-A event causing similar initiating event and transient evolution is “Loss of Main Feedwater Flow – ATWS Due to RPS [PS] Failure (State A)” in Reference [102]. Similar to this fault, the bounding case is spurious isolation of all main feedwater at full power level to maximise primary heat and to penalise the DNBR.

12.12.1.5.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.5.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on “SG level (narrow range) low 1” or “Pressuriser pressure high 2” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

d) The MSSVs open automatically when SG pressure reaches the setpoint.

e) The PSVs open automatically when pressuriser pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS].

12.12.1.5.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

The loss of main feedwater flow leads to increase of primary coolant temperature. Reactor trip is automatically triggered by “SG level (narrow range) low 1” or “pressuriser pressure high 2” signal of KDS [DAS], which subsequently actuates the turbine trip.

After reactor trip, the PSV and MSSV may open automatically to limit the primary and secondary pressure separately. The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory.

Then the controlled state can be reached.

b) From the Controlled State to the Safe State

The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.5.5 Analysis Result

The transient evolution and main safety functions of this event are nearly same as those of the DEC-A event “Loss of Main Feedwater Flow – ATWS Due to RPS [PS] Failure (State A)” in Reference [102]. Considering the safety margin shown in Reference [102], it is justified that the DNBR limit will not be exceeded and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this event.

12.12.1.6 Spurious Isolation of All RHR Trains (state C\D\E\F)

12.12.1.6.1 Description

In state C\D\E when RHR trains are connected to remove core decay heat, this event leads to loss of decay heat removal by RHR trains and thus the increase in primary coolant temperature. In state F there is no fuel in the core, so this event could not affect the reactor core safety (Reference [99]).

In state C1, C2 and C3a the RCP [RCS] is not open or can be pressurised, the secondary side can be used to remove the decay heat.

In state C3b, D and E, the RCP [RCS] is open and cannot be pressurised, the reactor coolant keeps evaporating due to decay heat and it may cause core level drop.

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

12.12.1.6.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

a) The core remains sub-critical;

b) The residual heat can be continuously removed, i.e., RCP [RCS] water inventory remains stable and the capacity of RIS [SIS] trains in RHR mode is able to satisfy the requirement of heat removal.

12.12.1.6.3 Main Safety Functions

In order to reach the controlled state and the safe state, the following main safety functions via KDS [DAS] or manual actions are required:

a) The MSSVs open automatically when SG pressure reaches the setpoint;

b) The PSVs open automatically when pressuriser pressure reaches the setpoint;

c) The RIS [SIS] is actuated by the “RCP [RCS] loop level low 1” signal;

d) The RIS/RHR trains are recovered via local manual actions.

Besides, in state C1, C2 and C3a, the secondary side can be used by the operator to remove the decay heat using VDA [ASDS] if necessary.

12.12.1.6.4 Typical Event Sequences

This event leads to loss of decay heat removal by RHR trains.

In state C1, C2 and C3a, the primary system is not open or can be pressurised. The temperature and pressure of primary system may rise. The secondary side can be used by the operator using VDA [ASDS] via KDS [DAS] to remove the decay heat.

In state C3b, D and E, the primary system is open and cannot be pressurised. The primary coolant temperature increases due to decay heat and it may cause core level drop. SI signal can be triggered by “RCP [RCS] loop level low 1” signal of KDS [DAS]. Then the primary coolant inventory can be compensated by MHSI flow.

The operator can perform local manual actions to recover the RIS/RHR trains to restore the decay heat removal.

12.12.1.6.5 Analysis Result

In state C3b, D and E, the transient evolution of this event is similar to that of the DEC-A event "Total Loss of Cooling Chain (TLOCC) (Shutdown Condition) (States C3b and D)" in Reference [103]. Considering the safety margin shown in Reference [103], it is justified that there is enough time for the operator to recover the RIS/RHR trains so as to restore the decay heat removal for this event.

In state C1, C2 and C3a, the consequence of this event can be bounded by the DEC-A event "Loss of Ultimate Heat Sink (LUHS) for 100 Hours (States A and B)" (Reference [104]) due to the similar mitigation measures (by the secondary side) and the higher residual heat to be removed in state A for the LUHS event. It is justified that there is enough time for the operator to recover the RIS/RHR trains so as to restore the decay heat removal for this event.

12.12.1.7 Spurious Isolation of One or More Steam Lines (State A\B)

12.12.1.7.1 Description

This event leads to decrease in or loss of secondary steam flow and thus the increase in primary coolant temperature and pressure. Therefore, this event may lead to the risk of DNB (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC event causing similar initiating event and transient evolution is "Inadvertent Closure of One or All Main Steam Isolation Valves" (Sub-chapter 12.8.2.1).

Similar to Sub-chapter 12.8.2.1, the bounding case is spurious isolation of one or all main steam lines at full power level because the core power is higher than that in other state.

12.12.1.7.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.7.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on “Pressuriser pressure high 2” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) The MSSVs open automatically when SG pressure reaches the setpoint.

f) The PSVs open automatically when pressuriser pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS].

12.12.1.7.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

This event leads to increase of primary coolant temperature and pressure. Reactor trip is automatically triggered by “Pressuriser pressure high 2” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the PSV and MSSV may open automatically to limit the primary and secondary pressure separately. The ASG [EFWS] may be automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory. The RCP [RCS] will remain stable and the controlled state can be reached.

b) From the Controlled State to the Safe State

The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.7.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to those of the DBC event in Sub-chapter 12.8.2.1. Compared with the DBC event, automatic reactor trip signal of this event may be a little later. Considering the safety margin shown in Sub-chapter 12.8.2.1, it is justified that the DNBR limit will not be exceeded and the limit of fuel pellet temperature and cladding temperature are not challenged for this event.

12.12.1.8 Spurious Shutdown of All the Reactor Coolant Pumps (State A\B\C)

12.12.1.8.1 Description

This event leads to decrease of primary coolant flowrate and thus results in increase of primary coolant temperature and pressure. Therefore, this event may lead to the risk of DNB (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DEC-A event causing similar initiating event and transient evolution is “LOOP - ATWS Due to RPS [PS] Failure (State A)” in Reference [102], which analyses the case of LOOP that leads to coast-down of all RCP [RCS] pumps and trip of all feedwater pumps and condensate pumps.

Similar to Reference [102], the bounding case is spurious shutdown of all the reactor coolant pumps at full power level to maximise primary heat and to penalise the DNBR.

12.12.1.8.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.8.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on “Low flowrate in one primary loop coincident with P8” or “Pressuriser pressure high 2” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) The MSSVs open automatically when SG pressure reaches the setpoint.

f) The PSVs open automatically when pressuriser pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS].

12.12.1.8.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

This event leads to rapid decrease of primary coolant flowrate and thus results in increase of primary coolant temperature and pressure. Reactor trip is automatically triggered by “Low flowrate in one primary loop coincident with P8” or “Pressuriser pressure high 2” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the PSV and MSSV may open automatically to limit the primary and secondary pressure separately. The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory.

Then the controlled state can be reached.

b) From the Controlled State to the Safe State

The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.8.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to

those of the DEC-A event "LOOP – ATWS Due to RPS [PS] Failure" in Reference [102]. Compared with the DEC-A event, the overheating consequence of this event is less serious because the DEC-A event leads to coast-down of all RCP [RCS] pumps as well as trip of all feedwater pumps. Considering the safety margin shown in Reference [102], it is justified that the DNBR limit will not be exceeded and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this event.

12.12.1.9 Spurious Isolation of RCV [CVCS] Letdown due to Isolation of the Containment at Stage A (State A\B\C\D\E\F)

12.12.1.9.1 Description

The isolation of the containment at stage A leads to several actions. However, the only action which may challenge the core safety is the isolation of RCV [CVCS] letdown with the charging line remains open. The increase in primary coolant inventory may result in increase in pressuriser pressure and level. The cooling down of the RCP [RCS] causes a core power increase due to moderator temperature feedback (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC event causing similar initiating event and transient evolution is "Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction" (Sub-chapter 12.7.5.1).

Similar to Sub-chapter 12.7.5.1, the bounding case is spurious isolation of RCV [CVCS] letdown at full power level because the core power is higher than that in other states.

12.12.1.9.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.9.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on "Pressuriser pressure high 2" signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) The MSSVs open automatically when SG pressure reaches the setpoint.

f) The PSVs open automatically when pressuriser pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The RCV [CVCS] charging lines can be isolated by the operator via KDS [DAS].

12.12.1.9.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

The isolation of RCV [CVCS] letdown leads to increase of pressuriser level and pressure. Reactor trip is automatically triggered by “Pressuriser pressure high 2” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the PSV and MSSV may open automatically to limit the primary and secondary pressure separately. The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory. The controlled state can be reached.

b) From the Controlled State to the Safe State

The RCV [CVCS] charging lines can be isolated by the operator via KDS [DAS] to terminate the increase in primary coolant inventory. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.9.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to that of the DBC event in Sub-chapter 12.7.5.1. Compared with the DBC event, automatic reactor trip signal of this event may be a little later, while the initiating event is less serious because the DBC event analyses a faster increase in primary coolant inventory due to the closure of RCV [CVCS] letdown line cumulated with a failure of the RCV [CVCS] charging line control valve during high purification mode, and two high pressure charging pumps are in operation. Considering the safety margin shown in Sub-chapter 12.7.5.1, it is justified that the DNBR limit will not be exceeded and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this event.

12.12.1.10 Spurious Actuation of One or More MHSI Trains with Large Miniflow Line Closed (State B)

12.12.1.10.1 Description

In state B, the RCP [RCS] pressure may be higher or lower than the MHSI injection header. When the RCP [RCS] pressure is lower than the MHSI injection header, this event leads to increase of primary coolant inventory and RCP [RCS] pressure (Reference [99]).

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

12.12.1.10.2 Acceptance Criteria

The acceptance criterion of overpressure to be considered for this event is that the RCP [RCS] pressure shall not exceed 100% design pressure.

12.12.1.10.3 Main Safety Functions

The MHSI can be stopped by the operator via local manual actions.

The main safety functions claimed from the controlled state to the safe state are similar to those described in Sub-chapter 12.12.1.1.3.

These functions can be performed by the manual actions of the operator via KDS [DAS].

12.12.1.10.4 Typical Event Sequences

In state B, the reactor is in Normal Shutdown with Steam Generators (NS/SG) mode and the pressuriser is in two-phase state. The RCP [RCS] pressure will rise to and stabilise at the MHSI injection pressure. After that, there will be no injection flow into the RCP [RCS]. Then the operator can stop MHSI via local manual actions to terminate the transient.

12.12.1.10.5 Analysis Result

It is justified that the limit of RCP [RCS] pressure will not be exceeded and the reactor can be taken to the safe state.

12.12.1.11 Spurious Actuation of One or More MHSI Trains with Large Miniflow Line Open (State C\D\E\F)

12.12.1.11.1 Description

In state C\D\E\F, the RCP [RCS] pressure is lower than the MHSI injection header so this event leads to increase of primary coolant inventory and RCP [RCS] pressure. Therefore the main consequence is the overpressure risk of RCP [RCS] in cold shutdown state (Reference [99]).

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding overpressure event causing similar initiating event and transient evolution is “Overpressure Protection in Cold Shutdown State - Category 2” (Reference [105]) which analyses the case of start-up of all 3 MHSI pumps with all large mini-flow lines open.

Similar to Reference [105], the bounding case is spurious actuation of all MHSI trains with large miniflow line open in state C2 because from the view of reactor pressure vessel brittle facture risk, low temperature is more limiting to the equipment and at state C3\D\E the RCP [RCS] loop level is either lower or not pressurisable, which are all not limiting in primary pressure.

12.12.1.11.2 Acceptance Criteria

Refering to Reference [105], the acceptance criteria of overpressure to be considered for this event is that the RCP [RCS] pressure shall not greater than 100% of RHR design pressure.

12.12.1.11.3 Main Safety Functions

The overpressure of RCP [RCS] is protected by opening of the RIS/RHR safety valves. Besides, the MHSI can be stopped by the operator via local manual actions.

For this event, the RIS/RHR trains initially in service can be used to maintain the long-term heat removal.

12.12.1.11.4 Typical Event Sequences

The actuation of MHSI trains leads to increase in primary coolant inventory and RCP [RCS] pressure. When RIS/RHR system pressure reaches the setpoint, the RIS/RHR safety valves will open automatically to limit RCP [RCS] pressure. The operator can stop MHSI via local manual actions to terminate the transient.

The RIS/RHR trains initially in service remain in operation during the transient, which allows maintaining the long-term heat removal.

12.12.1.11.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to the overpressure event analysed in Reference [105]. Considering the safety margin shown in Reference [105], it is justified that the limit of RCP [RCS] pressure will not be exceeded and the reactor can be taken to the safe state.

12.12.1.12 Spurious Opening of One PSV (State C\D\E\F)

12.12.1.12.1 Description

This event is spuriously actuated by “Hot leg pressure (WR) high 1”, “Hot leg pressure (WR) high 2” or “Hot leg pressure (WR) high 3” signal of PRS [PS]. These signals aim at providing low-temperature overpressure protection. The spurious signal could only actuate opening of one PSV due to the different setpoints of “Hot leg pressure high 1”, “Hot leg pressure high 2” and “Hot leg pressure high 3” signals. It is conservatively assumed that the affected PSV remains open during the transient. Thus this event could lead to loss of primary coolant which possibly results in core heat-up (Reference [99]).

Since this event is initiated by RPS [PS], both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC event causing similar initiating event and transient evolution is “Small Break - Loss of Coolant Accident (State C\D\E)” (Sub-chapter 12.9.5.4).

12.12.1.12.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

a) The peak cladding temperature must remain lower than 1204℃;

b) The maximum cladding oxidation must remain lower than 17% of the total cladding thickness before oxidation;

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

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

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

However, if the core remains covered during the transient, the above criteria are considered to be met.

12.12.1.12.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) The Safety Injection System (RIS [SIS]) is actuated by “RCP [RCS] loop level low 1” signal;

b) The RCP [RCS] pumps are stopped by “RCP [RCS] pump ΔP low 1 coincident with SI signal”.

The affected PSV can be closed by the operator via local manual actions.

For this event, the RIS/RHR trains initially in service can be used to maintain the long-term heat removal.

12.12.1.12.4 Typical Event Sequences

The spurious opening of one PSV leads to loss of primary coolant. RIS [SIS] is automatically actuated by “RCP [RCS] loop level low 1” SI signal of KDS [DAS]. The RCP [RCS] pumps are automatically stopped by “RCP [RCS] pump ΔP low 1 coincident with SI signal” of KDS [DAS].

The LHSI pumps in RHR mode ensure the RCP [RCS] heat removal. The MHSI flow compensates for the break flow and the RCP [RCS] inventory can stabilise. The controlled state can be reached.

The affected PSV can be closed by the operator via local manual actions. Then the safe state can be reached.

12.12.1.12.5 Analysis Result

The transient evolution and main safety functions of this event are similar to those of the corresponding DBC event “Small Break - Loss of Coolant Accident (State C\D\E)” in Sub-chapter 12.9.5.4. Compared with the DBC event, the equivalent break area of this event is a little larger, but the break is located on the top of the pressuriser so that there is no loss of SI flow and thus the consequence of this event is less serious. Besides, this event in state C can be bounded by the DEC-A event “Small Break Loss of Coolant Accident – ATWS Due to RPS [PS] Failure (State A)” analysed in Reference [102] because the core power and primary coolant temperature at full power level are higher than that in state C. Considering the safety margin shown in Sub-chapter 12.9.5.4 and Reference [102], it is justified that no significant core heat-up would occur and the safe state can be reached for this event.

12.12.1.13 Spurious opening of the letdown line or isolation of the charging line of RCV [CVCS] (State A\B\C\D\E\F)

12.12.1.13.1 Description

This event leads to decrease in primary coolant inventory which may result in inadequate core cooling. The spurious opening of RCV [CVCS] letdown line is actuated by SAS while the spurious isolation of RCV [CVCS] charging line is actuated by RPS [PS] (Reference [99]).

Since this event is initiated by RPS [PS] or SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DBC events causing similar initiating event and transient evolution are “Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction” (Sub-chapter 12.7.6.1) and “Uncontrolled RCP [RCS] Level Drop” (state C\D\E) (Sub-chapter 12.8.5.4).

Similar to Sub-chapter 12.7.6.1 and 12.8.5.4, this event includes 2 bounding cases:

a) At full power level in state A, because the core power and the primary coolant temperature are higher than that at any other power levels (Similar to Sub-chapter 12.7.6.1);

b) In state C3\D, because the RCP [RCS] level is lower and the primary coolant inventory is smaller than that in other states (Similar to Sub-chapter 12.8.5.4).

12.12.1.13.2 Acceptance Criteria

For this event occurred in State A\B, the decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied:

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

b) The peak cladding temperature must remain less than 1482℃;

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

For this event occurred in State C\D\E\F, the acceptance criteria to be considered are:

a) Core water inventory is stable;

b) Residual heat removal is ensured on a long term basis.

Both criteria are verified if the RIS [SIS]\RHR pumps are maintained in operation.

12.12.1.13.3 Main Safety Functions

a) Event occurred in state A\B

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

1) Reactor trip is actuated on “Pressuriser pressure low 2” signal;
2) Turbine trip is actuated by reactor trip signal;
3) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;
4) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;
5) The MSSVs open automatically when SG pressure reaches the setpoint;
6) The Safety Injection System (RIS [SIS]) is actuated by “Hot leg pressure low 3” signal;
7) The containment isolation at stage A is acutated by SI signal.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

1) Startup of ASG [EFWS]
2) Startup/Isolation of RBS [EBS]
3) Startup of cooldown via VDA [ASDS]
4) RCP [RCS] depressurisation
5) Accumulators isolation
6) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The RCV [CVCS] letdown lines can be isolated by the operator via KDS [DAS].

b) Event occurred in state C\D\E\F

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

1) The Safety Injection System (RIS [SIS]) is actuated by “RCP [RCS] loop level low 1” signal;
2) The containment isolation at stage A is acutated by SI signal.

The RIS/RHR trains initially in service can be used to maintain the long-term heat removal. The RCV [CVCS] letdown lines can be isolated by the operator via KDS [DAS].

12.12.1.13.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

1) Event occurred in state A\B

The decrease in primary coolant inventory causes decrease in RCP [RCS] pressure. Reactor trip is automatically triggered by “Pressuriser pressure low 2” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the MSSV may open automatically to limit the secondary pressure. If the setpoint of “SG level (wide range) low 2” signal of KDS [DAS] is reached, the ASG [EFWS] is automatically actuated to compensate for the secondary side inventory. If the RCP [RCS] pressure continues to drop and reaches the setpoint of “Hot leg pressure low 3” signal of KDS [DAS], SI signal is automatically actuated. The SI signal subsequently triggers the containment isolation at stage A, which includes the isolation of RCV [CVCS] letdown line to terminate the decrease in primary coolant inventory. Then the controlled state can be reached.

2) Event occurred at state C\D\E\F

The decrease in primary coolant inventory causes decrease in RCP [RCS] pressure and drop of water level. RIS [SIS] is automatically actuated by “RCP [RCS] loop level low 1” signal of KDS [DAS]. The SI signal subsequently triggers the containment isolation at stage A, which includes the isolation of RCV [CVCS] letdown line. Then the controlled state can be reached. If the SI signal is not triggered, the RCV [CVCS] letdown lines can be isolated by the operator via local manual actions to terminate the decrease in primary coolant inventory.

b) From the Controlled State to the Safe State

1) Event occurred at full power operation

The RCV [CVCS] letdown lines can be isolated by the operator via local manual actions. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

2) Event occurred at state C\D\E

The RCV [CVCS] letdown lines can be isolated by the operator via local manual actions. The RIS/RHR trains initially in service remain in operation during the transient, which allows keeping the long-term heat removal.

12.12.1.13.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to

those of the corresponding DBC events in Sub-chapter 12.7.6.1 and 12.8.5.4. Compared with the DBC event in Sub-chapter 12.7.6.1, automatic reactor trip signal of this event may be a little later, but the initiating event is less serious because the DBC event analyses a faster decrease in primary coolant inventory due to opening of both high pressure reducing stations while two charging pumps are in operation. Considering the safety margin shown in Sub-chapter 12.7.6.1, it is justified that the DNBR limit will not be exceeded and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this event. Compared with the DBC event in Sub-chapter 12.8.5.4, automatic SI signal of this event may be a little later. Considering the safety margin shown in Sub-chapter 12.8.5.4, it is justified that the core water inventory can be maintained and the safe sate can be reached for this event.

12.12.1.14 Spurious Start-up of All the Pressuriser Heaters (State A\B\C\D\E\F)

12.12.1.14.1 Description

In state A\B, this event leads to increase in the RCP [RCS] pressure and temperature which may cause the risk of DNB (Reference [99]).

In state C\D\E\F, this event leads to increase in the RCP [RCS] pressure which may cause the risk of overpressure in cold shutdown state (Reference [99]).

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding events causing similar initiating event and transient evolution is the DBC event “Spurious Pressuriser Heater Operation” (Sub-chapter 12.7.7.1) and the overpressure event “Overpressure Protection in Cold Shutdown State - Category 2” (Reference [105]).

This event includes 2 bounding cases:

a) At full power level in state A, because the core power and the primary coolant temperature are higher than that at other states (similar to Sub-chapter 12.7.7.1);

b) In state C2, because the temperature is lower to penalise the brittle facture risk (similar to Reference [105]).

12.12.1.14.2 Acceptance Criteria

For this event occurred in State A\B, the decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied:

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

b) The peak cladding temperature must remain less than 1482℃;

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

For this event occurred in State C\D\E\F, the acceptance criteria of overpressure to be

considered for this event is that the RCP [RCS] pressure shall not greater than 100% of RHR design pressure.

12.12.1.14.3 Main Safety Functions

a) Event occurred in state A\B

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

1) Reactor trip is actuated on “Pressuriser pressure high 2” signal;
2) Turbine trip is actuated by reactor trip signal;
3) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;
4) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;
5) The MSSVs open automatically when SG pressure reaches the setpoint;
6) The PSVs open automatically when pressuriser pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

1) Startup of ASG [EFWS]
2) Startup/Isolation of RBS [EBS]
3) Startup of cooldown via VDA [ASDS]
4) RCP [RCS] depressurisation
5) Accumulators isolation
6) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The pressuriser heaters can be stopped by the operator via manual actions.

b) Event occurred in state C\D\E\F

The overpressure of RCP [RCS] is protected by opening of the RIS/RHR safety valves. Besides, the pressuriser heaters can be stopped by the operator via manual actions.

For this event, the RIS/RHR trains initially in service can be used to maintain the long-term heat removal.

12.12.1.14.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

1) Event occurred in state A\B

The start-up of all pressuriser heaters causes increase in RCP [RCS] pressure and temperature. Reactor trip is automatically triggered by “Pressuriser pressure high 2” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the PSV and MSSV may open automatically to limit the primary and secondary pressure separately. The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory. The controlled state can be reached.

The start-up of all pressuriser heaters causes increase in RCP [RCS] pressure. When RIS/RHR pressure reaches the setpoint, the RIS/RHR safety valves will open automatically to limit RCP [RCS] pressure.

2) Event occurred in state C\D\E\F

The start-up of all pressuriser heaters causes increase in RCP [RCS] pressure. When RIS/RHR pressure reaches the setpoint, the RIS/RHR safety valves will open automatically to limit RCP [RCS] pressure.

b) From the Controlled State to the Safe State

1) Event occurred in state A\B

The pressuriser heaters can be stopped by the operator via manual actions. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

2) Event occurred in state C\D\E\F

The pressuriser heaters can be stopped by the operator via manual actions. The RIS/RHR trains initially in service can be used to maintain the long-term heat removal.

12.12.1.14.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to those of the corresponding DBC event in Sub-chapter 12.7.7.1 and of the overpressure event in Reference [105].

Compared with the DBC event in Sub-chapter 12.7.7.1, automatic reactor trip signal of this event may be a little later. Considering the safety margin shown in Sub-chapter 12.7.7.1, it is justified that the DNBR limit will not be exceeded and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this event.

Compared with the overpressure event in Reference [105], the main safety function is same. Considering the safety margin shown in Reference [105], it is justified that the limit of RCP [RCS] pressure will not be exceeded and the reactor can be taken to the safe state.

12.12.1.15 Spurious Opening of the Pressuriser Auxiliary Spray Line (State A\B\C\D\E\F)

12.12.1.15.1 Description

This event leads to decrease in the RCP [RCS] pressure which may cause the risk of DNB (Reference [99]).

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DEC-A events causing similar initiating event and transient is "Spurious Pressuriser Spraying - ATWS Due to RPS [PS] Failure (State A)" (Reference [102]), which analyses the case of spurious start-up of pressuriser spray.

Similar to Reference [102], the bounding case is spurious start-up of pressuriser auxiliary spray at full power level to maximise primary system heat-up and to penalise the DNBR.

12.12.1.15.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.15.3 Main Safety Functions

In order to reach the controlled state, the following main safety functions via KDS [DAS] are required:

a) Reactor trip is actuated on "Pressuriser pressure low 2" signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the "SG level (wide range) low 2" signal;

e) The MSSVs open automatically when SG pressure reaches the setpoint;

f) The Safety Injection System (RIS [SIS]) is actuated by "Hot leg pressure low 3" signal.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

In order to reach the safe state, the following manual safety functions are required:

a) Startup of ASG [EFWS]

b) Startup/Isolation of RBS [EBS]

c) Startup of cooldown via VDA [ASDS]

d) RCP [RCS] depressurisation

e) Accumulators isolation

f) Connection of RIS [SIS] in RHR mode

These functions can be performed by the manual actions of the operator via KDS [DAS]. The pressuriser auxiliary spray can be isolated by the operator via local manual actions.

12.12.1.15.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

The start-up of pressuriser auxiliary spray leads to decrease in RCP [RCS] pressure. Reactor trip is automatically triggered by “Pressuriser pressure low 2” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the MSSV may open automatically to limit the secondary pressure. The ASG [EFWS] is automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory. If the RCP [RCS] pressure continues to drop, RIS [SIS] is automatically actuated by “Hot leg pressure low 3” signal of KDS [DAS]. The controlled state can be reached.

b) From the Controlled State to the Safe State

The pressuriser auxiliary spray can be isolated by the operator via local manual actions. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.15.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to those of the DEC-A event “Spurious Pressuriser Spraying - ATWS Due to RPS [PS] Failure (State A)” in Reference [102]. Considering the safety margin shown in Reference [102], it is justified that the DNBR limit will not be exceeded and the limit of fuel cladding temperature and fuel melt temperature are not challenged for this

event.

12.12.1.16 Spurious Isolation of One or More PTR [FPCTS] Cooling Trains (State A\B\C\D\E\F)

12.12.1.16.1 Description

This event leads to loss of PTR [FPCTS] cooling trains and thus causes the increase of SFP water temperature. The main consequence is the risk of uncovery of the spent fuel assemblies (Reference [99]).

Since this event is initiated by RPS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DEC-A event causing similar initiating event and transient is "Loss of Three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) Trains" (Reference [106]).

The bounding case is spurious isolation of all three PTR [FPCTS] trains to penalise the heat-up of the SFP.

12.12.1.16.2 Acceptance Criteria

The safety criteria for the DBC accidents associated with spent fuel storage pool are as applied for this event:

a) Permanent maintenance of sub-criticality;

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

12.12.1.16.3 Main Safety Functions

The PTR [FPCTS] cooling trains can be recovered by the operator via local manual actions to restore the heat removal from SFP.

12.12.1.16.4 Typical Event Sequences

This event leads to loss of SFP cooling and thus results in the increase of SFP water temperature. When the SFP water temperature reaches the saturation temperature, the decay heat of SFP is removed via the continuous evaporation of the SFP water. The SFP water level decreases. Meanwhile, the fuel building pressure increases.

According to Reference [106], as it takes several hours for the SFP water to reach the saturation temperature, the PTR [FPCTS] cooling trains can be recovered by the operator via local manual actions before the SFP is boiling.

12.12.1.16.5 Analysis Result

This initiating event is quite similar to the DEC-A event analysed in Reference [106]. According to Reference [106], it is justified that there is enough time for the operator to recover the PTR [FPCTS] trains so as to restore the heat removal for this event.

The fuel assemblies are covered during the whole transient process and the sub-criticality of the fuel assemblies is ensured by the design of spent fuel storage rack. Therefore, all acceptance criteria are met for this event.

12.12.1.17 Total Loss of RRI [CCWS] due to a Certain Spurious Actuation (State A\B) (for Reactor Core)

12.12.1.17.1 Description

In state A\B, total loss of RRI [CCWS] may lead to the following systems and components to be unavailable (Reference [99]) which is similar to the LUHS event in Reference [104]:

a) GCT [TBS];

b) RCV [CVCS];

c) All trains of MHSI;

d) Train C of LHSI;

e) All RHR exchangers;

f) Thermal barriers of RCP [RCS] pumps.

This event results in trip of RCP [RCS] pumps due to loss of the seal injection and the thermal barriers, while the shaft seal system can ensure the primary system integrity. The risk concerned is the heat-up of primary system and the decay heat removal.

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

The corresponding DEC-A event causing similar initiating event and transient evolution is “Loss of Ultimate Heat Sink (LUHS) for 100 Hours (States A and B)” (Reference [104]).

Similar to Reference [104], the bounding case is total loss of RRI [CCWS] at full power operation to maximise primary heat.

12.12.1.17.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

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

b) The peak cladding temperature must remain less than 1482℃;

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

12.12.1.17.3 Main Safety Functions

In order to reach the controlled state and the safe state, the following main safety functions via KDS [DAS] or manual actions are required:

a) Reactor trip is actuated on “Low flowrate in one primary loop coincident with P8” signal;

b) Turbine trip is actuated by reactor trip signal;

c) The ARE [MFFCS] full load isolation is actuated by reactor trip signal;

d) The ASG [EFWS] is actuated by the “SG level (wide range) low 2” signal;

e) The MSSVs open automatically when SG pressure reaches the setpoint.

f) The PSVs open automatically when pressuriser pressure reaches the setpoint.

The VDA [ASDS] may not open automatically as RPS [PS] is assumed to be unavailable. The MSSVs can open automatically to limit the secondary system pressure after reactor trip and turbine trip.

The operator can perform local manual actions to recover the RRI [CCWS] cooling loops. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.17.4 Typical Event Sequences

a) From the Initiating Event to the Controlled State

This event results in loss of the seal injection and thermal barriers, consequently leading to trip of RCP [RCS] pumps. Reactor trip is automatically triggered by “Low flowrate in one primary loop coincident with P8” signal of KDS [DAS], which subsequently actuates the turbine trip and the isolation of all full load lines of ARE [MFFCS].

After reactor trip, the PSV and MSSV may open automatically to limit the primary and secondary pressure separately. The ASG [EFWS] may be automatically actuated by “SG level (wide range) low 2” signal of KDS [DAS] to compensate for the secondary side inventory. The RCP [RCS] will remain stable and the controlled state can be reached.

b) From the Controlled State to the Safe State

The operator can perform local manual actions to recover the RRI [CCWS] cooling loops. The reactor can be taken to the safe state via the actions described in Sub-chapter 12.12.1.1.4.

12.12.1.17.5 Analysis Result

The transient evolution and main safety functions of this event are quite similar to

those of the DEC-A event in Reference [104]. Compared with the DEC-A event, automatic reactor trip signal of this event may be a little later. Considering the safety margin shown in Reference [104], it is justified that there is enough time for the operator to recover the RRI [CCWS] cooling loops and the safe state can be reached.

12.12.1.18 Total Loss of RRI [CCWS] due to a Certain Spurious Actuation (State C\D\E\F) (for Reactor Core)

12.12.1.18.1 Description

In state C\D\E, total loss of RRI [CCWS] may lead to the following systems and components to be unavailable (Reference [99]):

a) RCV [CVCS];

b) All trains of MHSI;

c) Train C of LHSI;

d) All RHR exchangers.

Consequently, this event leads to loss of decay heat removal by RHR trains and thus the increase in primary coolant temperature which is similar to the event in Sub-chapter 12.12.1.6.

In state F there is no fuel in the core, so this event could not affect the reactor core safety.

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

12.12.1.18.2 Acceptance Criteria

The decoupling criteria of DBC-4 adopted as strict criteria for the DEC-A analysis are applied for this event:

a) The core remains sub-critical;

b) The residual heat can be continuously removed, i.e., RCP [RCS] water inventory remains stable and the capacity of RIS [SIS] trains in RHR mode is able to satisfy the requirement of heat removal.

12.12.1.18.3 Main Safety Functions

In state C1\C2\C3a, the operator can identify the alarm of high RCP [RCS] pressure or temperature. If necessary, the secondary side can be used by the operator to remove the decay heat via VDA [ASDS]. Then the operator can perform local manual actions to recover the RRI [CCWS] cooling loops and restore RIS/RHR trains manually.

In state C3b\D\E, the SI signal can be triggered by “RCP [RCS] loop level low 1” of KDS [DAS]. The LHSI train A and train B are actuated and the cooling for LHSI can

be switched to the Safety Chilled Water System (DEL [SCWS]). Then the operator can perform local manual actions to recover the RRI [CCWS] cooling loops and restore RIS/RHR trains manually.

12.12.1.18.4 Typical Event Sequences

The total loss of RRI [CCWS] results in loss of decay heat removal by RHR trains.

In state C1\C2\C3a, the primary system is not open or can be pressurisable. The temperature and pressure of primary system may rise. The secondary side can be used by the operator using VDA [ASDS] via KDS [DAS] to remove the decay heat.

In state C3b\D\E, the primary system is open and cannot be pressurisable. The primary coolant temperature increases until evaporating due to decay heat and it may cause core level drop. SI signal can be triggered by “RCP [RCS] loop level low 1” signal of KDS [DAS]. Then the primary coolant inventory can be compensated by LHSI flow.

The operator can perform local manual actions to recover the RRI [CCWS] cooling loops and restore RIS/RHR trains manually.

12.12.1.18.5 Analysis Result

In state C3b\D\E, the transient evolution of this event is similar to those of the TLOCC event in Reference [103]. The LHSI flow is sufficient to compensate the evaporation of the primary coolant. Considering the safety margin shown in Reference [103], it is justified that there is enough time for the operator to recover the RRI [CCWS] cooling loops so as to restore the decay heat removal by RIS/RHR trains.

In state C1\C2\C3a, the consequence of this event can be bounded by the LUHS event in Reference [104] due to the similar mitigation measures (by the secondary side) and the higher residual heat to be removed in state A for the LUHS event. It is justified that there is enough time for the operator to recover the RRI [CCWS] cooling loops so as to restore the decay heat removal by RIS/RHR trains.

12.12.1.19 Total Loss of RRI [CCWS] due to a Certain Spurious Actuation (State A\B\C\D\E\F) (for SFP)

12.12.1.19.1 Description

This event leads to loss of cooling for pumps and exchangers of PTR [FPCTS] which results in loss of PTR [FPCTS] cooling trains for the SFP. The consequence of this event is quite similar to that of the event described in Sub-chapter 12.12.1.16 (Reference [99]).

Since this event is initiated by SAS, both RPS [PS] and SAS are assumed to be unavailable to provide protection or mitigation.

12.12.1.19.2 Acceptance Criteria

The safety criteria for the DBC accidents associated with spent fuel storage pool are as applied for this event:

a) Permanent maintenance of sub-criticality;

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

12.12.1.19.3 Main Safety Functions

The RRI [CCWS] cooling loops can be recovered by the operator via local manual actions to restore the PTR [FPCTS] cooling trains.

12.12.1.19.4 Typical Event Sequences

This event leads to loss of SFP cooling and thus results in the increase of SFP water temperature. When the SFP water temperature reaches the saturation temperature, the decay heat of SFP is removed via the continuous evaporation of the SFP water. The SFP water level decreases. Meanwhile, the fuel building pressure increases.

According to Reference [106], as it takes several hours for the SFP water to reach the saturation temperature, the PTR [FPCTS] cooling trains can be recovered by the operator via local manual actions before the SFP is boiling.

12.12.1.19.5 Analysis Result

The consequence of this event is quite similar to that of the event described in Sub-chapter 12.12.1.16. It is justified that there is enough time for the operator to recover the PTR [FPCTS] trains so as to restore the heat removal for this event.

The fuel assemblies are covered during the whole transient process and the sub-criticality of the fuel assemblies is ensured by the design of spent fuel storage rack. Therefore, all acceptance criteria are met for this event.

12.12.2 Loss of Support Systems

12.12.2.1 Loss of RRI [CCWS] or SEC [ESWS] train A and train C (State C\D\E) (for Reactor Core)

12.12.2.1.1 Description

This event is classified as a specific condition and is the representative of the following events which cause similar transient impact on the reactor core (Reference [100]):

a) Loss of LVB ([UPS(NI-380V-2h)]) / LVP ([UPS(NI-380V-24h)]);

b) Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room (DVL [EDSBVS] 4510/4520CL- and DVL [EDSBVS] 5510/5520CL-).

This event leads to loss of two RIS-RHR trains in operation (train A and train C assumed) superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]). Besides, the additional impact on other key safety functions is loss of MHSI train A and train C, loss of LHSI train A (if the DEC-A features are not considered) and train C, loss of ASG [EFWS] train C and loss of RBS [EBS] train C.

12.12.2.1.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

a) Core water inventory is stable;

b) Heat removal is ensured on a long term basis.

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

12.12.2.1.3 Analysis Result

It is justified that the consequence of this event is not worse than and can be bounded by the DEC-A event "Total loss of RRI [CCWS] or SEC [ESWS] (A\B\C\D\E) (for Reactor Core)" in Sub-chapter 4.2 in Reference [100] due to the following reasons:

a) The SFC or preventive maintenance is not considered for this event according to the analysis rules;

b) This event leads to loss of two RIS-RHR trains, while the DEC-A event leads to loss of three RIS-RHR trains;

c) This event leads to loss of two MHSI trains and two LHSI trains, while the DEC-A event leads to loss of three MHSI trains and three LHSI trains;

d) The mitigation measures required for this event are similar to that required for the DEC-A event;

e) The analysis rules are the same for the two events.

As the acceptance criteria used for this event are the same as that of the DEC-A event "Total loss of RRI [CCWS] or SEC [ESWS] (A\B\C\D\E) (for Reactor Core)" in Reference [100], thus this event is bounded by the DEC-A event.

12.12.2.2 Loss of RRI [CCWS] or SEC [ESWS] train A and train C (State A\B) (for Reactor Core)

12.12.2.2.1 Description

This event is classified as a specific condition which causes transient impact on the reactor core (Reference [100]).

This event leads to loss of main feedwater superposed with increase/decrease in RCV

[CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]). Besides, the additional impact on other key safety functions is loss of MHSI train A and train C, loss of LHSI train A (if the DEC-A features are not considered) and train C, loss of RIS-RHR train A and train C, loss of ASG [EFWS] train C and loss of RBS [EBS] train C.

12.12.2.2.2 Acceptance Criteria

In terms of fuel integrity, the following acceptance criteria are used for this event:

a) The amount of the fuel experiencing DNB must remain less than 10%;

b) The peak cladding temperature must remain less than 1482℃;

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

For this event, the acceptance criteria of no DNB and no fuel melting are conservatively applied as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

12.12.2.2.3 Analysis Result

It is justified that the consequence of this event is similar to that of loss of RRI [CCWS] or SEC [ESWS] train A (State A\B) event described in Sub-chapter 12.7.9.1 due to the following reasons:

a) The SFC or preventive maintenance is not considered for this event according to the analysis rules;

b) The transient evolution, the required safety functions and mitigation measures are similar to that claimed in Sub-chapter 12.7.9.1;

c) Compared to that event analysed in Sub-chapter 12.7.9.1, though this event leads to loss of some safety function trains, the remaining trains are able to carry out the required functions.

As the acceptance criteria used for this event are the same as that used in Sub-chapter 12.7.9.1, there are reasons to believe that the acceptance criteria can be met for this event based on the analysis result in Sub-chapter 12.7.9.1.

12.12.2.3 Loss of RRI [CCWS] or SEC [ESWS] train A and train C (State A\B\C\D\E\F) (for SFP)

12.12.2.3.1 Description

This event is classified as a specific condition and is the representative of the following event which causes similar transient impact on the SFP (Reference [100]):

a) Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room (DVL [EDSBVS] 4510/4520CL- and DVL [EDSBVS] 5510/5520CL-).

This event leads to loss of two PTR [FPCTS] cooling trains in operation (train A and train C assumed). Besides, there is no additional impact on other key safety functions in terms of the SFP.

The following DBC-2 and DBC-3 events cause similar transient impact on the SFP:

a) Loss of One PTR [FPCTS] Train (State A\B\C\D) (Sub-chapter 12.7.8.1);

b) Loss of One PTR [FPCTS] Train (State E\F) (Sub-chapter 12.8.6.2).

12.12.2.3.2 Acceptance Criteria

The following acceptance criteria associated with the SFP are used for this event:

a) Permanent maintenance of sub-criticality;

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

12.12.2.3.3 Analysis Result

It is justified that the consequence of this event is not worse than and can be bounded by that described in Sub-chapter 12.7.8.1 and 12.8.6.2 due to the following reasons:

a) The SFC or preventive maintenance is not considered for this event according to the analysis rules;

b) This event leads to loss of two PTR [FPCTS] cooling trains, which is actually equivalent to the events analysed in Sub-chapter 12.7.8.1 and 12.8.6.2 where the initiating event leads to loss of one PTR [FPCTS] cooling train and another train is assumed to be unavailable due to the single failure or preventive maintenance. As a result, the remaining third train is available.

As the acceptance criteria used for this event are the same as that used in Sub-chapter 12.7.8.1 and 12.8.6.2, thus there are reasons to believe that the acceptance criteria can be met for this event.

12.12.2.4 Loss of RRI [CCWS] or SEC [ESWS] train A and train B (State A\B) (for Reactor Core)

12.12.2.4.1 Description

This event is classified as a specific condition and is the representative of the following event which causes similar transient impact on the reactor core (Reference [100]):

a) Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room (DVL [EDSBVS] 4510/4520CL- and DVL [EDSBVS] 5510/5520CL-).

This event leads to loss of main feedwater superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]) and loss of RCP [RCS] pumps (i.e. pump shutdown). Additionally, the impact on other key safety functions is loss of MHSI trains A and train B, loss of LHSI train A and train B (if the DEC-A features are not considered) and loss of RIS-RHR train A and train B.

12.12.2.4.2 Acceptance Criteria

In terms of fuel integrity, the following acceptance criteria are used for this event:

a) The amount of the fuel experiencing DNB must remain less than 10%;

b) The peak cladding temperature must remain less than 1482℃;

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

For this event, the acceptance criteria of no DNB and no fuel melting are conservatively applied as follows:

a) The minimum DNBR shall be greater than DNBR design limit;

b) The peak cladding temperature shall remain lower than 1482℃ and the fuel pellet temperature shall not exceed { }℃.

12.12.2.4.3 Analysis Result

It is justified that the consequence of this event is similar to that described in Sub-chapter 12.8.8.1 due to the following reasons:

a) The SFC or preventive maintenance is not considered for this event according to the analysis rules;

b) The transient evolution, available safety functions and mitigation measures which are required are similar to that claimed in Sub-chapter 12.8.8.1.

As the acceptance criteria used for this event are the same as that used in Sub-chapter 12.8.8.1, there are reasons to believe that the acceptance criteria can be met for this event.

12.12.2.5 Loss of DVL [EDSBVS] train A&B local cooling units in RRI [CCWS] pump room (DVL [EDSBVS] 4510/4520CL- and DVL [EDSBVS] 5510/5520CL-) (State C) (for Reactor Core)

12.12.2.5.1 Description

This event is classified as a specific condition which causes transient impact on the reactor core (Reference [100]).

This event leads to loss of two RIS-RHR trains in operation superposed with increase/decrease in RCV [CVCS] charging/letdown flow (i.e. control failure of RCV [CVCS]) and loss of RCP [RCS] pumps (i.e. pump shutdown). Besides, the additional

impact on other key safety functions is loss of two MHSI trains and loss of two LHSI trains.

12.12.2.5.2 Acceptance Criteria

The acceptance criteria to be considered for this event are:

a) Core water inventory is stable;

b) Heat removal is ensured on a long term basis.

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

12.12.2.5.3 Analysis Result

It is justified that the consequence of this event is not worse than and can be bounded by the DEC-A event "Total loss of RRI [CCWS] or SEC [ESWS] (A\B\C\D\E) (for Reactor Core)" in Sub-chapter 4.2 in Reference [100] due to the same reasons as that presented in Sub-chapter 12.12.2.1.

As the acceptance criteria used for this event are the same as that of the DEC-A event, thus this event does not need further analysis.

As the acceptance criteria used for this event are the same as that of the DEC-A event "Total loss of RRI [CCWS] or SEC [ESWS] (A\B\C\D\E) (for Reactor Core)" in Reference [100], thus this event is bounded by the DEC-A event.

12.12.3 Others

12.12.3.1 Double-ended Guillotine Failure of Largest RCS Pipe

12.12.3.1.1 Description

A Large Break Loss of Coolant Accident (LB-LOCA) including Double-ended Guillotine Failure of Largest RCS Pipe induces a rapid loss of primary coolant. It results in an abrupt decrease of RCP [RCS] pressure and pressuriser level with a significant core heat-up due to limited heat removal capacity under accident condition. Core heat-up may lead to fuel damage. As the core at full power brings more challenge in heat removal function and higher possibility of fuel damage, the LB-LOCA at state A is analysed. LB-LOCA is classified as specific study since the main coolant line is classified as HIC. Further clarification for LB-LOCA safety case is presented in Reference [107].

12.12.3.1.2 Acceptance Criteria

With loss of primary reactor coolant, fuel integrity and core cooling may be challenged. To limit fuel failure and ensure core cooling, the following acceptance criteria shall be met during this transient:

a) The Peak cladding Temperature (PCT) must remain lower than 1204 ℃;

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

c) The maximum hydrogen generation must remain lower than 1% of the amount that would be generated if the whole active part of the cladding were to react;

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

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

12.12.3.1.3 Analysis Result

The detailed analysis of this fault (see Reference [101]) shows that the highest PCT is 1131.2℃, which is lower than the acceptance criteria (1204℃). The maximum oxidation thickness rate is 8.11% (with initial value), which is smaller than 17% of the acceptance criteria. Total core hydrogen generation is lower than 0.89%. Therefore, total core hydrogen generation is below 1% the postulated maximum hydrogen generation, thus meets the acceptance criteria. The analysis results show that the core coolable geometry could be maintained during the transient.

12.12.3.2 Main Steam Line Large Break (Pipe with HIC classification)

For Main Steam Line Large Break (Pipe with HIC classification), the transient analysis is bounded by that of DBC-4 event: Steam System Piping Large Break.

12.13 Fault Schedule

12.13.1 Purpose and Production

The production of a Fault Schedule is relevant good practice (RGP) in the UK. The Fault Schedule establishes an auditable link between initiating faults considered in the design and requirements to be applied to safety measures. This visible link helps both designers and regulators to understand the status of design and work in a more efficient way. Thus a Fault Schedule for the UK HPR1000, which is a key tool for the UK HPR1000 design evolution during Generic Design Assessment (GDA), is produced and provided to ONR. During GDA, Fault Schedule is used as an input to system design process.

The objectives of the Fault Schedule are:

a) Establish a visible link between initiating faults considered in the design and requirements to be applied to safety measures (golden thread);

b) Help provide confidence that probabilistic targets set for the UK HPR1000 will ultimately be met;

c) Provide a connection between the deterministic analysis and the probabilistic analysis;

Two versions of the Fault Schedule are produced:

1) One is the Early Version of Fault Schedule [108]. It is a start point for Fault Schedule evolution, which is based on the DBC list in the PSR. For the early version, the diverse protection line is not demonstrated by transient analysis. This Fault Schedule will be used to inform the transient analysis for diverse protection lines.

2) The second is the UK HPR1000 Fault Schedule [109], which will be based on the DBC List for the UK HPR1000. The diverse protection lines are demonstrated by the transient analysis.

Reference [110] provides the detailed production methodology for the Fault Schedule.

As a complement to Fault Schedule, Confinement Schedule which focus on the confinement safety functions of containment and peripheral buildings, is produced [111]. Via Confinement Schedule, the safety requirements claimed in accidental radiological consequences can be found.

12.13.2 Main Information and Template

The Fault Schedule covers all DBCs and DEC-A sequences for UK HPR1000 and diverse protection lines are provided for frequent faults. According to the categorisation and classification methodology for the UK HPR1000, an important FC1 safety function in primary protection lines should be backed up by FC2 safety

functions; an important FC2 safety function in primary protection lines should be backed up by FC3 safety functions. The UK HPR1000 Fault Schedule follows this categorisation and classification methodology.

The initiating events in UK HPR1000 Fault Schedule and Confinement Schedule are based on *The Design Condition List and Acceptance Criteria*.

The final version of UK HPR1000 Fault Schedule includes DBCs, DEC-As and specific studies identified from loss of support systems and spurious actuation of I&C systems. The diverse protection lines are demonstrated and related supporting studies are linked.

In Confinement Schedule, safety function requirements for representative faults are selected and presented.

The template of the UK HPR1000 Fault Schedule and Confinement Schedule is presented in T-12.13-1. The following information is provided for each event:

a) All initiating faults considered in the design with their respective frequencies;

b) The safety functions involved for each initiating fault;

c) The safety systems to physically achieve the safety functions, including the mechanical systems, the signals to trigger the safety functions, the I&C platform to deal with the signal, the way of safety function actuation;

d) Categorisation and classification of the safety systems;

e) Links between the faults and their detailed analysis, which include the overall claim for the fault and the consequences.

Requirement management arrangements have been completed in UK HPR1000 Fault Schedule and Confinement Schedule.

T-12.13-1 Template of Fault Schedule

Event	Event frequency	Target state (CS, SS, FS)	Fundamental Safety Function	High Level Safety Function	Low Level Safety Function	Safety Function Requirement Code	Designation of Safety Function Requirement	Signal description	Safety system	Action mode (Automatic, Manual, Passive or Local)	I&C system	Safety category requirement	Diverse line type	Supporting Studies	Notes
						Information for Primary protection line									
						Information for Diverse Protection Line									

12.14 Limits and Conditions for Operation

In the process of safety analysis, assumptions involving different operational states and safety functions are taken into account. The future licensee shall guarantee that the reactor is operated within these assumptions. These assumptions define some LCOs that need to be taken into account in nuclear site licensing phase.

Three kinds of LCOs are derived from fault analysis:

a) Limits on normal operation states, defined by initial conditions in transient and radiological consequences analysis, including:

   1) The combination of reactor thermal power, RCP [RCS] loop highest temperature in cold leg and pressuriser pressure shall not exceed the limits specified in the Core Physical Limits Diagram of *Thermal Hydraulic Design*, Reference [15].

   2) The main operation parameters shall not exceed operation domain, which is mainly specified in T-12.4-1 and Reference [112].

   3) The core power distribution shall be managed within the assumed range in fault analysis [113] [114].

   4) The core-related parameters used in fault analysis including heat flux hot channel factor, nuclear enthalpy rise hot channel factor, axial power offset, control rod limits and rod position indication, moderator temperature coefficient and initial boron concentration shall not be breached [113] [114].

   5) Containment pressure and temperature shall be maintained within its normal operation range;

   6) Primary activity concentration shall be managed in line with the assumption adopted in source term analysis [79];

   7) Primary to secondary leakage shall be managed in line with the assumption adopted in source term analysis [79].

b) Limits on SSCs performance claimed in the transient and radiological consequences analysis

   LCOs relating to SSCs performance are transformed to functional requirements of safety systems, and are collated in the corresponding system design manuals.

   Faults analysis determines LCOs for front-line SSCs, these LCOs shall be extended to their support systems.

c) Limits on availability of SSCs, in terms of train or division numbers assumed in the transient and radiological consequences analysis.

LCOs relating to SSCs availability define the boundaries for operation design, such as preventive maintenance arrangement.

1) During corresponding system's valid states, One or more trains of the following systems or equipment shall be available, despite one train being unavailable due to a single failure:
   - ASG [EFWS]
   - VDA [ASDS]
   - RIS [SIS]
   - RBS [EBS]
   - Main feedwater isolation
   - Containment isolation
   - SG blowdown isolation
   - PTR [FPCTS]
   - EDE [AVS]
   - EBA [CSBVS]
   - DWL [SBCAVS]
2) The following SSCs shall be available:
   - Control Rod Drive Mechanism (CRDM)
   - MSIV
   - PSV
   - MSSV
   - APG transfer line

These LCOs shall be extended to the supporting systems, such as EDG, RPS, SAS, KDS, and Component Cooling Water System, Essential Service Water System, HVAC, etc.

12.15 ALARP Assessment

12.15.1 Holistic ALARP Assessment

12.15.1.1 Evolution of the HPR1000

The Hua-long Pressurised Reactor (HPR1000), developed by China General Nuclear Power Corporation (CGN), is a design evolution from the Chinese Pressurised Reactor (CPR1000), Chinese Improved Pressurised Reactor (CPR1000+) and Advanced Chinese Pressurised Reactor (ACPR1000). The design of HPR1000 incorporates feedback from continuous good practices and scheme selection after multiple discussion screening and evaluation with the defence in depth principle and the design reliability principle as the guidance. The development of HPR1000 fully makes use of and integrates advanced design ideas and achievements of nuclear power development and research in recent years. The process of continuous improvement through analysing potential improvements and then selecting reasonably practicable solutions has been followed throughout the development of the HPR1000. The full evolution of HPR1000 is presented in Reference [115]. Two of the design evolution tightly related to Fault Studies is introduced below.

First of all, the high pressure head injection is not adopted in the design of HPR1000. The maximum injection pressure of MHSI pump is lower than the set pressure of the MSSV. This design makes that the MSSV is prevented from opening during the injection of MHSI under SGTR accident. This risk of containment bypass under the condition of SG overflow is reduced and the uncontrolled release of radioactive material to the atmosphere is avoided. From ACPR1000, the automatic control logic of SG auxiliary feedwater flow control valve is added to reduce the risk of radiation release caused by the overflow of the SG under SGTR and to improve the safety of the unit. By these design evolution, overflow of affected SG under SGTR accident is successfully avoided for HPR1000.

Another design evolution is that HPR1000 incorporates passive heat removal system ASP [SPHRS] to reduce the dependence on ASG [EFWS]. The fault mitigation duration is also extended. ASP [SPHRS] enhances diversity for the ASG [EFWS] and cooling of spent fuel pool.

12.15.1.2 Compliance with RGP

The deterministic analysis in Fault Studies follows mature safety analysis method in nuclear engineering and is compliant with the IAEA safety guidance or standards identified through a process of collection, screening, and comprehensive assessment, Section 4.2 in Reference [116].

12.15.1.3 OPEX Review

OPEX has been incorporated into the deterministic safety studies through following the RGP identified in Section 12.15.1.2.

12.15.1.4 Risk Assessment

Chapter 12 provides the assessment of the effective dose received by any person arising from design basis fault sequences in terms of RPT-4. The design basis analysis is updated at the different stages of the GDA process to accurately reflect design changes and demonstrate the acceptance criteria are met.

Design basis analyses provide important insights into design and supports decision-making for the UK HPR1000 design. Design basis analysis is used to assess the safety functions provided by safety systems and identify potential design improvements to help reduce potential risk. The results of design basis analyses including core consequences and radiological consequences are the major basis for risk assessment. From the comparison between results of design basis analyses and acceptance criteria or safety criteria, potential risks could be identified.

Based on the appropriate analysis approach demonstrated in this chapter, the design basis analysis plays the following roles in the ALARP demonstration of the UK HPR1000 design:

a) Demonstrate that the UK HPR1000 meets RPT-4 following a systematic and comprehensive DBC analysis that is consistent with RGP (section 4.2 in Reference [116]);

   The identification of PIEs and determination of DBCs follows a systematic process presented in Sub-chapter 12.4. The DBC analysis from Sub-chapter 12.7 to Sub-chapter 12.9 is performed based on conservative method and assumptions. The evaluation of radiological consequences is presented in Sub-chapter 12.11.

b) Identification of improvements based on design basis analyses process and results;

   The risk assessment is conducted through the following three aspects:

   1) Fault evaluation against acceptance criteria;

   2) Dose evaluation against RPT-4;

   3) Functional adequacy of diverse protections.

All acceptance criteria specified in Sub-section 12.5.1 are met according to design basis analysis in Sub-section 12.7-12.9. The conservatism on analysis method and the margin to basic acceptance criteria contributes to ALARP in terms of fuel integrity and core cooling.

No occurrence on DNB, PCI-SSC and PCMI is demonstrated for frequent faults. In particular, design modification on “Overpower ΔT Reactor trip” signal is taken to eliminate potential PCI occurrence for *Inadvertent Opening of One SG Relief Train or of One Safety Valve,* Reference [9][117].

All infrequent faults with DNB as acceptance criteria except for *Reactor Coolant Pump Seizure (Locked Rotor)* and *Reactor Coolant Pump Shaft Break* and *Spectrum of RCCA Ejection Accident* would not lead to DNB occurrence. The two faults for which the analysis shows DNB occurrence are specifically studied. Cycle by cycle analysis could be adopted to reduce the DNB fraction [118].

ALARP is performed for all the representative faults by considering both on-site and off-site radiological consequences. All representative faults can meet BSL targets. Some of them can satisfy BSO targets. ALARP demonstration for radiological consequences (RPT-4) is based on a systematic review of design and analysis assumptions. A detailed analysis from fault mitigation to source term and dose evaluation is conducted to find potential improvements. The radiological consequence is highly dependent on the evaluation methods of source term and dose. Doses based on more realistic assumptions are assessed to support ALARP [119].

Design modifications that contribute to the reduction of radiological consequences are introduced hereafter:

a) The risk of release through main coolant line break is reduced as the main coolant line is classified to HIC.

b) Design modification of spent fuel delivery process, which introduces cask stand in the loading pit for completing the sealing process of spent fuel cask and set impact limiters along the lifting route of spent fuel cask, can ensure the integrity of spent fuel cask from dropping.

c) The risk of handling tool dropping together with the fuel assembly can be eliminated with the change from overhead crane to gantry crane.

One of the most challenging faults for radiological consequence is SGTR (one tube). SGTR leads to containment bypass and direct release to the environment. It is concluded that the design of HPR1000 regarding to preventions and protections for SGTR relies on mature techniques and is competitive compared to other PWRs after a systematic review with regard to the occurrence frequency, design evolution of HPR1000, precautions in the design and operation, fault mitigation, source term and dose evaluation. Compared to R.G.1.183, more realistic source term evaluation assumptions regarding to iodine specification and primary coolant activity are adopted.

A systematic process is adopted to demonstrate the diverse protection lines for frequent faults. To satisfy the requirements in diversity, design modifications in isolation valves, Spent fuel pool makeup by ASP [SPHRS], SBO DG and some other supporting systems are implemented (section 4.4.3 in Reference [116]). These design improvements reduce the risk in common cause failure and enhance the reliability of safety functions.

12.15.2 Specific ALARP Assessment

Risk associated with boron dilutions and inadvertent reactor pit flooding is also studied [116].

External heterogeneous dilution and inadvertent reactor pit flooding are practically eliminated [120] and prevention measures including start-up procedure of reactor coolant pumps about new implementation FC1 interlocks are designed [121]. *Boron Dilution due to Rupture of One Heat Exchanger Tube* is eliminated by increasing the pressure of the RIS side in the seal cooling heat exchanger [116]. Inherent boron dilution accompanying with LOCA accidents of given break sizes in LOOP condition is studied and the core will always remain subcritical, Reference [57].

For potential inadvertent reactor pit flooding, the occurrence frequency is lower than 1.0E-07 /ry and the consequence is limited: inadvertent flooding of reactor pit will not lead fast fracture for RPV nor risk of fuel and cladding failure. The optioneering shows that maintaining the original design is preferred option to prevent from inadvertent reactor pit flooding due to the valves' internal leakage. Hence, the risk associated with inadvertent reactor pit flooding is reduced to ALARP level [116].

12.15.3 ALARP conclusion

To conclude, in the view of fault studies, the risk from UK HPR1000 is ALARP considering that:

a) The methodology for deterministic analysis adopted in fault studies is consistent with RGP.

b) Acceptance criteria and RPT-4 are met with margins;

c) Practical design modifications are implemented to reduce risk in fuel failure and radiological consequences through the optioneering process;

d) Diversity in the design is improved through optioneering process.

12.16 Concluding Remarks

Chapter 12 is for demonstrating that the radiological consequences following design basis faults on the UK HPR1000 are within the acceptance criteria and that the risks under design basis conditions will be demonstrated as ALARP with the design evolution of UK HPR1000. This chapter provides evidence as follows:

a) All potential Initiating design basis faults are identified and fault sequences are developed which are listed in this chapter. The SSCs required to protect the plant following the faults based on the DBC list for UK HPR1000 (except for loss of support system and spurious I&C actuation) are identified and is recorded in a comprehensive Fault Schedule.

b) A suite of computer codes are identified with verification and validation evidence to justify their use in the analysis of design basis faults.

c) Detailed analysis of the design basis faults identified is undertaken using appropriate codes to confirm that the SSCs claimed in the fault schedule are sufficient to ensure that the radiological releases are limited to an acceptable level. The analyses demonstrate that the relevant acceptance criteria identified are met following identified design basis faults. Functional requirements from safety analysis are also provided.

d) The radiological analysis methodology described in this chapter demonstrates that the radiological consequences of the design basis faults identified are appropriately assessed to confirm whether the radiological acceptance criteria required in Chapter 4 are met.

e) Fault Schedule for UK HPR1000 is produced, providing an overall view of safety function related design for UK HPR1000.

f) Demonstration of diverse protection line are undertaken to prove reactor safety in case of loss of primary protections.

g) Limits and conditions for operation required to permit reactor safety are discussed.

h) Potential design changes to reduce the consequences of design basis events are identified and support ALARP assessment.

12.17 References

[1] CGN, UK HPR1000 Design Reference Report, NE15BW-X-GL-0000-000047, Rev. I, 2021.

[2] CGN, Internal Hazards Schedule Report, GHX84200051DOZJ03GN, Rev. C, 2021.

[3] CGN, External Hazards Schedule Report, GHX86000015DOZJ03GN, Rev. G, 2021.

[4] CGN, General Safety Requirements, GHX00100017DOZJ03GN, Rev. F, 2019.

[5] CGN, General Principles for Application of Laws, Regulation, Codes and Standards, GHX00100018DOZJ03GN, Rev. H, 2020.

[6] CGN, Suitability Analysis of Codes and Standards in Fault Studies, GHX00800008DRAF02GN, Rev. C, 2020.

[7] CGN, Methodology of PIEs Identification, GHX00100008DOZJ03GN, Rev. H, 2019.

[8] CGN, The Design Condition List and Acceptance Criteria, GHX00100029DOZJ04GN, Rev. J, 2020.

[9] CGN, Supporting Report on No Fuel Failure for Frequent Faults, GHX00600274DRAF02GN, Rev. E, 2021.

[10] CGN, Evaluation of Passive Single Failures, GHX00600267DRAF02GN, Rev. C, 2020.

[11] CGN, EMIT Strategy Implementation Report, GHX42EMT005DOYX45GN, Rev. A, 2020.

[12] CGN, Main Design Technical Parameters, GHX00100010DOZJ03GN, Rev. D, 2020.

[13] CGN, NSSS Operating Parameters, GHX00100003DRRG03GN, Rev. D, 2019.

[14] CGN, Decay Heat Report, GHX00100047DRAF03GN, Rev. B, 2019.

[15] CGN, Thermal Hydraulic Design, GHX00100004DRRG03GN, Rev. F, 2021.

[16] CGN, Increase in Feedwater Flow due to Feedwater System Malfunctions,

GHX00600075DRAF02GN, Rev. C, 2019.

[17] CGN, Excessive Increase in Secondary Steam Flow, GHX00600082DRAF02GN, Rev. E, 2021.

[18] CGN, Turbine Trip, GHX00600128DRAF02GN, Rev. C, 2019.

[19] CGN, Long Term Turbine Trip, GHX00600247DRAF02GN, Rev. B, 2019.

[20] CGN, Short Term LOOP of 2 Hours Duration, GHX00600028DRAF02GN, Rev. D, 2019.

[21] CGN, Loss of Normal Feedwater Flow, GHX00600071DRAF02GN, Rev. C, 2019.

[22] CGN, Long Term Loss of Normal Feedwater Flow, GHX00600138DRAF02GN, Rev. C, 2019.

[23] CGN, Loss of One RIS [SIS] Train in RHR Mode, GHX00600115DRAF02GN, Rev. C, 2019.

[24] CGN, Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump, GHX00600051DRAF02GN, Rev. C, 2019.

[25] CGN, Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition (State A), GHX00600095DRAF02GN, Rev. E, 2021.

[26] CGN, Uncontrolled Rod Cluster Control Assembly Bank Withdrawal at Power, GHX00600094DRAF02GN, Rev. D, 2021.

[27] CGN, RCCA Misalignment up to Rod Drop without Limitation, GHX00600091DRAF02GN, Rev. D, 2021.

[28] CGN, Decrease in Boron Concentration in Reactor Coolant due to malfunction of RCV [CVCS], REA [RBWMS] and TEP[CSTS], GHX00600002DRDG02GN, Rev. F, 2021.

[29] CGN, Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction, GHX00600046DRAF02GN, Rev. C, 2019.

[30] CGN, Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction, GHX00600047DRAF02GN, Rev. C, 2019.

[31] CGN, Inadvertent Opening of a Pressuriser Safety Valve (State A), GHX00600288DRAF02GN, Rev. B, 2019.

[32] CGN, Spurious Pressuriser Heater Operation, GHX00600059DRAF02GN,

Rev. D, 2019.

[33] CGN, Spurious Pressuriser Spray Operation, GHX00600060DRAF02GN, Rev. D, 2019.

[34] CGN, Loss of One PTR [FPCTS] Train (Sate A\B\C\D), GHX00600116DRAF02GN, Rev. E, 2021.

[35] CGN, Reduction in Feedwater Temperature due to Feedwater System Malfunctions, GHX00600073DRAF02GN, Rev. D, 2019.

[36] CGN, Inadvertent Closure of One or All Main Steam Isolation Valves, GHX00600089DRAF02GN, Rev. C, 2019.

[37] CGN, Medium Term LOOP of 24 Hours Duration, GHX00600030DRAF02GN, Rev. D, 2020.

[38] CGN, Forced Reduction in Reactor Coolant Flow (3 Pumps), GHX00600050DRAF02GN, Rev. C, 2019.

[39] CGN, Frequency Compliance Analysis Report, GHX05000029DEDQ45GN, Rev. B, 2020.

[40] CGN, Inadvertent Core Loading of Fuel Assemblies (State A to E), GHX00600006DRDG02GN, Rev. C, 2020.

[41] CGN, Uncontrolled Single RCCA Withdrawal, GHX00600093DRAF02GN, Rev. C, 2019.

[42] CGN, SG Tube Rupture (One Tube), GHX00600084DRAF02GN, Rev. E, 2021.

[43] CGN, Optioneering on the Reduction of SGTR Radiological Consequence, GHX00600370DRAF02GN, Rev. C, 2021.

[44] CGN, Small Break - Loss of Coolant Accident (State A), GHX00100043DRAF03GN, Rev. C, 2021.

[45] CGN, Uncontrolled RCP [RCS] Level Drop, GHX00600048DRAF02GN, Rev. D, 2021.

[46] CGN, Examination, Maintenance, Inspection and Testing (EMIT) Windows, GHX42EMT002DOYX45GN, Rev. D, 2021.

[47] CGN, LOOP (>2 hours) Affecting Fuel Pool Cooling, GHX00600029DRAF02GN, Rev. D, 2021.

[48] CGN, Criticality Analysis of Fuel Storage, GHX00600005DRDG02GN, Rev. D, 2020.

[49] CGN, Loss of One PTR [FPCTS] Train (State E\F), GHX00600118DRAF02GN, Rev. D, 2021.

[50] CGN, Isolatable Piping Failure on a System Connected to Spent Fuel Pool, GHX00600079DRAF02GN, Rev. F, 2021.

[51] CGN, Steam System Piping Large Break, GHX00600081DRAF02GN, Rev. D, 2021.

[52] CGN, Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG, GHX00600072DRAF02GN, Rev. C, 2019.

[53] CGN, Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break, GHX00600049DRAF02GN, Rev. C, 2019.

[54] CGN, Spectrum of RCCA Ejection Accidents, GHX00600092DRAF02GN, Rev. D, 2021.

[55] CGN, SG Tube Rupture (Two Tubes in One SG), GHX00600085DRAF02GN, Rev. C, 2019.

[56] CGN, Intermediate Break and up to Surge Line Break - Loss of Coolant Accident (State A\B), GHX00100042DRAF03GN, Rev. D, 2021.

[57] CGN, Inherent heterogeneous boron dilution analysis, GHX00600363DRAF02GN, Rev. A, 2020.

[58] CGN, Small Break - Loss of Coolant Accident (State B), GHX00600002DRAF02GN, Rev. C, 2019.

[59] CGN, Small Break - Loss of Coolant Accident (State C\D\E), GHX00600001DRAF02GN, Rev. C, 2019.

[60] CGN, RHR System Piping Break inside or outside Containment, GHX00600124DRAF02GN, Rev. C, 2019.

[61] CGN, Non Isolable Small Break or Isolable RIS [SIS] Break Affecting Fuel Pool Cooling, GHX00600125DRAF02GN, Rev. C, 2019.

[62] CGN, Bounding Case Selection for Diverse Protection Line Demonstration, GHX00600277DRAF02GN, Rev. F, 2021.

[63] CGN, Transient Analysis Report for Diverse Protection Line Demonstration,

GHX00600141DRAF02GN, Rev. C, 2020.

[64] CGN, ATWS by Rods Failure - Forced Reduction in Reactor Coolant Flow (3 pumps) (State A), GHX00600285DRAF02GN, Rev. B, August 2020.

[65] CGN, Small Break LOCA with Failure of Reactor Trip Sensor, GHX00600283DRAF02GN, Rev. B, August 2020.

[66] CGN, ATWS by Rods Failure - Uncontrolled Rod Cluster Control Assembly (RCCA) Bank Withdrawal at a Subcritical or Low Power Startup (State A\B\C), GHX00600291DRAF02GN, Rev. B, August 2020.

[67] CGN, RCCA Bank Withdrawal at Power with Failure of Sensor, GHX00600292DRAF02GN, Rev. C, August 2020.

[68] CGN, ATWS by Rods Failure - RCCA Bank Withdrawal at Power, GHX00600290DRAF02GN, Rev. C, August 2020.

[69] CGN, ATWS by Rods Failure -Uncontrolled Single RCCA Withdrawal, GHX00600293DRAF02GN, Rev. B, August 2020.

[70] CGN, Justification report on Boron dilution isolation valves for RCV [CVCS] malfunction mitigation, GHX00600026DRDG03GN, Rev. A, May 2020.

[71] CGN, Optioneering on PTR [FPCTS] related to the Loss of Isolation induced by CCF under Isolable Piping Break, GHX00100071DNHX03GN, Rev. C, July 2020.

[72] CGN, Isolatable Piping Failure on a System Connected to Spent Fuel Pool, GHX00600079DRAF02GN, Rev. F, June 2021.

[73] CGN, Inadvertent Closure of All Main Steam Isolation Valves with PSVs Fail to Open, GHX00600284DRAF02GN, Rev. B, August 2020.

[74] CGN, Optioneering report on Containment isolation, GHX00100069DNHX03GN, Rev. B, July 2020.

[75] CGN, Optioneering on VVP [MSS] related to the Loss of MSL Isolation induced by CCF under SGTR (one tube), GHX00100070DNHX03GN, Rev. B, July 2020.

[76] CGN, ATWS by Rods Failure - Spurious Pressuriser Heater Operation, GHX00600378DRAF02GN, Rev. A, August 2020.

[77] CGN, Primary Source Term Calculation Report, GHX00800006DRDG03GN, Rev. G, 2021.

[78] US NRC, Alternative Radiological Source Terms for Evaluating Design Basis Accidents at Nuclear Power Reactors, Regulatory Guide 1.183, 2000.

[79] CGN, Design Basis Accident Source Term Methodology Report, GHX00800002DRAF03GN, Rev. F, 2021.

[80] NEA, Containment leaktightness test for nuclear power plants, NB/T 20018, 2010.

[81] CGN, Off-site Radiological Consequences Analysis Methodology for DBC Accidents of UK HPR1000, GHX00540004DOHB00GN, Rev. A, July 2020.

[82] CGN, On-site (MCR) Radiological Consequences analysis for Representative DBC Accidents of UK HPR1000, GHX00100010DOHB00GN, Rev. C, March 2021.

[83] CGN, DBC Operator Distribution Report, GHX11101001DOYX45GN, Rev. A, 2019.

[84] CGN, Worker Dose Assessment Methodology during Accident Condition, GHX00100036DNFP03GN, Rev. E, 2021.

[85] CGN, Off-site Radiological Consequences analysis for Representative DBC Accidents of UK HPR1000, GHX00100011DOHB00GN, Rev. C, 2021.

[86] CGN, Source Term Analysis of Turbine Trip Accident, GHX00600306DRAF02GN, Rev. B, 2020.

[87] CGN, Source Term Analysis of SG Tube Rupture (SGTR) (One Tube), GHX00600012DRAF02GN, Rev. F, 2021.

[88] CGN, Source Term Analysis of Small Break - Loss of Coolant Accident, GHX00600307DRAF02GN, Rev. B, 2020.

[89] CGN, Source Term Analysis of Rupture of a Line Carrying Primary Coolant Outside Containment, GHX00600246DRAF02GN, Rev. C, 2020.

[90] CGN, Source Term Analysis of Volume Control Tank Break, GHX00600308DRAF02GN, Rev. B, 2020.

[91] CGN, Source Term Analysis of RCCA Ejection Accidents, GHX00600013DRAF02GN, Rev. E, 2020.

[92] CGN, Source Term Analysis of Steam System Piping Large Break, GHX00600011DRAF02GN, Rev. F, 2020.

[93] CGN, Source Term Analysis of Large Break - Loss of Coolant Accident, GHX00600008DRAF02GN, Rev. E, 2020.

[94] CGN, Source Term Analysis of SG Tube Rupture (SGTR) (Two Tubes in One SG), GHX00600253DRAF02GN, Rev. D, 2021.

[95] CGN, Source Term Analysis of RHR System Piping Break outside Containment, GHX00600312DRAF02GN, Rev. B, 2020.

[96] CGN, Source Term Analysis of A Locked Rotor Accident, GHX00600024DRAF02GN, Rev. E, 2020.

[97] CGN, Dropping of Fuel Assembly, GHX00600131DRAF02GN, Rev. F, 2021.

[98] CGN, Radiological Consequence Analysis of Dropping of Spent Fuel Cask, GHX00600384DRAF02GN, Rev. B, April, 2021.

[99] CGN, Analysis for Spurious I&C Actuation Events, GHX00600348DRAF02GN, Rev. B, 2020.

[100] CGN, Analysis for Loss of Support System Events, GHX00600349DRAF02GN, Rev. A, 2020.

[101] CGN, Large Break - Loss of Coolant Accident (up to double-ended break), GHX00600004DRAF02GN, Rev. D, 2021.

[102] CGN, Anticipated Transient Without Scram (ATWS) Due to Protection System (RPS [PS]) Failure (State A), GHX00600300DRAF02GN, Rev. A, November 2019.

[103] CGN, Total Loss of Cooling Chain (TLOCC) (Shutdown Condition) (States C3b and D), GHX00600120DRAF02GN, Rev. C, November 2019.

[104] CGN, Loss of Ultimate Heat Sink (LUHS) for 100 Hours (States A and B), GHX00600251DRAF02GN, Rev. C, December 2020.

[105] CGN, Overpressure Protection in Cold Shutdown State - Category 2, GHX00600139DRAF02GN, Rev. B, November 2019.

[106] CGN, Loss of Three Fuel Pool Cooling and Treatment System (PTR [FPCTS]) Trains, GHX00600250DRAF02GN, Rev. D, July 2021.

[107] CGN, LB-LOCA safety case clarification and core assessment report, GHX00600007DRRL02GN, Rev. C, 2021.

[108] CGN, Early Version of Fault Schedule, GHX82036001DRAF03GN, Rev. B,

2018.

[109] CGN, UK HPR1000 Fault Schedule, GHX00600276DRAF02GN, Rev. E, 2021.

[110] CGN, Fault Schedule Production Methodology, GHX00600172DRAF02GN, Rev. D, 2019.

[111] CGN, Confinement Schedule, GHX00600379DRAF02GN, Rev. A, 2020.

[112] CGN, Definition of Plant Normal Operating Domain, GHX11100001DOZJ45GN, Rev. B, 2018.

[113] CGN, Nuclear Design Report for first cycle, GHX00600001DRDG03TR, Rev. B, 2020.

[114] CGN, Nuclear Design Report for equilibrium cycle, GHX00600002DRDG03TR, Rev. B, 2020.

[115] CGN, HPR1000 R&D History, GHX99980001DXZJ01MD, Rev. C, 2020.

[116] CGN, ALARP Demonstration Report of Fault Studies, GHX00100055KPGB03GN, Rev. E, 2021.

[117] CGN, Resolution Report of PCI Risk for INVDA, GHX00600388DRAF02GN, Rev. B, January 2021.

[118] CGN, Supporting report on ALARP Assessment for DNB analysis, GHX00120001DRAF00GN, Rev. D, March, 2021.

[119] CGN, ALARP Assessment for DBC radiological consequence, GHX00600375DRAF02GN, Rev. B, 2021.

[120] CGN, Demonstration of the Elimination of External Heterogeneous Boron Dilution, GHX00600001DOZJ45GN, Rev. C, February 2021.

[121] CGN, Functional Requirements for Prevention and Protection against Boron Dilution, GHX11000001DOZJ45GN, Rev. D, February 2021.

[122] CGN, PINE - A Lattice Physics Code: Verification and Validation Report, GHX00600004DRDG02TR, Rev. D, November 2020.

[123] CGN, COCO - A 3-D Nuclear Design Code: Verification and Validation Report, GHX00600001DRDG02TR, Rev. D, November 2020.

[124] CGN, POPLAR - A 1-D Core Calculation Code: Verification and Validation Report, GHX00600003DRDG02TR, Rev. D, July 2020.

[125] CGN, GINKGO - A Transient System Analysis Code: Verification and Validation Report, GHX00600141DRAF02TR, Rev. D, March 2021.

[126] CGN, LINDEN - A Subchannel Analysis Code: Verification and Validation Report, GHX00600142DRAF02TR, Rev. E, January 2021.

[127] CGN, LOCUST - A Thermal-hydraulic System Analysis Code: Verification and Validation Report, GHX00600143DRAF02TR, Rev. D, March 2021.

[128] CGN, BIRCH - A Fuel Rod Temperature Analysis Code: Verification and Validation Report, GHX00600138DRAF02TR, Rev. E, May 2020.

[129] CGN, CATALPA - A Thermal-hydraulic Containment Analysis Code: Verification and Validation Report, GHX00600139DRAF02TR, Rev. B, July 2020.

[130] CGN, CAMPHOR - A Subcompartment Analysis Code: Verification and Validation Report, GHX00600167DRAF02TR, Rev. C, November 2020.

[131] CGN, PALM - A Depletion Calculation Code: Verification and Validation Report, GHX00600002DRDG02TR, Rev. D, November 2020.

[132] National Radiological Pretention Board, A methodology for assessing doses from short-term planned discharges to the atmosphere, NPRB-W54, March 2004.

Appendix 12A Computer Codes Used in the Fault Studies and Radiological Release Analysis

The computer codes used in the Fault Studies and Radiological Release Analysis are listed in T-12A-1 to T-12A-3. The brief descriptions of computer codes used are provided.

T-12A-1 Computer Codes Used in Chapter 12

Analyses of DBC-2 Events

Sub-chapter	DBC Faults	Computer codes for fault analysis
12.7.1.1	Increase in Feedwater Flow due to Feedwater System Malfunctions (Sate A\B)	GINKGO LINDEN
12.7.1.2	Excessive Increase in Secondary Steam Flow (State A\B)	GINKGO LINDEN
12.7.1.3	Inadvertent Opening of a SG Relief Train or of a Safety Valve (State A\B)	---
12.7.2.1	Turbine Trip (State A\B)	GINKGO LINDEN
12.7.2.2	Short Term LOOP of 2 Hours Duration (Sate A\B\C\D\E\F)	GINKGO LINDEN
12.7.2.3	Loss of Normal Feedwater Flow (Sate A\B)	GINKGO LINDEN
12.7.2.4	Spurious reactor trip (Sate A\B\C)	---
12.7.2.5	Loss of One RIS [SIS] Train in RHR Mode (State C\D\E) (State C\D\E)	---
12.7.3.1	Partial Loss of Core Coolant Flow due to Loss of One Reactor Coolant Pump (Sate A\B\C)	GINKGO LINDEN
12.7.4.1	Uncontrolled RCCA Bank Withdrawal at a Subcritical or Low Power Startup Condition (State A\B\C)	COCO POPLAR GINKGO LINDEN BIRCH
12.7.4.2	Uncontrolled RCCA Bank Withdrawal at Power (State A)	GINKGO LINDEN
12.7.4.3	RCCA Misalignment up to Rod Drop (State A)	COCO POPLAR GINKGO LINDEN

Sub-chapter	DBC Faults	Computer codes for fault analysis
12.7.4.4	Startup of an Inactive Reactor Coolant Pump at an Improper Temperature (Sate C\D\E)	---
12.7.4.5	Decrease in Boron Concentration in Reactor Coolant due to Malfunction of RCV [CVCS], REA [RBWMS] and TEP[CSTS]	COCO LINDEN
12.7.5.1	Increase in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sate A\B\C\D\E)	GINKGO LINDEN
12.7.6.1	Decrease in RCP [RCS] Inventory due to RCV [CVCS] Malfunction (Sate A\B)	GINKGO LINDEN
12.7.6.2	Inadvertent Opening of a Pressuriser Safety Valve (State A)	GINKGO LINDEN
12.7.7.1	Spurious Pressuriser Heater Operation (Sate A\B\C)	GINKGO LINDEN
12.7.7.2	Spurious Pressuriser Spray Operation (Sate A\B\C)	GINKGO LINDEN
12.7.8.1	Loss of One PTR [FPCTS] Train (Sate A\B\C\D)	---
12.7.9.1	Loss of RRI [CCWS] or SEC [ESWS] Train A (State A\B)	---

T-12A-2 Computer Codes Used in Chapter 12

Analyses of DBC-3 Events

Sub-chapter	DBC Faults	Computer codes for fault analysis
12.8.1.1	Reduction in Feedwater Temperature due to Feedwater System Malfunctions (State A\B)	GINKGO LINDEN
12.8.1.2	Steam System Piping Small Break Including Breaks in Connecting Lines (State A\B)	---
12.8.2.1	Inadvertent Closure of One or All Main Steam Isolation Valves (State A\B)	GINKGO LINDEN
12.8.2.2	Medium Term LOOP of 24 Hours Duration (State A to F)	LOCUST
12.8.2.3	Feedwater System Piping Small Break Including Breaks in Connecting Lines to SG (State A\B)	---
12.8.3.1	Forced Reduction in Reactor Coolant Flow (3 Pumps) (State A\B\C)	GINKGO LINDEN
12.8.4.1	Inadvertent Core Loading of Fuel Assemblies (State A\B\C\D\E)	COCO
12.8.4.2	Uncontrolled Single RCCA Withdrawal (State A\B\C)	COCO POPLAR GINKGO LINDEN BIRCH
12.8.5.1	Rupture of a Line Carrying Primary Coolant outside Containment (State A\B\C\D\E)	---
12.8.5.2	SG Tube Rupture (one tube) (State A\B\C)	LOCUST
12.8.5.3	Small Break - Loss of Coolant Accident (State A)	LOCUST LINDEN
12.8.5.4	Uncontrolled RCP [RCS] Level Drop (State C\D\E)	---
12.8.5.5	Inadvertent Opening of one Pressuriser Safety Valve (State B\C)	---
12.8.6.1	LOOP (>2 hours) Affecting Fuel Pool Cooling (State A to F)	---
12.8.6.2	Loss of One PTR [FPCTS] Train (State E\F)	---
12.8.6.3	Isolatable Piping Failure on a System Connected to Spent Fuel Pool (State A to F)	---
12.8.7.1	Volume Control Tank break	---
12.8.8.1	Loss of DVL [EDSBVS] Ventilation in Switchgear	---

Sub-chapter	DBC Faults	Computer codes for fault analysis
	and I&C Cabinets Rooms of Safeguard Building Division B (State A\B)	
12.8.8.2	Loss of RRI [CCWS] or SEC [ESWS] Train A (State C\D\E)	---

T-12A-3 Computer Codes Used in Chapter 12

Analyses of DBC-4 Events

Sub-chapter	DBC Faults	Computer codes for fault analysis
12.9.1.1	Steam System Piping Large Break (State A\B)	COCO GINKGO LINDEN
12.9.2.1	Feedwater System Piping Large Break Including Breaks in Connecting Lines to SG (State A\B)	LOCUST
12.9.2.2	Long Term LOOP of 168 Hours Duration (State A to F)	---
12.9.3.1	Reactor Coolant Pump Seizure (Locked Rotor) or Reactor Coolant Pump Shaft Break (State A\B\C)	GINKGO LINDEN BIRCH
12.9.4.1	Spectrum of RCCA Ejection Accidents (State A\B)	COCO LINDEN BIRCH
12.9.5.1	SG Tube Rupture (Two Tubes in One SG) (State A\B\C)	LOCUST
12.9.5.2	Intermediate Break and up to Surge Line Break - Loss of Coolant Accident (State A\B)	LOCUST
12.9.5.3	Small Break - Loss of Coolant Accident (State B)	LOCUST
12.9.5.4	Small Break - Loss of Coolant Accident (State C\D\E)	LOCUST
12.9.5.5	RHR System Piping Break inside or outside Containment (State C\D\E)	LOCUST
12.9.5.6	Inadvertent Opening of Severe Accident Dedicated Valves (One Train) (State A\B\C)	---
12.9.6.1	Dropping of fuel assembly (State A to F)	---
12.9.6.2	Dropping of Spent Fuel Cask (State A to F)	---
12.9.7.1	Non Isolable Small Break or Isolable RIS [SIS] Break Affecting Fuel Pool Cooling (State E)	---
12.9.8.1	Loss of DVL [EDSBVS] Ventilation in Switchgear and I&C Cabinets Rooms of Safeguard Building Division B (State C)	---

a) PCM

PCM is a nuclear design code package that contains PINE and COCO. PINE is an advanced Pressurized Water Reactor (PWR) fuel assembly calculation code, and COCO is a three-dimensional (3-D) core calculation code. PINE generates two-group parameter tables for macroscopic cross-sections and the assembly discontinuity factors, which COCO uses to calculate these parameters.

1) PINE

PINE [122] performs 2-D lattice calculation for single assembly and multiple assemblies of PWR and generates two-group parameter tables. The parameters include diffusion coefficients, macroscopic cross-section, surface dependent discontinuity factors, xenon and samarium microscopic densities, flux shape factor for power reconstruction and kinetic parameters.

PINE uses multi-group cross section databank of IAEA WIMS-D update program.

The physical models of PINE include resonance calculation, transport calculation, leakage correction and burn-up calculation.

The equivalence principle is applied to carry out resonance calculation. The Method of Characteristics (MOC) is applied to perform two-dimensional heterogeneous transport calculation. B1 approximation is applied to take into account the leakage effect. PINE uses two different advanced burn-up calculation strategies, which are Linear Rate (LR) method and Log Linear Rate (LLR) method.

2) COCO

COCO [123] is used for PWR nuclear reactor design. The main functions include loading pattern design, critical boron concentration search, evolution calculation, control rod worth assessment, reactivity coefficients calculation, shutdown margin calculation, etc. COCO is also used to perform transient calculations such as Reactivity Induced Accidents (RIA).

The solver of COCO is based on Nodal Expansion Method (NEM) which can handle 2-D and 3-D geometries. The NEM solver can provide flux distribution in full core and 1/4 core geometries. Furthermore, the NEM solver is accelerated using CMFD method.

The feedback of COCO includes a closed-channel thermal-hydraulic model, which is responsible for moderator temperature and density, and a fuel temperature calculation model.

Both microscopic and macroscopic burn-up models are developed. The former focuses on the fission products, minor actinides, etc. The latter handles the intra-node burn-up distribution. In macroscopic burn-up, nodal surface burn-up is calculated to correct cross-sections.

The PCM nuclear design code package has been intensively validated against Nuclear Power Plant (NPP) data, experimental data and benchmarks.

b) POPLAR

POPLAR [124] is a 1-D neutron diffusion-depletion code. POPLAR is used to perform bite calculation, calibration calculation, xenon depletion calculation, transient xenon calculation, control rod worth calculation and control rod cross section modification. Furthermore, POPLAR is used for transient calculation.

POPLAR obtains relevant input of the core from COCO, and the tables of few-group parameters from PINE.

The physical models of POPLAR include cross section interpolation, 3-D to 1-D conversion, two-group 1-D diffusion solver, leakage correction, thermal feedback and 1-D control rod insertion.

The validation of the POPLAR includes NPP data validation.

c) GINKGO

GINKGO [125] is a system transient analysis code, which is used to analyse PWR transients under normal operating conditions and accident conditions. For these transients, GINKGO simulates the reactor vessel and core, hot and cold legs, pressuriser, steam generator, reactor coolant pump in PWR plant. The modelling of Nuclear Steam Supply System (NSSS), Engineered Safety System (ESS), Reactor Protection System (RPS), Instrumentation and Control System (I&C) and secondary system components are also taken into account.

To account for the thermal-hydraulics features of the coolant in different transients, the separated phase model at thermal equilibrium is used in the code. Three governing mixture balance equations combined with a drift-flux model are applied. A reactor point kinetic model with six-group delayed neutron and a simplified decay heat model are combined to predict the core transients.

The validation of GINKGO includes separate effect validation and integral effect validation.

d) LINDEN

LINDEN [126] is a sub-channel analysis code which is used for thermal-hydraulic design and safety analysis of reactor core. It calculates the thermal-hydraulic parameters of coolant in reactor core under various conditions, such as pressure, mass

velocity, quality and void fraction, etc. Based on the calculated thermal-hydraulic parameters, the Departure from Nucleate Boiling (DNB) of reactor core can be predicted by using a specific Critical Heat Flux (CHF) correlation.

The flow model in LINDEN is a four-equation model combined with a drift-flux correlation, which takes into account the slip velocity between liquid and vapour phases under two-phase flow. The four-equation model includes a mixture mass equation, a mixture energy equation, a mixture momentum equation and a liquid energy equation. Among them, the liquid energy equation is used to simulate the thermal non-equilibrium of liquid phase during sub-cooled boiling.

The code has been validated using experimental data, including single channel experiments and rod bundle experiments.

e) LOCUST

LOCUST [127] is a system thermal-hydraulic code which has the capability of performing LOCA analysis. It focuses on the analysis of LB-LOCA, IB/SBLOCA, SGTR and DEC-A.

LOCUST is used to simulate two-fluid, non-equilibrium, and heterogeneous hydrodynamic conditions in various NPP transients. A six-equation model is employed in hydrodynamics model, which forms the trunk of LOCUST. Auxiliary models include heat structure model, trip system, control system, and point reactor kinetics model.

The most important features of LOCUST are flexible nodalization, capability to analyse two-fluid, thermal non-equilibrium in all fluid volumes. The code is incorporated with models to simulate special processes such as choked flow, thermal stratification, and counter-current flooding limitations.

The validation of LOCUST includes phenomenological validation, separate effect validation and integral effect validation.

f) BIRCH

BIRCH [128] is a fuel rod temperature analysis code, mainly used to analyse the integrity of fuel rod in PWR under accident conditions. BIRCH calculates the radial temperature distribution of a fuel rod and the heat flux of cladding surface during transient conditions. In addition, it also calculates energy storage in the fuel pellet, gap heat transfer coefficient and thermal expansion of pellet and cladding, etc.

A 1-D heat conduction differential equation is implemented in heat conduction model together with other physical models, including cladding-coolant heat transfer model, gap conductance model, Zircaloy-water reaction model and fuel pellet melting model, etc.

The physical properties of coolant and data of evolution of nuclear power required in

the calculation are obtained from the system transient analysis code GINKGO or 3-D core calculation code COCO.

The validation of BIRCH includes analytical solution verification, constitute relation validation and fuel rod temperature validation.

g) CATALPA

CATALPA [129] is a containment analysis code. It is used to simulate the transient change of pressure and temperature inside PWR containment under the accidents with the release of high-energy fluid into containment, such as Loss of Coolant Accident (LOCA) and Steam Line Break Accident (SLB).

The basic model of the code is a single-volume model. The substances inside the containment are divided into two systems: a gas phase system and a liquid phase system, and the air contained in containment are assumed to be ideal gas. The mass, energy and volume conservation laws are used to build the conservation equations of these two systems. In addition, steam condensation, heat conduction of structural components and heat transfer on containment wall are also considered in the code.

The code has been validated using experimental data, including separate effect experiments and integral effect experiments.

h) CAMPHOR

CAMPHOR [130] is a sub-compartment analysis code. It is used for pressure and temperature calculation inside compartments under the accidents with high energy pipe failure.

A quasi-steady-state approximation is used to represent accident transients. Besides, air, steam and water in compartments are assumed to be in thermal equilibrium in each compartment. In addition, steam condensation, heat conduction of structural components and heat transfer through walls are also considered in the code.

The code has been validated using experimental data, including some separate effect experiments and integral effect experiments.

i) PALM

PALM [131] is a point-depletion and radioactivity-decay calculation code. PALM is capable of calculating the nuclide number density, decay heat, neutron emission rates and photon emission rates of given material. The result can be used in safety analysis and radioactivity shielding design.

PALM uses the cross-section, decay constant, fission product yield and decay photon emission data from JEFF3.3.

Neutron reaction data include neutron reaction cross sections of 562 isotopes and the fission products of 19 fission nuclei. Decay data include decay constants and the

fractions of each decay mode of 3852 isotopes. A set of burn-up dependent neutron spectrums is used to reduce the number of groups of cross-sections from 361 to 1. The burn-up equations are then built and solved by matrix exponent method.

j) Atmospheric Dispersion Modelling System (ADMS)

ADMS 5 [132] is a practical, short-range dispersion model that simulates a wide range of buoyant and passive releases to atmosphere. It is used to simulate atmospheric diffusion. It is also capable of calculating the cloud gamma dose rate.

User guidance

The user guidance report system includes code user manuals, reference deck, calculation notes and methodology reports. The contents of these reports are summarised as follows,

a) User manual: the report introduces the code assumption and limitation, operation environment and method, input deck format, the physical meaning of each variable and the output data.

b) Reference deck: the reference deck presents a reference input deck for UK HPR1000 design, providing references for the subsequent accident analysis.

c) Calculation notes: the calculation notes include accident analysis notes and the V&V notes, which record the process of the accident analysis for each calculation step, as well as code V&V in details.

d) Methodology reports: these reports introduce the principles of accident analysis, use of the codes, general design input and specific analysis methods. They will provide guidance for users to carry out accident analysis correctly and conservatively.

Appendix 12B Limiting Conditions for Sizing

Limiting conditions for system sizing is summarized in T-12B-1.

T-12B-1 Limiting Conditions for System/Equipment Sizing

No.	Safety System/Equipment	Performance Parameters	Limiting Conditions
1	MHSI	MHSI pump maximum discharge head	SGTR (1 tube)
2	MHSI	Minimum flowrate (with large miniflow pipeline closed)	SB-LOCA(State A)
3	MHSI	Minimum flowrate (with large miniflow pipeline open)	SB-LOCA(State A)
4	MHSI	Maximum flowrate (with large miniflow pipeline closed)	1) Overpressure Protection in Cold Shutdown State - Category 4; 2) SGTR (1 tube)
5	MHSI	Maximum flowrate (with large miniflow pipeline open)	1) Overpressure Protection in Cold Shutdown State - Category 3; 2) Overpressure Protection in Cold Shutdown State - Category 4
6	LHSI	Minimum flowrate of LHSI in cold leg	LB-LOCA (State A)
7	LHSI	Minimum flowrate of LHSI in hot leg	P&T limit requirements of LOCA (State A)

No.	Safety System/Equipment	Performance Parameters	Limiting Conditions
8	LHSI (RHR)	Closure time of isolation valve of RIS/RHR train	P&T requirements of RHR System Piping Break inside or outside Containment
9	RHR safety valve	Setpoint and minimum flowrate	Overpressure Protection in Cold Shutdown State - Category 2
10	ACCU	Total volume, available water volume, pressure, temperature and discharge line resistance coefficient	LB-LOCA (State A)
11	PSV	Setpoint and minimum flowrate	1) Primary Side Overpressure Analysis - Category 3; 2) Primary Side Overpressure Analysis - Category 4

No.	Safety System/Equipment	Performance Parameters	Limiting Conditions
12	PSV	Setpoint and minimum flowrate	1) Overpressure Protection in Cold Shutdown State - Category 3; 2) Overpressure Protection in Cold Shutdown State - Category 4
13	PSV	Minimum and maximum primary depressurization rate	FLB (with LOOP and the single failure of one EDG train failed corresponding to the unaffected loop)
14	MSSV	Setpoint and minimum flowrate	1) Secondary Side Overpressure Analysis - Category 3 2) Secondary Side Overpressure Analysis - Category 4
15	VDA [ASDS]	Setpoint and minimum flowrate	Secondary Side Overpressure Analysis - Category 2

No.	Safety System/Equipment	Performance Parameters	Limiting Conditions
16	ASG [EFWS]	Minimum flowrate	FLB (with LOOP and the single failure of one ASG train failed corresponding to one unaffected SG)
17	ASG [EFWS]	Maximum flowrate	Containment pressure and temperature analysis of MSLB (with single failure of failure to close the MSIV)
18	ASG [EFWS]	ASG [EFWS] water tank inventory	Remove the residual heat in hot shutdown state for 24h; FLB
19	ASG [EFWS]	ASG [EFWS] water tank temperature	Refer to Chinese NPP operating experience
20	RBS [EBS]	Minimum volume of boric acid tank	The minimum volume of one emergency boric acid tank should meet the requirement of bring the plant from the controlled state to the safe state

No.	Safety System/Equipment	Performance Parameters	Limiting Conditions
21	RBS [EBS]	Minimum flowrate	During the process from hot shutdown to safe shutdown for DBC events, with one RBS [EBS] train injection in the minimum flowrate, it should be ensured that the insertion of positive reactivity can be compensated
22	RBS [EBS]	Maximum flowrate	Under DBC events, when RBS [EBS] is used for boron injection in the maximum flowrate and the discharge function of the RCV [CVCS] is not considered, it should be ensured that the pressuriser will not overflow.
23	ASP [SPHRS]	ASP [SPHRS] heat exchanger capacity	1) TLOCC with loss of secondary cooling (failure of ASG [EFWS] or VDA [ASDS]) (State A); (DEC-A) 2) TLOFW (DEC-A)
24	ASP [SPHRS]	ASP [SPHRS] water tank inventory	1) TLOCC with loss of secondary cooling (failure of ASG [EFWS] or VDA [ASDS]) (State A); (DEC-A) 3) LUHS for 100 hours (States A and B); (DEC-A) 4) Loss of three PTR [FPCTS] trains (DEC-A)