Form10/00

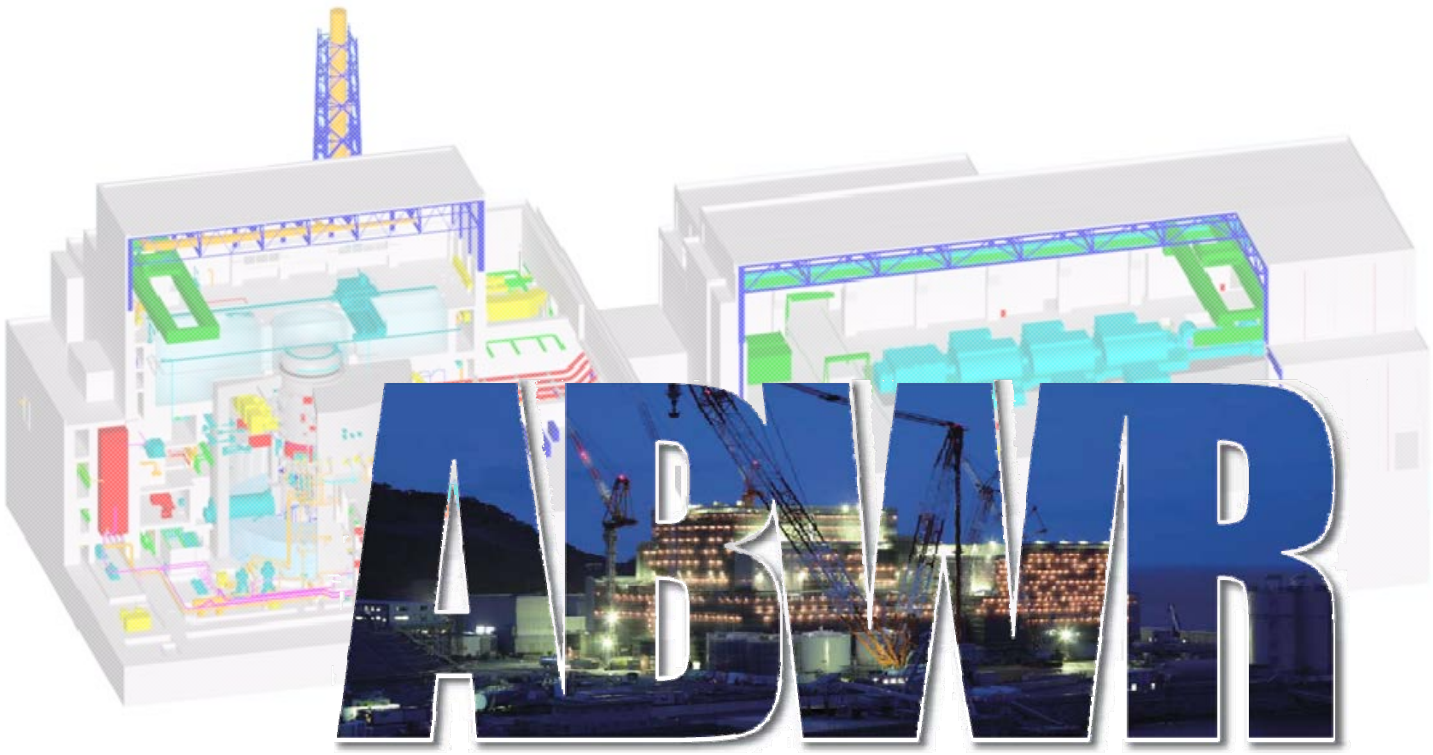
HITACHI

UK ABWR

Document ID	:	GA91-9901-0038-00001
Document Number	:	XE-GD-0149
Revision Number	:	B

UK ABWR Generic Design Assessment

Preliminary Safety Report on Mechanical Engineering



Hitachi-GE Nuclear Energy, Ltd.

DISCLAIMERS

Proprietary Information

This document contains proprietary information of Hitachi-GE Nuclear Energy, Ltd. (Hitachi-GE), its suppliers and subcontractors. This document and the information it contains shall not, in whole or in part, be used for any purpose other than for the Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR. This notice shall be included on any complete or partial reproduction of this document or the information it contains.

Copyright

Table of Contents

Abbreviations and Acronyms List

ABWR	Advanced Boiling Water Reactor
AC	Atmospheric Control System
AD/G	Alternative Emergency Diesel Generator System
ADS	Automatic Depressurisation System
AHEF	Alternate Heat Exchange Facility
ALARP	As Low as Reasonably Practicable
ARI	Alternative Rod Insertion
AS	Turbine Auxiliary Steam System
ATWS	Anticipated Transient Without Scram System
B/B	Backup Building
BOP	Balance of Plant
BS	British Standard
BSL	Basic Safety Limit
CAE	Claim, Argument and Evidence
C/B	Control Building
CCI	Commercial Confidentiality Information
CD	Condensate Demineralizer
CF	Condensate Filter Facility
CFDW	Condensate and Feedwater System
C&I	Control and Instrumentation
CR	Control Rod
CRD	Control Rod Drive System
CUW	Reactor Water Clean-up System
CW	Circulating Water System
D/G	Emergency Power Supply System
DSA	Deterministic Safety Analysis
DW	Domestic Water System
DWC	Drywell Cooling System
ECCS	Emergency Core Cooling System
EMIT	Examination, Maintenance, Inspection and Test
ES	Extraction Steam System
FCS	Flammability Control System

FCVS	Filtered Containment Venting System
FDW	Feedwater System
FHM	Fuel Handling Machine
FLSR	Flooding System of Reactor Building
FLSS	Flooding System of Specific Safety Facility
FMCRD	Fine Motion Control Rod Drive
FPC	Fuel Pool Cooling Clean-up System
GDA	Generic Design Assessment
GEN	Generator
HCU	Hydraulic Control Unit
HD	Feedwater Heater Drain System
HGNE	Hitachi-GE Nuclear Energy, Ltd.
HNCW	HVAC Normal Cooling Water System
HPCF	High Pressure Core Flooder System
HPIN	High Pressure Nitrogen Gas Supply System
HS/HSCR	Heating Steam System and Heating Steam Condensate Water Return System
HSE	Health and Safety Executive
HV	Feedwater Heater Vent System
HVAC	Heating Ventilating and Air Conditioning System
Hx/B	Heat Exchanger Building
IA	Instrument Air System
IAEA	International Atomic Energy Agency
ISO	International Organization for Standardization
LDF	Lower Drywell Flooder System
LLRC	Lower Level Reliability Claim
LOCA	Loss of Coolant Accident
LOOP	Loss of Offsite Power
LPFL	Low Pressure Core Flooder System
MCR	Main Control Room
ME	Mechanical Engineering
MS	Turbine Main Steam System
MSIV	Main Steam Isolation Valve
MSQA	Management of Safety and Quality Assurance
MSV	Main Stop Valve

MUWC	Makeup Water Condensate System
NB	Nuclear Boiler System
OG	Off-Gas System
ONR	Office for Nuclear Regulation's
PC	Performance Claim
PCV	Primary Containment Vessel
pfd	Probability of Failure on Demand (per reactor-year)
PI	Personal Information
P&ID	Piping and Instrumentation Diagram
PSA	Probabilistic Safety Assessment
R/B	Reactor Building
RC	Reliability Claim
RCIC	Reactor Core Isolation Cooling System
RC&IS	Rod Control and Information System
RCPB	Reactor Coolant Pressure Boundary
RCW	Reactor Building Cooling Water System
RD	Radioactive Drain Transfer System
RHR	Residual Heat Removal System
RI	Regulatory Issue
RIP	Reactor Internal Pump
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RRS	Reactor Recirculation System
RSW	Reactor Building Service Water System
RW/B	Radwaste Building
SA	Service Air System
SAP	Safety Assessment Principles for Nuclear Facilities
S/B	Service Building
SDC	Reactor Shutdown Cooling Mode
SFC	Safety Functional Claim
SFP	Spent Fuel Pool
SGTS	Standby Gas Treatment System
SI	Statutory Instrument
SLC	Standby Liquid Control System

S/P	Suppression Pool
SPCU	Suppression Pool Clean-up System
SPD	Suppression Pool Water Drainage System
SRV	Safety Relief Valve
SSCs	Structures, Systems and Components
TAGs	Technical Assessment Guides
T/B	Turbine Building
TBP	Turbine Bypass System
TCW	Turbine Building Cooling Water System
TGS	Turbine Gland Steam System
TSW	Turbine Building Service Water System
WENRA	Western European Nuclear Regulators' Association

List of Tables

List of Figures

1. Objective

The Preliminary Safety Report on Mechanical Engineering presents an overview on the UK ABWR safety case from the Mechanical Engineering perspective within the Generic Design Assessment (GDA) process based on the strategy determined with the Regulators during Step 1.

2. Background

2.1. Hitachi-GE's Experience

Since the introduction to Japan of the boiling water reactor technology by General Electric in the 1960s, Hitachi has participated in the design, development and construction of over 20 nuclear power plants within Japan.

Today, Hitachi-GE has participated in the construction of all 4 operating ABWRs in Japan with responsibilities ranging from the complete plant (Shika-2), the nuclear island (Kashiwazaki-Kariwa-7) or the turbine island (Kashiwazaki-Kariwa-6, Hamaoka-5). Hitachi-GE are involved in the on-going construction of the Shimane 3 and Ohma-1 ABWRs in Japan.

For further details on Hitachi-GE's experience refer to Step 1 C2a document "Genesis of ABWR design" [Ref-8].

2.2. Reference Design

The design of the mechanical Structures, Systems and Components (SSCs) of UK ABWR derives from the generic design of Japanese ABWR. The standard design of the first ABWR (units 6 and 7 of Kashiwazaki-Kariwa Nuclear Power Plant) together with further optimisation from subsequent ABWR plants and operational experience will be the reference design for mechanical SSCs of the UK ABWR.

Additionally, the UK ABWR will incorporate new mechanical SSCs to deliver a higher level of protection against severe external hazards beyond the design basis as described in this document. This basically includes post-Fukushima countermeasures from the lessons learned.

Furthermore, it is expected that the UK ABWR design will incorporate any additional changes to deal specifically with UK requirements and expectations.

3. Scope of Mechanical Engineering

3.1. Definition of Mechanical SSCs

The scope of UK ABWR mechanical engineering safety case covers SSCs generally containing dynamic elements and in some cases a number of static elements.

Mechanical engineering scope should be distinguished from Structural Integrity discipline, which covers static SSCs associated with the confinement safety function (reactor pressure vessel and boundary elements).

Examples of representative dynamic SSCs scope of mechanical engineering are as follows:

Table 3.1-1 Example of Dynamic Mechanical SSCs

Example of Dynamic Mechanical SSCs
- Fine Motion Control Rod Drive Mechanisms
- Pumps (Reactor Internal Pumps, RHR Pumps, RCW Pumps, etc.)
- Valves (Safety Relief Valves, isolation valves, check valves, motor operated valves, etc.)
- Cranes and mechanical handling systems (Fuel Handling Machine, R/B Overhead Crane, etc.)
- Nuclear ventilation systems used to maintain nuclear containment barriers (Standby Gas Treatment System, etc.)
- Heating Ventilation and Air Conditioning Systems (HVAC, etc.)
- Diesel generators (Emergency diesel generators, etc.)
- Cooling and injection systems (ECCS, etc.)

Examples of representative static SSCs scope of mechanical engineering are as follows:

Table 3.1-2 Example of Static Mechanical SSCs

Example of Static Mechanical SSCs
- Heat exchangers
- Strainers
- Filters
- Gloveboxes, cabinets
- Stillages
- Doors, hatches and seals

3.2. ABWR Mechanical Systems

3.2.1. Functions of ABWR Mechanical Systems

Mechanical engineering covers a wide range of systems which deliver one or several of the basic functions indicated below:

(1) IAEA Main Safety Functions to Ensure Nuclear Safety

To ensure nuclear safety, these following three safety functions must be maintained during normal operation and fault conditions:

1. Reactivity Control
2. Cooling/Heat Removal
3. Confinement

(2) Auxiliary Functions

They deliver power supply, cooling water supply, air supply, heating and ventilating, etc. to support the delivery of the rest of functions (1), (3) and (4) during normal operation and fault conditions.

(3) Environmentally Important Functions

Functions to monitor, control and limit the release of radioactive material in the liquid or airborne emissions during normal operation.

(4) Power Generation

Functions required for plant power generation during normal operation such as main steam transfer from the reactor to the turbine, steam condensation and feedwater transfer from the turbine to the reactor, etc.

Mechanical systems can be found in most of the facilities of the nuclear power plant covering the Reactor Building (R/B), the Turbine Building (T/B), the Radioactive Waste Building (RW/B), the Control Building (C/B), the Heat Exchanger Building (Hx/B), the Cooling Water Structure, the Backup Building (B/B) and the Service Building (S/B).

3.2.2. List of ABWR Mechanical Systems

The UK ABWR mechanical systems relevant for the safety case are classified as follows.

1 Reactor Coolant System, Reactivity Control System and Associated Systems
- 1.1 Reactor Coolant System
  - 1.1.1 Nuclear Boiler System (NB)
    - 1.1.1.1 Feedwater System (FDW)
    - 1.1.1.2 Main Steam System
  - 1.1.2 Reactor Recirculation System (RRS)
- 1.2 Reactivity Control
  - 1.2.1 Control Rod Drive System (CRD)
  - 1.2.2 Standby Liquid Control System (SLC)
- 1.3 Associated Systems
  - 1.3.1 Reactor Water Clean-up System (CUW)
  - 1.3.2 Residual Heat Removal System (RHR)
  - 1.3.3 Reactor Core Isolation Cooling System (RCIC)

2 Engineered Safety Features
- 2.1 Containment System
  - 2.1.1 Primary Containment System
    - 2.1.1.1 Containment Heat Removal System (Residual Heat Removal System (RHR))
    - 2.1.1.2 Combustible Gas Control in Containment Systems (Flammability Control System (FCS), Atmospheric Control System (AC))
  - 2.1.2 Secondary Containment System
    - 2.1.2.1 Standby Gas Treatment System (SGTS)
- 2.2 Emergency Core Cooling Systems
  - 2.2.1 High Pressure Core Flooder System (HPCF)
  - 2.2.2 Reactor Core Isolation Cooling System (RCIC)
  - 2.2.3 Low Pressure Core Flooder System (LPFL)
  - 2.2.4 Automatic Depressurisation System (ADS)

3 Auxiliary Systems

3.1 Water Systems

3.1.1 Reactor Building Service and Cooling Water Systems
(Reactor Building Service Water System (RSW), Reactor Building Cooling Water System (RCW))

3.1.2 Turbine Building Service and Cooling Water Systems
(Turbine Building Service Water System (TSW), Turbine Building Cooling Water System (TCW))

3.1.3 Makeup Water System
(Makeup Water Condensate System (MUWC))

3.2 Process Auxiliary Systems

3.2.1 Compressed Air System
(Instrument Air System (IA), Service Air System (SA), High Pressure Nitrogen Gas Supply System (HPIN))

3.2.2 Drain System
(Radioactive Drain Transfer System (RD))

3.2.3 Steam Supply System
(Heating Steam System and Heating Steam Condensate Water Return System (HS/HSCR))

3.3 Heating, Ventilation and Air Conditioning Systems (HVAC)

3.4 Other Auxiliary Systems

3.4.1 Emergency Power Supply System

3.4.2 Suppression Pool Clean-up System (SPCU)

3.5 Severe Accident Management Systems

3.5.1 Flooder System

3.5.1.1 Flooding System of Specific Safety Facility (FLSS)

3.5.1.2 Flooding System of Reactor Building (FLSR)

3.5.1.3 Lower Drywell Flooder System (LDF)

3.5.2 Filtered Containment Venting System (FCVS)

3.5.3 Alternate Heat Exchange Facility (AHEF)

3.5.4 Alternative Emergency Power Supply System

4 Steam and Power Conversion System
- 4.1 Main Turbine
- 4.2 Generator (GEN)
- 4.3 Turbine Main Steam System (MS)
- 4.4 Extraction Steam System (ES)
- 4.5 Turbine Gland Steam System (TGS)
- 4.6 Feedwater Heater Drain and Vent System (HD HV)
- 4.7 Condenser
- 4.8 Circulating Water System (CW)
- 4.9 Condensate and Feedwater System (CFDW)
- 4.10 Condensate Purification System

5 Radioactive Waste Management
- 5.1 Liquid Waste Treatment System
- 5.2 Off-Gas System (OG)
- 5.3 Solid Waste Treatment System

6 Fuel Storage and Handling
- 6.1 Fuel Handling
  - 6.1.1 Fuel Handling Machine (FHM) related Systems
  - 6.1.2 R/B Overhead Crane Systems
- 6.2 Spent Fuel Pool, Spent Fuel Pool Cooling, Clean-up and Makeup Systems

3.3. Interfacing Disciplines with Mechanical Engineering

Mechanical engineering interacts with several other technical areas important for the whole safety case. The principal technical areas which are expected to interact with mechanical engineering throughout the GDA process are listed below.

(1) Fault Studies and Probabilistic Safety Assessment [Ref.11]
(2) Structural Integrity [Ref.12]
(3) Management of Safety and Quality Assurance (MSQA) [Ref.9]
(4) Generic Site Envelope & External Hazards [Ref.13], [Ref.14]
(5) Internal Hazards [Ref.15]
(6) Civil Engineering [Ref.14]
(7) Control and Instrumentation (C&I) [Ref.16]
(8) Electrical Engineering [Ref.17]
(9) Turbine Hall
(10) Human Factors
(11) Fuel and Core Design [Ref.18]
(12) Reactor Chemistry [Ref.19]
(13) Radioactive Waste [Ref.20]
(14) Decommissioning [Ref.21]
(15) Radiological Protection [Ref.22], [Ref.23]
(16) Environment

4. Overview of Mechanical Engineering Safety Case

4.1. Introduction

UK ABWR mechanical engineering safety case is a top down process where first safety claims are put on the SSCs which ensure safety. Secondly, in order to achieve those claims the SSCs are designed, and the way they are designed becomes the arguments to support the claims. Lastly, the achievement of the safety claims and adequacy of the design is demonstrated with evidence substantiating the safety case.

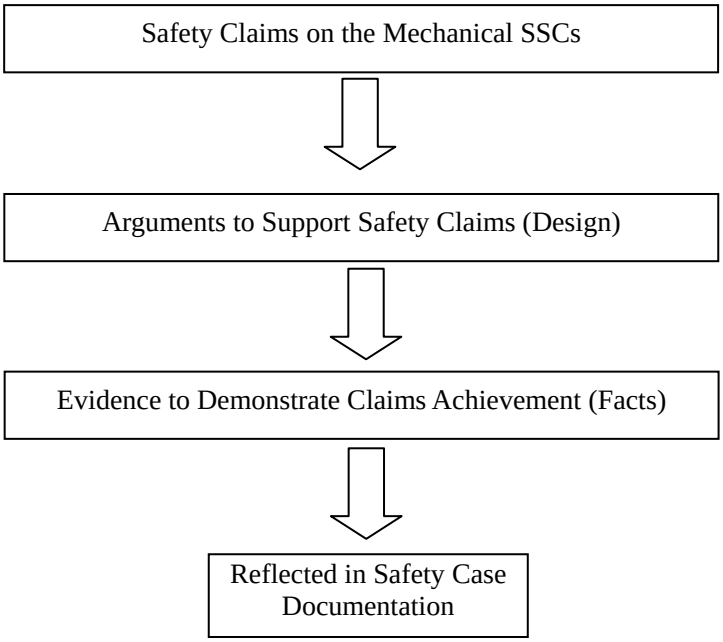


Figure 4.1-1 Summary of Mechanical Engineering CAE Process

One of the objectives of Step 2 is the assessment of key claims on the mechanical SSCs. The safety case starts from the fundamental top claim stating that: “The UK ABWR is safe”. All the safety claims derive from this fundamental top level claim and they can be divided into Plant Level Claims, which are general claims on safety, and System Level Claims, which are the safety claims on the mechanical SSCs. The following figure shows the basic flow of claims for a fault conditions case.

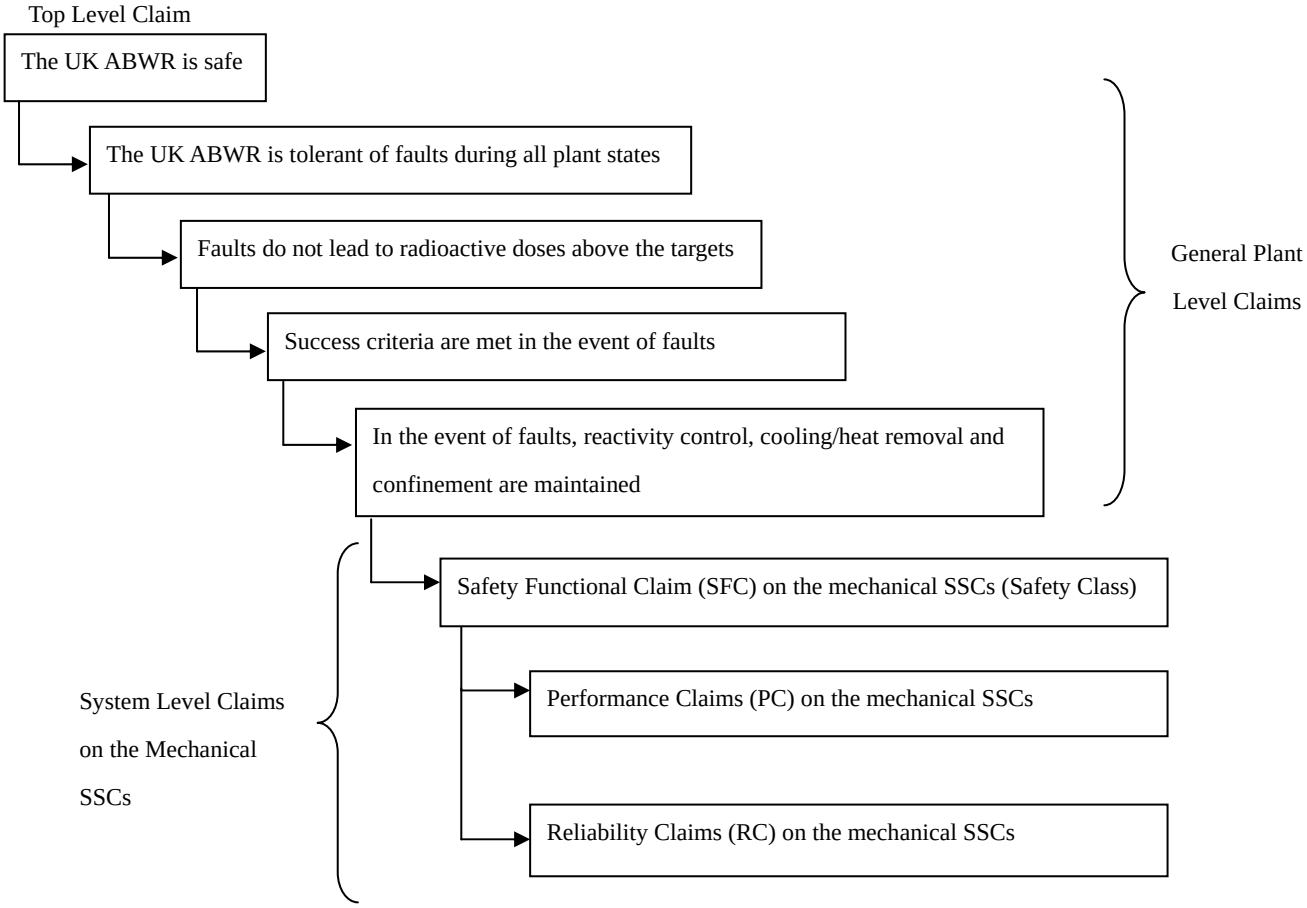


Figure 4.1-2 Example of Flow of Claims on Mechanical SSCs

As shown on the figure, System Level Claims on the Mechanical SSCs are further divided into Safety Functional Claims (SFC), which derive into low level Performance Claims (PC) and Reliability Claims (RC).

4.2. Definition of Claims

Following the fault conditions example, Safety Functional Claims (SFCs) on mechanical SSCs important to safety as a mitigation measures in a fault scenario derive from the Fault Schedule generated in the Fault Studies.

These SFCs are the safety functions that the safety SSCs are claimed to deliver for mitigation of faults, and therefore are common to the mechanical system and all the rest of systems (C&I, electrical system, HVAC, etc.) that in conjunction with it form the means to deliver the safety function. The SFCs correspond to the safety classes defined in the safety categorisation and classification of UK ABWR [Ref-10]. Since SFCs are too high level to design the mechanical SSCs, low level performance and reliability claims are derived so as to satisfy them.

Performance Claims (PCs) come from the Deterministic Safety Analysis (DSA) in order to justify the success criteria in the case of fault conditions. They become the input claims on the SSCs, which must be designed in order to satisfy them. Examples of performance claims are actuation time, flow rate, heat removal capacity, pressure, etc.

Reliability Claims (RCs) come from the Probabilistic Safety Assessment (PSA) in order to justify the success criteria in the case of fault conditions. They become the input claims on the SSCs, which must be designed in order to satisfy them. The reliability claim derived from the PSA is the probability of failure of the SSCs, which is provisionally defined as highest reliability for Class 1, high reliability for Class 2 and standard industrial reliability for Class 3. However, not all RCs come from the fault assessment. RCs such as the design operational life of the SSCs come from plant specifications.

In order to satisfy RCs on the probability of failure, these RCs are further divided into Lower Level Reliability Claims (LLRC) such as the following examples:
LLRC1: Class 1 SSCs are designed with redundancy against single failure of any dynamic component under the worst permissible system availability state (SAP EDR.2, EDR.4).
LLRC2: Class 1 SSCs are designed with independence and segregation against common cause failure (SAP EDR.2, EDR.3).
LLRC3: mechanical interfaces are designed such that failure in a lower class item will not propagate to Class 1 items (SAP paragraph 155).
LLRC4: Class 1 SSCs are designed and qualified to deliver the safety function claimed with the reliability claimed under the environmental and operational conditions during normal operation, transient and accident conditions (SAP EQU.1, paragraph 163).
LLRC5: Class 1 SSCs are protected or designed to withstand the effects of internal and external hazards (SAP ESS.18).
LLRC6: Class 1 SSCs are designed with the capability for being tested, maintained and monitored during operation or refuelling outages to ensure the reliability claimed for Class 1 SSCs without compromising the availability to deliver the safety function (SAP EMT.1, EMT.2, EMT.5, EMT.6).
LLRC7: Class 1 SSCs are designed manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate nuclear-specific codes and standards or equivalent leading to a conservative design commensurate with Class 1 reliability (SAP ECS.3, paragraph 148, 159).
LLRC8: No human intervention is necessary for approximately 30 minutes following the start of the requirement for the safety function claimed (SAP ERL.3, ESS.8, paragraph 344).

With regard to mechanical SSCs important to safety outside a fault scenario such as mechanical SSCs to prevent the initiation of faults during normal operation or mechanical SSCs necessary to minimise the release of radioactive material in the liquid or airborne emissions during normal operation, as defined in the safety categorisation and classification of UK ABWR [Ref-10], the SFCs come from regulatory requirements, guidance, design practices, standards, the reference design of the ABWR, the consequences of failure of the SSCs, etc. Likewise these SFCs derive into PCs, RCs and LLRCs to design the mechanical SSCs so as to satisfy them.

Attachment-1 shows specific examples of SFCs, PCs, RCs and LLRCs for fault and normal operation scenarios.

4.3. Definition of Arguments

The mechanical SSCs are designed, manufactured, qualified and tested in order to satisfy the safety claims described in section 4.2. First, based on the mature design of the Japanese reference plant, an optioneering process to satisfy the claims raised and also reduce the risk to a As Low As Reasonably Practicable (ALARP) level is carried out. As a result, the design features of mechanical SSCs are determined (specifications, architecture, materials, layout, protection, tests provisions, codes and standards, etc.), which become the arguments that support the claims. The following table shows an example of representative arguments to support the claims mentioned in the previous section.

In addition, Attachment-1 shows specific examples of arguments for fault and normal operation scenarios.

Table 4.3-1 Examples of Arguments

Claim	Argument	Example
Performance	Provision of SSCs with adequate specifications	Provision of an accumulator of (xxMPa) and (xxm^3) of capacity
Reliability	Design of system architecture	Design with (xx) redundant divisions, independent and physically separated
	Design of system interfaces	Installation of isolation valves at the interface
	Selection of adequate materials Determination of adequate design pressures/temperatures Qualification provisions put in place	Material: Ex. SUS (xxMPa) design pressure (xx^oC) design temperature Implementation of qualification tests to verify equipment behaviour (fracture test, cycles, etc.)
	System layout design Protection against LOOP Provision of fire protection	Provision of physical separation/barriers Provision of fail-safe passive valves Provision of fire walls
	Examination, Maintenance, Inspection and Test (EMIT) provisions in place	Facilities for tests during operation and outages, monitoring instrumentation. Design with accessibility for maintenance
	Codes and Standards	Application of ASME Section III

4.4. Definition of Evidence

The claims put on Mechanical SSCs are demonstrated with evidence that substantiate the arguments supporting them. The adequacy of the design to satisfy the claims is finally evaluated with the arguments and evidence, and depending on the results, these are fed back to the design process to modify the design if necessary. The following table shows an example of representative evidence to justify the claims mentioned before.

In addition, Attachment-1 shows specific examples of evidence for fault and normal operation scenarios.

Table 4.4-1 Examples of Evidence

Claim	Evidence	Example
Performance	Design specifications	Equipment design specifications
	Analysis results	DSA results
	Qualification results	Performance test results
	Tests results	Operational test results
	Operational Experience	Reference plant results
Reliability	Analysis results	PSA results
	Drawings	P&ID, equipment drawings, plot plan drawings
	Qualification results	Procedures and test results
	Tests results	Operational test procedures and data, outage test procedures and data
	Maintenance provisions	Maintenance procedures and record
	Surveillance provisions	Surveillance/monitoring procedures, data
	Codes and Standards	Code certification
	Operational Experience	Reference plant results

The following chapters show a preliminary safety case with specific claims and examples of arguments of the most representative mechanical systems delivering the three main safety functions fundamental for safety (reactivity control, cooling/heat removal and confinement).

5. Control Rod Drive System Preliminary Safety Case

5.1. System Summary Description

This section is a general introduction to the Control Rod Drive System (CRD) where the system roles, system functions, system configuration and modes of operation are briefly described.

5.1.1. System Roles

The main roles of the CRD are the following:

(1) The CRD drives the electro-hydraulic Fine Motion Control Rod Drive mechanism (FMCRD) through an electric motor and thereby changes the position of the Control Rods (CRs) in the core to control the reactivity during normal operation.

During abnormal transients of the plant, the FMCRDs are hydraulically driven by pressurized water from the Hydraulic Control Unit (HCU) to rapidly insert all the CRs into the core, action known as Scram, and thereby shut down the reactor safely.

(2) During normal operation the CRD Pumps supply purge water to the FMCRDs, the Reactor Internal Pumps (RIPs), and the Reactor Water Clean-up System pump (CUW Pump) while continuously maintain the HCU Accumulators pressurized to keep them charged at high pressure for eventual scrams.

5.1.2. Functions Delivered

The CRD is designed to perform the following functions:

(1) The CRD through its electric motors position the CRs in the core depending on the control signal from the Rod Control and Information System (RC&IS) when performing normal insertion and withdrawal for control of changes in core reactivity.

(2) The CRD through the FMCRDs implements reactor scram operation when receiving the scram signal from the Reactor Protection System (RPS). The FMCRD electric motors are actuated to back up the full insertion of the CRs with the scram follow-in signal from the RPS.

(3) The CRD opens the scram valves provided on the outlet of each HCU accumulator and thereby the pressurised water stored in the HCU accumulator is supplied to the piston section of the FMCRD in the event that the scram signal was initiated. As a result, the FMCRDs are hydraulically driven and each CR is rapidly inserted to shut down the reactor.

(4) Through the Alternative Rod Insertion (ARI) signal, from the Anticipated Transient without Scram System (ATWS), the CRD allows the CRs to be hydraulically inserted in case scram could not be performed upon scram signal.

(5) At the same time, the CRD actuates the FMCRD electric motors to back up the full insertion of the CRs with the FMCRD run-in signal from the ATWS.

(6) The CRD supplies purge water from the discharge side of the CRD Pumps in order to prevent deposition of crud from the reactor side in the FMCRDs during plant normal operation.

(7) The CRD supplies purge water from the discharge side of the CRD Pumps in order to prevent leakage of reactor water into the Reactor Internal Pumps (RIPs) and the Reactor Water Clean-up System pumps (CUW Pumps) during plant normal operation.

(8) The CRD is utilised to pressurise the Reactor Pressure Vessel (RPV) when the leakage and hydrostatic test is implemented.

5.1.3. Basic Configuration

The CRD consists of the following main components:

(1) Fine Motion Control Rod Drive (FMCRD)

The FMCRDs provide electric-motor-driven positioning for normal insertion and withdrawal of the control rods and hydraulic-powered rapid insertion (scram) of control rods during abnormal operating conditions. There are a total of 205 FMCRDs mounted in housings welded into the reactor vessel bottom head.

Furthermore, the FMCRD electric motors are actuated to back up the full insertion of the CRs with the scram follow-up signal from the RPS.

(2) Hydraulic Control Unit (HCU)

The hydraulic power required for scram is provided by high pressure water stored in 103 individual HCUs. Each HCU contains a nitrogen-water accumulator charged to high pressure and the necessary valves and components to scram two FMCRDs. In addition, during normal operation, the HCUs provide a flow path for purge water to the associated FMCRDs.

(3) Control Rod Drive System Pumps (CRD Pumps)

Through the CRD Pumps the CRD supplies clean, demineralised water which is regulated and distributed to provide charging of the HCU scram accumulators and purge water flow to the FMCRDs during normal operation. The CRD Pumps also supply pressurised water for purging the RIPs and the CUW Pumps.

(4) Control Rod Drive System Drive Water Heater (CRD Drive Water Heater)

(5) Suction filters (CRD Pump Suction Filters)

(6) Control Rod Drive System Drive Water Filters (CRD Drive Water Filters)

(7) CRD Charging Header Accumulator

(8) HCU Nitrogen Gas Charging Equipment

(9) Valves, piping, instrumentation, and controllers

Figure 5-1 shows an outline of the CRD configuration.

5.1.4. Modes of Operation

(1) Normal Operation Mode

Normal operation is defined as those periods of time when no control rod drives are in motion. Under this condition, the CRD System provides charging pressure to the HCUs and supplies purge water to the CR drives, RIPs and CUW Pumps.

(2) Control Rod Insertion and Withdrawal Mode

The CRD receives the control signal from the RC&IS and actuates the FMCRD electric motors to drive the CRs according to the specified insertion steps when implementing normal insertion/withdrawal of the CRs for control of changes in core reactivity.

(3) Scram Drive Mode

Upon loss of electric power to both scram pilot valve solenoids, the scram valve in the associated HCU opens to apply the hydraulic insert forces to its respective FMCRDs using high pressure water stored within the pre-charged accumulator to shut down the reactor.

(4) Scram Completion Mode

The RC&IS transmits the control signal to the FMCRDs after receiving the control signal from the RPS. In consequence the FMCRDs actuate the electric motors in order to initiate the scram follow.

(5) Alternative Rod Insertion (ARI)

The ARI function of the CRD System provides an alternate means for actuating hydraulic scram that is diverse from the RPS. The signals to initiate the ARI are high reactor dome pressure or low reactor vessel water Level 2 or manual operator action. Following receipt of any of these signals, solenoid-operated valves on the scram air header open to reduce pressure in the header, allowing the HCU scram valves to open. The FMCRDs then insert the control rods hydraulically in the same manner as the RPS initiated scram. The same signals that initiate ARI will simultaneously actuate the FMCRD motors to insert the control rods electrically.

5.2. Design Bases

This section describes the claims put on the CRD, from high level safety functional claims (common to the CRD and all the rest of systems that in conjunction with it deliver the safety function) to low level performance claims and reliability claims that apply only to the CRD in this case.

5.2.1. Safety Functional Claims

The CRD has been designed to meet the following Safety Functional Claims (SFCs) (SAP EKP. 1~5):

Normal Operation:

SFC1. Part of the CRD forms the Reactor Coolant Pressure Boundary (RCPB). Therefore, the components within the RCPB ensure the pressure integrity of the boundary and preserve reactor coolant, loss of which would lead to consequences above the BSL. From this perspective, the CRD delivers a Category A preventive function and the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC2. Part of the CRD forms the Primary Containment Vessel Boundary (PCV Boundary). Therefore, the components within the PCV boundary form a barrier to maintain the integrity of the boundary and thus prevent the dispersion of radioactive substances. From this perspective, the CRD delivers a Category A mitigation function (containment) and the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

Fault Conditions:

SFC3. The CR and CRD are the principal means to provide reactor rapid shutdown by performing control rod insertion, actuation known as scram, so that fuel design margins are not exceeded in the event of frequent faults. Furthermore, the CR and CRD are the principal means to provide scram in the event of infrequent faults requiring reactor shutdown. From this perspective, the CRD delivers a Category A mitigation function, and as a principal means, the components necessary to deliver scram are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC4. The CR and CRD are the principal means of maintaining core sub-criticality. From this perspective, the CRD delivers a Category A mitigation function, and as a principal means, the components necessary to deliver maintenance of sub-criticality are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC5. The CR and CRD are the principal means to prevent excessive reactivity insertion due to a CR drop event after reactor shutdown. From this perspective, the CRD delivers a Category A prevention function, and as a principal means, the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

The categorisation and classification above described also applies to the support systems and components necessary to deliver the claimed safety functions unless failure does not prejudice the successful delivery. The Safety Categorisation and Classification is addressed in Step S2b document [Ref.10].

For this particular example, only claim SFC3 (reactor rapid shutdown), SFC4 (maintenance of core sub-criticality) and SFC5 (prevention of excessive reactivity insertion) are developed. Safety functional claims SFC3, SFC4 and SFC5 are high level claims that derive into lower level performance and reliability claims on the mechanical SSCs of the CRD to design them so as to satisfy the high level claims.

5.2.2. Performance Claims

The following Performance Claim PC1 is derived from safety functional claims SFC3 and SFC4 in order to ensure reactor rapid shutdown and maintenance of core sub-criticality.

Fault Conditions:

SFC3. The CR and CRD are the principal means to provide reactor rapid shutdown by performing control rod insertion, actuation known as scram, so that fuel design margins are not exceeded in the event of frequent faults. Furthermore, the CR and CRD are the principal means to provide scram in the event of infrequent faults requiring reactor shutdown. From this perspective, the CRD delivers a Category A mitigation function, and as a principal means, the components necessary to deliver scram are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC4. The CR and CRD are the principal means of maintaining core sub-criticality. From this perspective, the CRD delivers a Category A mitigation function, and as a principal means, the components necessary to deliver maintenance of sub-criticality are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

PC1. The average maximum scram time for insertion of all control rods into the core under hot reactor conditions with accumulator available and reactor steady state pressure as measured at the vessel bottom below 7.48MPa [gage] meets the following performance (time from de-energising of the scram pilot valves):

Table 5.2-1 Control Rod Insertion Times

Percent of CR Insertion into the Core	Time (seconds)
60% Insertion Position	≤1.44
100% Insertion Position (Full insertion)	≤2.80

(All time values represent the elapsed time after the opening of the ON/OFF control contacts of the dual solenoids of HCU scram pilot valve and include a maximum time delay from the opening of the contacts to the initiation of the FMCRD action (0% lead switch dropping out). However, the above indicated times do not include the time delay from the initiation of the scram signal by the scram signal detectors till the opening of the ON/OFF control contacts).

5.2.3. Reliability Claims

The following Reliability Claims RC1 and RC2 are derived from safety functional claims SFC3, SFC4 and SFC5:

SFC3. The CR and CRD are the principal means to provide reactor rapid shutdown by performing control rod insertion, actuation known as scram, so that fuel design margins are not exceeded in the event of frequent faults. Furthermore, the CR and CRD are the principal means to provide scram in the event of infrequent faults requiring reactor shutdown. From this perspective, the CRD delivers a Category A mitigation function, and as a principal means, the components necessary to deliver scram are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC4. The CR and CRD are the principal means of maintaining core sub-criticality. From this perspective, the CRD delivers a Category A mitigation function, and as a principal means, the components necessary to deliver maintenance of sub-criticality are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC5. The CR and CRD are the principal means to prevent excessive reactivity insertion due to a CR drop event after reactor shutdown. From this perspective, the CRD delivers a Category A prevention function, and as a principal means, the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

RC1. CRD Class 1 SSCs are designed with the highest reliability to deliver SFC3, SFC4 and SFC5 (SAP Paragraph 166, ERL.1).

RC2. CRD SSCs not subjected to replacement are designed and qualified to be capable to deliver the performance and reliability claimed throughout an operational life of 60 years (SAP EQU.1).

In order to satisfy RC1, the following Lower Level Reliability Claims LLRC1~LLRC9 are derived from it:

RC1. CRD Class 1 SSCs are designed with the highest reliability to deliver SFC3, SFC4 and SFC5.

LLRC1. CRD Class 1 SSCs are designed with redundancy against single failure of any dynamic component under the worst permissible system availability state so that single failure does not prevent the delivery of SFC3, SFC4 and SFC5 (SAP EDR.2, EDR.4).

LLRC2. CRD Class 1 SSCs are designed with independence and separation such that failure of one dynamic component does not lead to a common cause failure that could prevent the delivery of SFC3, SFC4 and SFC5 (SAP EDR.2, EDR.3).

LLRC3. The mechanical interfaces between SSCs of different safety classes and the mechanical interfaces with the pressure boundary are designed such that failure in a lower class item will not propagate to CRD Class 1 items and jeopardise the delivery of SFC3, SFC4 and SFC5 (SAP paragraph 155).

LLRC4. CRD Class 1 SSCs are designed and qualified to deliver SFC3, SFC4 and SFC5 under the environmental and operational conditions during normal operation, during and after transient and accident conditions with the reliability claimed throughout their respective operational lives (SAP EQU.1, paragraph 163).

LLRC5. CRD Class 1 SSCs are protected or designed to withstand the effects of internal hazards so that they do not affect the delivery of SFC3, SFC4 and SFC5 (SAP ESS.18).

LLRC6. CRD Class 1 SSCs are protected or designed to withstand the effects of external hazards so that they do not affect the delivery of SFC3, SFC4 and SFC5 (SAP ESS.18).

LLRC7. CRD Class 1 SSCs are designed with the capability for being tested, maintained and monitored during operation or refuelling outages to ensure the reliability claimed without compromising the availability to deliver SFC3, SFC4 and SFC5 (SAP EMT.1, EMT.2, EMT.5, EMT.6).

LLRC8. CRD Class 1 SSCs are designed manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate nuclear-specific codes and standards or equivalent leading to a conservative design commensurate with Class 1 reliability (SAP ECS.3, paragraph 148, 159).

LLRC9. No human intervention is necessary for approximately 30 minutes following the start of the requirement for reactor rapid shutdown (SAP ERL.3, ESS.8, paragraph 344).

5.3. System Design Description

This section describes the design of the CRD with arguments to support the performance and reliability claims derived from SFC3, SFC4 and SFC5.

5.3.1. Overall Design and Operation

(1) Scram Drive Mode

Upon loss of electric power to both scram pilot valve solenoids, the scram inlet valve in the associated HCU opens to apply the hydraulic insert forces to its respective FMCRDs using high pressure water stored within the previously charged HCU Accumulator (the nitrogen-water accumulator previously been pressurized with charging water from the CRD Pumps). Once the hydraulic force is applied, the hollow piston disengages from the ball-nut and inserts the control rod rapidly to deliver SFC3 and SFC4. The water displaced from the drive is discharged into the RPV. Indication that the scram has been successfully completed (all rods full-in position) is displayed to the operator.

5.3.2. Equipment Design and Operation

(1) Fine Motion Control Rod Drive (FMCRD)

(a) Configuration

There are a total of 205 FMCRDs, one for each CR. The FMCRD penetrates the bottom head of the RPV. The FMCRD consists of the components enclosed inside the CRD housing mounted on the bottom head of the RPV.

The FMCRD used for positioning the control rod in the reactor core is a mechanical/hydraulic actuated mechanism. An electric motor-driven ball-nut and ball screw is capable of positioning the drive during normal operation according to the signals from the RC&IS. On the other hand, hydraulic pressure is used for scrams after receiving the scram signal from the RPS or the ARI signal.

During fault conditions, a single HCU powers the scram action of two FMCRDs. Upon scram valve initiation, high pressure nitrogen from the HCU raises the piston within the accumulator, forcing water through the scram piping. This water is directed to each FMCRD connected to the HCU. Inside each FMCRD, high-pressure water lifts the hollow piston off the ball-nut and drives the control rod into the core. A spring washer buffer

assembly stops the hollow piston at the end of its stroke. Departure from the ball-nut automatically releases spring-loaded latches in the hollow piston that engage slots in the guide tube. These latches are redundant and support the control rod in the inserted position to prevent excessive reactivity insertion due to an eventual drop of the control rod. The control rod cannot be withdrawn until the ball-nut is driven up and engaged with the hollow piston. These components are designed to satisfy SFC5.

A bayonet coupling is located between the control rod and the FMCRD. The coupling spud at the top end of the FMCRD hollow piston engages and locks into a mating socket at the base of the control rod. The coupling requires a 45^{o} rotation for engaging or disengaging. Once locked, the drive and rod form an integral unit that can only be unlocked manually by specific procedures before the components can be separated. Therefore, when assuming a control rod drop accident, the CRs will drop coupled with the hollow piston of the FMCRDs. This control rod bayonet coupling is also designed to satisfy SFC5.

(b) Performance

The FMCRD components for scram are designed to be hydraulically actuated by the HCU and thus fully insert the CRs to deliver reactor rapid shutdown (SFC3) and maintenance of core sub-criticality (SFC4) within 2.8 seconds as claimed in PC1.

(2) Hydraulic Control Unit (HCU)

(a) Configuration

Each HCU furnishes pressurised water for scram, on signal from the RPS, to the two associated FMCRDs. There are 103 HCUs in total, of which 102 units actuate two FMCRDs and one unit actuates one FMCRD. Additionally, each HCU provides the capability to adjust purge flow to the two associated FMCRDs.

The HCU basically consists of a purge water solenoid valve, a scram pilot valve, a scram valve, the accumulator and the nitrogen gas bottle. Each HCU (except for the one driving only one FMCRD) is capable to accumulate the energy required to force the scram of two FMCRDs.

The scram pilot valve is operated by the signal from the RPS. The scram pilot valve consists of two three-way solenoid valves with single diaphragm to control the scram valve. The scram pilot valve is solenoid-operated and is normally energised. Upon loss of electrical signal to the solenoids (loss of power supply), the inlet port closes and the exhaust port opens to assure fail-safe condition. The scram pilot valve is designed so that so that both solenoids must be de-energised before air pressure can be discharged from the

scram valve actuator. This prevents the inadvertent scram of both drives associated with a given HCU in the event of a failure of one of the pilot valve solenoids.

The scram valves are provided in order to assure a reliable scram when required. The scram valve opens to supply pressurised water to the bottom of the hollow piston. This valve is operated by an internal spring and air pressure. The scram valves are kept closed by the effect of the air pressure during normal operation. The scram valves are designed such that in the event of loss of electric power of the scram pilot valve or air supply, the actuator discharges the pressurised air and the valves open to perform scram (fail-safe design). The scram valves are opened by the pressurised air discharge from the actuator upon any of the following events:

(i) Both of the scram pilot valve solenoids stop being excited

(ii) The scram pilot valve air line is depressurized by the backup scram pilot valves or the ARI electromagnetic valves.

Therefore no operator action is required to perform scram as claimed in LLRC9.

The scram accumulator stores sufficient energy to fully insert two control rods at any reactor pressure within the time claimed in PC1. The accumulator is cylinder with a free-floating piston. The piston separates the water on top from the nitrogen below. A check valve in the accumulator charging header prevents loss of water pressure in the event that supply pressure is lost. During normal plant operation, the accumulator piston is seated at the bottom of its cylinder. In order to ensure that the accumulator is always available to perform scram, instrumentation is installed in the HCU to confirm the nitrogen gas is maintained at high pressure and there is no water leakage.

(b) Performance

The HCU accumulators are designed as follows in order to satisfy the performance claimed in PC1.

The capacity of water side and nitrogen side of the HCU accumulators is the necessary to insert the two control rods of each HCU within the determined time claimed in PC1 in the event of scram according to the performance test results carried out.

The HCU unit actuating one FMCRD is also designed and arranged such that the distance with the control rod is sufficient to ensure insertion times. The scram times claimed in PC1 are attained even at the lowest charge pressure of the HCU Accumulator (Accumulator Low Pressure Alarm set value).

5.3.3. Main Support Systems

The main systems supporting mechanical SSCs for the delivery of SFC3, SFC4 and SFC5 are briefly described as follows.

(1) Instrumentation and Control

The main instrumentation and control provisions related to CRD operation from the performance and reliability points of view are summarised as follows.

(a) Instrumentation

As claimed in LLRC7, instrumentation is provided to measure and monitor the operating conditions of the CRD components necessary for the delivery of SFC3, SFC4 and SFC5 and thus ensure their performance and reliability. The status, measurements and alarms of the components and valves to be remotely operated are generally displayed in the Main Control Room. An example of some provisions for instrumentation is given as follows.

(i) Charging water header pressure

(ii) Scram pilot valve air header inlet pressure

(iii) HCU accumulator pressure

(b) Control

An example of the main control provisions related to the delivery of SFC3, SFC4 and SFC5 is given as follows.

(i) The HCU scram pilot valve is actuated (discharge) by the scram signal from the RPS and thereby the scram valve is opened to implement scram.

(ii) The charging water header low-low pressure signal is transmitted to the RPS for implementing the reactor scram before the scram function is lost.

(2) Power Supply System

Power supply is not required for the delivery of SFC3, SFC4 and SFC5.

(3) Heating Ventilating and Air Conditioning System (HVAC)

The HVAC maintains the temperature range in the HCU room within 20°C (provisional) and 40°C (provisional) in order to suppress accumulator water reduction due to volume expansion of nitrogen gas in the HCU Accumulator.

5.3.4. System Architecture

(1) Redundancy

In order to satisfy LLRC1 and ensure SFC3 and SFC4, redundant FMCRDs and HCUs are arranged with an interval equal to or greater than [ ] pitches around the core such that in the

event of single failure of a HCU unit reactor cold shutdown can be completed. That is, failure of up to two FMCRDs does not prevent reactor cold shutdown. Therefore single failure does not prevent the delivery of SFC3 and SFC4.

From the point of view of delivery of SFC5, the FMCRD has multiple features to prevent control rod drop (control rod coupling, hollow piston, latch, guide tube, ball-nut, ball screw and brake). Furthermore, as mentioned before, even if single failure of a CR or FMCRD reactor cold shutdown can be maintained, and therefore, it does not lead to an insertion of excessive positive reactivity into the core.

(2) Independence

In order to satisfy LLRC2 and ensure the delivery of SFC3, SFC4 and SFC5, each HCU group with its two associated FMCRDs are independently and separately arranged around the core such that failure of one FMCRD does not affect the others, and failure of one HCU can only affect the two associated FMCRDs but not the rest of HCUs.

5.3.5. System Interfaces

As claimed in LLRC3, the interfaces between SSCs of different safety classes and with the pressure boundary are appropriately designed to ensure that any failure in a lower class item will not propagate to an item of a higher class. As a general rule, equipment providing the function to prevent the propagation of failures is assigned to the higher class. When SSCs of different classes are connected, design requirements equivalent to those for higher class are applied to the lower class. Alternatively, adequate functional isolation by means of, for example, isolation devices equivalent to higher class are considered so that the safety functions of the SSCs of higher class are not impaired of the failure of the lower SSCs.

5.3.6. Qualification

Qualification provisions are put in place to ensure that the CRD SSCs are capable of delivering the performance and reliability claimed throughout their respective operational lives and under the environmental and operational conditions claimed in order to satisfy RC2 and LLRC4.

The CRD is first designed with adequate materials, design pressure and temperatures to withstand the operational and environmental conditions upon which SFC3, SFC4 and SFC5 are required without sustaining damage that could lead to the loss of the safety function. In addition, qualification procedures (prototype tests, factory acceptance tests, commissioning tests, etc.) to physically demonstrate that individual items can deliver their safety function under the required conditions with the performance and reliability claimed are implemented.

5.3.7. Hazards Protection

As claimed in LLRC5 and LLRC6, design provisions against the effects of hazards that could affect the delivery of SFC3, SFC4 and SFC5 are put in place.

(1) Internal Hazards

CRD components necessary to deliver SFC3, SFC4 and SFC5 are protected with specific countermeasures against the effects of internal flooding, internal fire, dropped loads, internal missiles, failure of pipes, tanks, pumps and valves (pipe whip, etc.) and internal explosions as applicable. An example of the main provisions to satisfy LLRC5 is given as follows.

(a) Fire

HCU groups are strategically arranged in different locations and physically separated in fire compartments as a countermeasure against fire hazards.

(2) External Hazards

An example of the main provisions to satisfy LLRC6 is given as follows.

(a) Seismic Design

CRD Class 1 components are designed with the seismic resistance corresponding to Seismic Category 1 assigned to ensure the reliability required by SFC3, SFC4 and SFC5 under design basis earthquake conditions.

(b) Design against LOOP

As described in 5.3.3 (2), power supply is not required for the delivery of SFC3, SFC4 and SFC5.

5.3.8. Examination, Maintenance, Inspection and Test (EMIT)

As claimed in LLRC7, the CRD is designed to facilitate test, maintenance and surveillance (monitoring) tasks during operation or shutdown periods to ensure the performance and reliability claimed without compromising the availability for the delivery of SFC3, SFC4 and SFC5. An example of some EMIT provisions is given as follows.

(1) On-line and Outage Tests

(a) The FMCRDs are designed such that insertion, withdrawal and scram operation test can be performed during refuelling outage.

(2) Maintenance

(a) FMCRDs inside the drywell are designed such that maintenance is facilitated during refuelling outages. The components outside the drywell such us HCUs are designed such that maintenance can be performed easily and within the minimum time during normal plant operation.

(b) The layout of CRD facilities are designed to facilitate operator's access to the maintenance and repair areas. Plant layout design considers the handling of removed parts of heavy components and machinery for maintenance and repair.

(3) Surveillance (Monitoring)

(a) An example of monitoring provisions is given in section 5.3.3 (1) (a).

(b) Equipment is arranged such that personnel and equipment required for integrity tests and surveillance can access into the area as close as possible.

(c) The FMCRDs are designed such that surveillance can be performed to verify the rods integrity during reactor normal and stable operating conditions.

5.3.9. Codes and Standards

Codes and standards are selected to satisfy LLRC8 and thus ensure the reliability claimed. Mechanical equipment is designed in accordance with ISO, BS and European Standards in principle.

5.4. System Design Evaluation

As explained in section 5.3, the claims raised in 5.2 are supported with arguments, which will be further developed during Step 3. The evidence substantiating the arguments and demonstrating the achievement of the claims will be developed during Step 3 and Step 4.

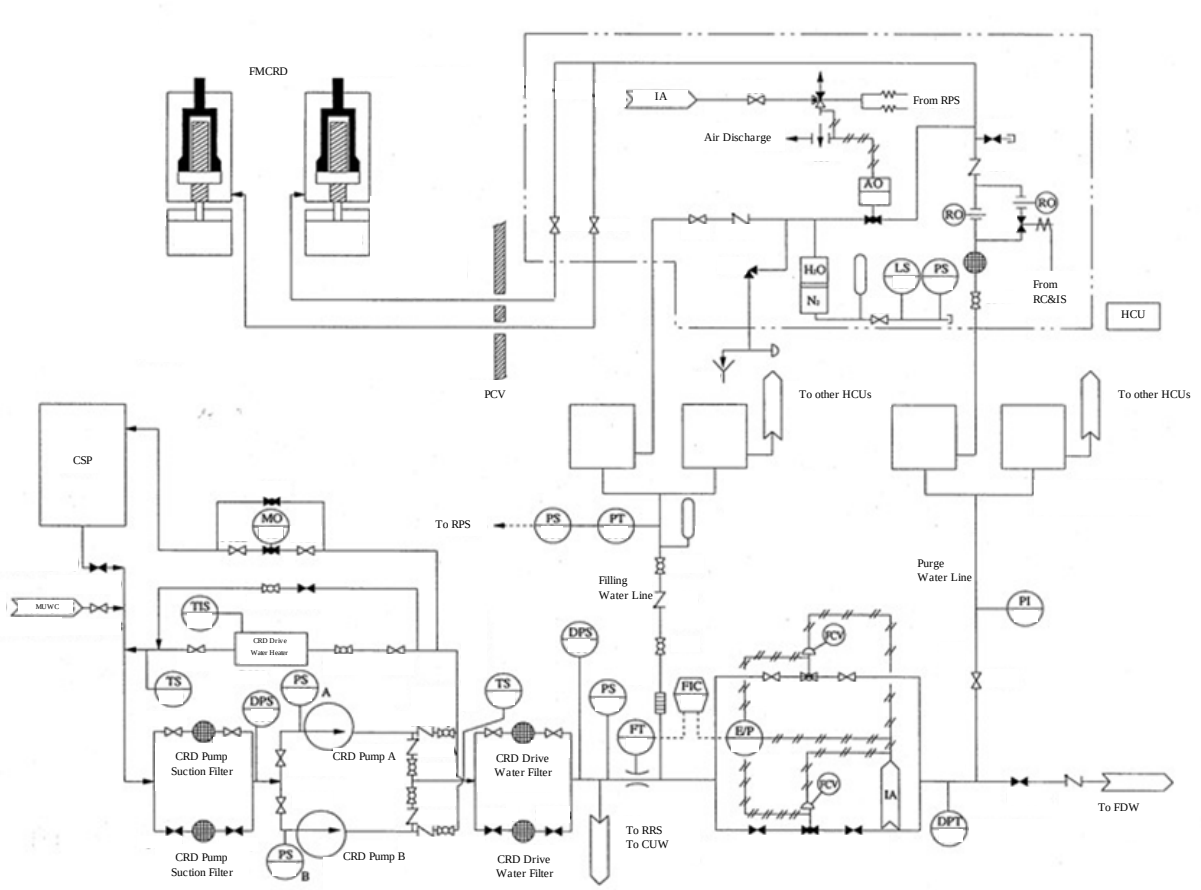


Figure 5-1 Outline of the Control Rod Drive System

6. Residual Heat Removal System Preliminary Safety Case

6.1. System Summary Description

This section is a general introduction to the Residual Heat Removal System (RHR) where the system roles, system functions, system configuration and modes of operation are briefly described.

6.1.1. System Roles

The main roles of the RHR are to remove decay heat during normal reactor shutdown and in the event of unavailability of the main condenser, and to cool the reactor core in the event of a Loss of Coolant Accident (LOCA).

6.1.2. Functions Delivered

The RHR is designed to perform the following functions:

(1) The RHR provides core cooling water supply to the reactor to compensate for water loss in the event of LOCA.

(2) The RHR provides cooling to remove heat released to the Suppression Pool (S/P) as necessary.

(3) The RHR provides Primary Containment Vessel (PCV) cooling through sprays provided in the drywell and wetwell to remove heat and condense steam in the containment following a LOCA and thus prevent over pressurisation. In addition, the drywell sprays are intended to provide removal of fission products released during a LOCA.

(4) The RHR provides cooling to remove decay and sensible heat from the reactor after normal shutdown and in the event that main condenser is not available.

(5) The RHR can work as a backup to cool the Spent Fuel Storage Pool (SFP) if the heat load exceeds the Fuel Pool Cooling and Clean-up System (FPC) maximum cooling capacity.

(6) The RHR can provide makeup water to the SFP from the S/P when the water level of the SFP lowers.

6.1.3. Basic Configuration

The RHR consists of three independent divisions, A, B, and C. Each division has water injection function into the Reactor Pressure Vessel (RPV) and heat removal function from the RPV or the PCV. The necessary piping, valves, pumps and heat exchangers are included in each division.

The RHR includes all the process pipes, strainers, pumps, motors, valves, instrumentation and controllers as shown on Figures 6-1 and 6-2. The main components are summarized as follows:

(1) Pumps and piping, heat exchangers and valves included in the discharge lines running from the pumps to the S/P, feed-water spargers (to the connection with FDW), drywell/wetwell spray spargers, and water injection spargers into the RPV.
(2) Valves, piping, and strainers included in suction lines from the S/P to the respective pumps.
(3) Valves and piping included in suction lines from the reactor shutdown cooling nozzle to the connection to the S/P suction line.
(4) Minimum flow piping and test piping with their valves.
(5) Instrumentation, controllers, operation logic/circuit and control panels.
(6) Piping and valves connecting to the FPC.

6.1.4. Modes of Operation

The RHR can deliver the following operation modes by switching the position of the valves.

(1) Low Pressure Flooder Mode (LPFL)

The RHR cools the reactor core during LOCA (removal of decay heat from the reactor core) as part of the Emergency Core Cooling Systems (ECCS). The LPFL operates to cool the core in conjunction with the High Pressure Core Flooder System (HPCF), the Reactor Core Isolation Cooling System (RCIC) and the Automatic Depressurisation System (ADS) in order to maintain the fuel cladding temperature below the design basis criteria. The three RHR divisions are provided with this mode. Figure 6-2 shows an outline of this operation mode.

(2) Suppression Pool Cooling Mode

During this mode the RHR cools the S/P to remove the heat released as required. The three RHR divisions are provided with this mode.

(3) Primary Containment Vessel (PCV) Spray Cooling Mode

The RHR removes the heat and condenses steam inside the drywell and wetwell after a LOCA in order to prevent over pressurisation of the containment. In addition, it removes fission products. RHR divisions B and C are provided with this mode.

(4) Reactor Shutdown Cooling Mode (SDC)

The RHR provides reactor cold shutdown during reactor normal shutdown and in the event that main condenser is not available. The RHR removes the reactor decay heat so that refuelling and maintenance can be implemented after shutdown. The three RHR divisions are provided with this mode. Figure 6-1 shows and outline of this operation mode.

(5) Auxiliary Operation Mode

In addition, all three RHR divisions are provided with the following auxiliary operation modes:

(a) Fuel Pool Cooling Function

As described in 6.1.2 (5).

(b) Fuel Pool Make-up Function

As described in 6.1.2 (6).

(c) Suppression Pool Water Transfer Function

RHR transfers S/P water to the Suppression Pool Water Drainage System (SPD) surge tank or the Liquid Waste System when the S/P is under maintenance.

6.2. Design Bases

This section describes the claims put on the RHR, from high level safety functional claims (common to the RHR and all the rest of systems that in conjunction with it deliver the safety function) to low level performance claims and reliability claims that apply only to the RHR in this case.

6.2.1. Safety Functional Claims

The RHR has been designed to meet the following Safety Functional Claims (SFCs) (SAP EKP. 1~5):

Normal Operation:

SFC1. The RHR is the principal means to remove residual heat after normal reactor shutdown with the main condenser available to reach reactor cold shutdown. In addition, in the event of unavailability of the main condenser the RHR removes the decay heat of fission products from the reactor without exceeding the fuel design margins and Reactor Coolant Pressure Boundary design conditions after reactor shutdown. From this perspective, the RHR delivers a Category A safety function, and as principal means, the components necessary to deliver residual heat removal are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC2. Part of the RHR forms the Reactor Coolant Pressure Boundary (RCPB). Therefore, the components within the RCPB ensure the pressure integrity of the boundary and preserve reactor coolant, loss of which would lead to consequences above the BSL. From this perspective, the RHR delivers a Category A safety function (containment) and the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC3. Part of the RHR forms the Primary Containment Vessel Boundary (PCV Boundary). Therefore, the components within the PCV boundary form a barrier to maintain the integrity of the boundary and thus prevent the dispersion of radioactive substances. From this perspective, the RHR delivers a Category A safety function (containment) and the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

Fault Conditions:

SFC4. The RHR is a principal means to provide reactor core cooling as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of infrequent faults such as LOCA. From this perspective, the RHR delivers a Category A mitigation function, and as principal means, the components necessary to deliver core cooling are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC5. The RHR is a principal means to supply the SFP with makeup water to maintain the water level within the limits in the event of design basis faults. From this perspective, the RHR delivers a Category A (provisional) mitigation function, and as principal means, the components necessary to deliver SFP makeup water are classified as Class 1 (provisional) safety components according to the safety categorisation and classification of UK ABWR.

SFC6. The RHR supports the PCV confinement function in the event of LOCA by cooling the containment through the wetwell and drywell sprays to maintain its integrity. Furthermore, the spray water contributes to remove fission products. From this perspective, the RHR delivers a Category B (provisional) mitigation function to support the PCV, and therefore, the components necessary to deliver PCV cooling are classified as Class 2 (provisional) safety components according to the safety categorisation and classification of UK ABWR.

The categorisation and classification above described also applies to the support systems and components necessary to deliver the claimed safety functions unless failure does not prejudice the successful delivery. The Safety Categorisation and Classification is addressed in Step S2b document [Ref.10].

For this particular example, only claim SFC1 (heat removal after reactor shutdown) and claim SFC4 (reactor core cooling) are developed. Safety functional claims SFC1 and SFC4 are high level claims that derive into lower level performance and reliability claims on the mechanical SSCs of the RHR to design them so as to satisfy the high level claims.

6.2.2. Performance Claims

The following Performance Claims PC1, PC2 and PC3 are derived from safety functional claims SFC1 and SFC4 in order to ensure heat removal after reactor shutdown and reactor core cooling:

Normal Operation:

SFC1. The RHR is the principal means to remove residual heat after normal reactor shutdown with the main condenser available to reach reactor cold shutdown. In addition, in the event of unavailability of the main condenser the RHR removes the decay heat of fission products from the reactor without exceeding the fuel design margins and Reactor Coolant Pressure Boundary design conditions after reactor shutdown. From this perspective, the RHR delivers a Category A safety function, and as principal means, the components necessary to deliver residual heat removal are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

PC1. The RHR is capable to deliver the minimum flow rate of [ ] m^3/h (provisional) determined by the safety analysis to maintain reactor water level and prevent uncovery of the core.

PC2. The RHR is capable of bringing the reactor to cold shutdown (reactor coolant temperature below 100^oC) within 36 hours after reactor shutdown (control rods insertion) with the main condenser unavailable in the event of Loss of Offsite Power (LOOP) and assuming a single failure in the RHR.

Fault Conditions:

SFC4. The RHR is a principal means to provide reactor core cooling as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of infrequent faults such as LOCA. From this perspective, the RHR delivers a Category A mitigation function, and, as principal means, the components necessary to deliver core cooling are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

PC1. The RHR is capable to deliver the minimum flow rate of [ ] m^3/h (provisional) determined by the safety analysis to maintain reactor water level and prevent uncovery of the core (the same claim as for SFC1).

PC3. The RHR is capable to allow water injection into the reactor within 37 seconds (including 2 seconds of delay for the reception of the automatic initiation and reactor low pressure permissive signals).

6.2.3. Reliability Claims

The following Reliability Claims RC1 and RC2 are derived from safety functional claims SFC1 and SFC4:

SFC1. The RHR is the principal means to remove residual heat after normal reactor shutdown with the main condenser available to reach reactor cold shutdown. In addition, in the event of unavailability of the main condenser the RHR removes the decay heat of fission products from the reactor without exceeding the fuel design margins and Reactor Coolant Pressure Boundary design conditions after reactor shutdown. From this perspective, the RHR delivers a Category A safety function, and as principal means, the components necessary to deliver residual heat removal are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC4. The RHR is a principal means to provide reactor core cooling as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of infrequent faults such as LOCA. From this perspective, the RHR delivers a Category A mitigation function, and, as principal means, the components necessary to deliver core cooling are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

RC1. RHR Class 1 SSCs are designed with the highest reliability to deliver SFC1 and SFC4 (SAP Paragraph 166, ERL.1).

RC2. RHR SSCs not subjected to replacement are designed and qualified to be capable to deliver the performance and reliability claimed throughout an operational life of 60 years (SAP EQU.1).

In order to satisfy RC1, the following Lower Level Reliability Claims LLRC1~LLRC9 are derived from it:

RC1. RHR Class 1 SSCs are designed with the highest reliability to deliver SFC1 and SFC4.

LLRC1. RHR Class 1 SSCs are designed with redundancy against single failure of any dynamic component under the worst permissible system availability state so that single failure does not prevent the delivery of SFC1 and SFC4 (SAP EDR.2, EDR.4).

LLRC2. RHR Class 1 SSCs are designed with independence and separation such that failure of one dynamic component does not lead to a common cause failure that could prevent the delivery of SFC1 and SFC4 (SAP EDR.2, EDR.3).

LLRC3. The mechanical interfaces between SSCs of different safety classes and the mechanical interfaces with the pressure boundary are designed such that failure in a lower class item will not propagate to RHR Class 1 items and jeopardise the delivery of SFC1 and SFC4 (SAP paragraph 155).

LLRC4. RHR Class 1 SSCs are designed and qualified to deliver SFC1 and SFC4 under the environmental and operational conditions during normal operation, during and after transient and accident conditions including LOCA with the reliability claimed throughout their respective operational lives (SAP EQU.1, paragraph 163).

LLRC5. RHR Class 1 SSCs are protected or designed to withstand the effects of internal hazards so that they do not affect the delivery of SFC1 and SFC4 (SAP ESS.18).

LLRC6. RHR Class 1 SSCs are protected or designed to withstand the effects of external hazards so that they do not affect the delivery of SFC1 and SFC4 (SAP ESS.18).

LLRC7. RHR Class 1 SSCs are designed with the capability for being tested, maintained and monitored during operation or refuelling outages to ensure the reliability claimed without compromising the availability to deliver SFC1 and SFC4 (SAP EMT.1, EMT.2, EMT.5, EMT.6).

LLRC8. RHR Class 1 SSCs are designed manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate nuclear-specific codes and standards or equivalent leading to a conservative design commensurate with Class 1 reliability (SAP ECS.3, paragraph 148, 159).

LLRC9. No human intervention is necessary for approximately 30 minutes following the start of the requirement for low pressure reactor core cooling injection (SAP ERL.3, ESS.8, paragraph 344).

6.3. System Design Description

This section describes the design of the RHR with arguments to support the performance and reliability claims derived from SFC1 and SFC4.

6.3.1. Overall Design and Operation

The RHR is composed of three electrically and mechanically independent divisions designated A, B, and C. Each division contains the necessary piping, pumps, valves and heat exchangers.

By switching the position of the valves, the RHR can operate to deliver heat removal after reactor shutdown and reactor core cooling as described as follows.

(1) Reactor Shutdown Cooling Mode (SDC)

In the normal shut down process, the steam is blown to the main condenser to be cooled down until the reactor pressure reaches 0.93MPa [gage] or less before this operation mode. Then, when reactor pressure is below is 0.93MPa [gage], and the reactor mode switch is in “shutdown” or “refuelling” position, the RHR Reactor Shutdown Cooling Mode is initiated, residual heat is removed from the reactor water at a rate below the RCPB cooling rate of limit of 55°C/h to reduce the temperature to 52°C within 20 hours after control rods insertion according to the Japanese practice. These conditions are considered the bounding case for reactor shutdown cooling capacity, which are more severe than the performance claimed in PC2. They are achieved for normal operation where all the three RHR divisions are operating together. Finally, the water temperature is maintained or reduced to perform refuelling or service inspections.

Reactor water is directly drawn from the RPV through the reactor shutdown cooling suction nozzle, passing through the RHR Heat Exchanger, cooled and returned to the reactor before opening the RPV. Division A returns water through the feed-water line A, and divisions B and C return water through the respective low pressure flooder return lines.

This operation mode is initiated and stopped by operator's manual operation from the Main Control Room (MCR) or via the initiation of the Low Pressure Flooder Mode. Figure 6-1 shows and outline of this operation mode.

(2) Low Pressure Flooder Mode (LPFL)

The LPFL supplies sufficient coolant to maintain the fuel cladding temperature below the design-basis criteria and remove the core decay heat during LOCA. During the this mode, each division of the RHR draws water from the S/P and injects the water into the RPV outside the core shroud (RHR division A injects water via the feed-water line A and divisions B and C via their respective low pressure lines into the RPV).

The LPFL Mode is initiated automatically upon drywell high pressure or reactor low water level (L1) starting signals from four independent and redundant sensors, and therefore no operator action is required during the first 30 minutes following an accident as claimed in LLRC9. The RHR pump and injection valve are designed to allow water injection into the reactor in less than 35 seconds after receiving the automatic initiation and reactor low pressure permissive signals, till the pump reaches rated revolutions and the injection valve fully opens as described in section 6.3.2.

Each division is provided with a minimum flow bypass line to return the water to the S/P to prevent pump damage until the pump reaches the necessary injection flow while the injection valve is closed. A motor-operated valve on the bypass line automatically closes when flow in the main discharge line is sufficient to provide reactor core cooling. Figure 6-2 shows and outline of this operation mode.

6.3.2. Equipment Design and Operation

(1) RHR Pump

(a) Configuration

Each division of the RHR is provided with one turbo type pump of 954m^3/h of design flow rate driven by an induction motor to deliver heat removal after reactor shutdown and low pressure core flooding for reactor cooling. This flow rate satisfies the required minimum flow rate of [ ] m^3/h (provisional) to maintain reactor water level according the safety analysis to satisfy claim PC1. Therefore, a total of three pumps delivering 954m^3/h each are provided.

(b) Performance

The RHR Pump is designed to perform as follows in order to satisfy the performance claimed in PC1.

Table 6.3-1 RHR Pump Capacity

Item	Minimum Flow	Flow Rate	Run-out
Flow (m^3/h)	100	954	≤1200
Total Head (m)	-	125 (provisional)	-

The RHR Pumps are designed such that they can be initiated with the discharge valves closed and reach rated flow within 28 seconds (provisional) after receiving the initiation signal to satisfy the performance claimed in PC3. The necessary time to assure emergency power supply in case of loss of normal power supply is included in the previous time.

(2) RHR Heat Exchanger

(a) Configuration

The RHR is provided with three horizontal U-tube/shell type (provisional) heat exchangers of 8.15MW/unit of heat exchange capacity for heat removal after reactor shutdown in order to satisfy claim PC2. The tube side water is reactor coolant drawn from the RPV or S/P water. The shell side cooling water is supplied by the RCW.

(b) Performance

The RHR Heat Exchanger is designed to perform as follows in order to satisfy the performance claimed in PC2.

	Tube Side	Shell side
Fluid:	S/P Water	Fresh water (cooling water)
Flow (m^3/h):	954	1200
Inlet Temperature (°C):	52	32.6(Provisional)
Outlet Temperature (°C):	44.6 (Provisional)	38.5(Provisional)
Heat exchange capacity (MW/unit):	8.15 (Provisional)	

Assumption: The design temperature of the service water is 30°C (provisional).

(3) RHR Injection Valve

(a) Configuration

One motor-operated high speed gate valve is mounted on each LPFL injection line.

(b) Performance

The injection valves are designed to completely open within 33 seconds (provisional) after receiving the automatic initiation signal and thus satisfy the performance claimed in PC3 (elapsed time to full open includes the time delays necessary for emergency power supply establishment and the allowing signal for injection valve opening).

The stem stroke of the valves is approximately ≥25mm/s (opening time ≤10 seconds).

6.3.3. Main Support Systems

The main systems supporting mechanical SSCs for the delivery of SFC1 and SFC4 are briefly described as follows.

(1) Instrumentation and Control

The main instrumentation and control provisions related to RHR operation from the performance and reliability points of view are summarised as follows.

(a) Instrumentation

As claimed in LLRC7, instrumentation is provided to measure and monitor the operating conditions of the RHR components necessary for the delivery of SFC1 and SFC4 and thus ensure their performance and reliability. An example of some provisions for instrumentation is given as follows.

(i) Local pressure indicators are installed at the pump suction lines to monitor the pump

NPSH and head.

(ii) Flow-meters are mounted downstream the RHR Heat Exchangers to monitor system flow rate and to control minimum flow bypass valve.

(iii) Temperature indicators are provided on the inlet and outlet of the RHR Heat Exchanger in order to monitor the heat exchanger performance, verify injection water into the reactor and S/P temperature and confirm warming completion before shutdown cooling operation.

(b) Interlocks

An example of the main interlocks related to the delivery of SFC1 and SFC4 is given as follows.

(i) System Isolation

Full closure of shutdown cooling isolation valves is performed under the following signals:

- Reactor low water level (L3)
- Reactor high pressure
- Pump room high temperature conditions

An interlock is provided to prevent S/P water suction isolation valves from opening if the reactor water suction valve is not fully closed.

(ii) RHR Pumps

An interlock is provided to the RHR Pumps to prevent them being initiated manually if the S/P water or the reactor water suction valves are not fully opened.

(iii) RPV Injection Valves

An interlock is provided to prevent valves opening whenever pressure is above the high pressure limits.

(c) Logic

An example of the main logic related to the delivery of the SFC4 is given as follows.

The RHR Low Pressure Flooder mode automatically starts after receiving LOCA signal (reactor low water level L1 or drywell high pressure 13.7kPa [gage]). The following sequence is implemented after start signal reception:

(i) The RHR Pumps receive the initiation signal after the auxiliary power supply or the emergency power supply is assured.

(ii) The RHR Heat Exchanger outlet valves receive opening signal.

(iii) The injection valves are opened upon reactor low pressure conditions (3.10MPa [gage]).

(2) Power Supply System

The configuration of the power supply systems necessary to deliver SFC1 and SFC4 is summarised as follows.

(a) The RHR is connected to separated and independent divisions of AC and DC power sources supplying the required power to all electrical components in each division (RHR Division A is connected to power Division I, RHR Division B is connected to power Division II and RHR Division C is connected to power Division III).

(b) The normal AC power supply to the RHR electrical components is provided by an independent and reliable off-site source (external grid). In addition, independent divisional power sources such as diesel generators provide a reliable source of electrical power in the event of LOOP to satisfy LLRC6.2.

(3) Reactor Building Cooling Water System (RCW)

The RCW supplies water to the RHR Heat Exchangers, RHR Pumps, motors, bearings and seal water cooling equipment. The RHR is connected to independent and separated RCW divisions (A, B, C).

(4) Heating Ventilating and Air Conditioning System (HVAC)

Exclusive cooling equipment is provided in order to assure that the environment conditions of the components constituting the RHR are within the specified limits. The HVAC maintains the temperature range within 20°C (provisional) and 40°C (provisional).

6.3.4. System Architecture

(1) Redundancy

In order to satisfy LLRC1 and ensure SFC1 and SFC4, the RHR consists of three redundant divisions A, B, and C with their respective pumps, heat exchangers, strainers, piping, valves, test line, minimum flow line and instrumentation such that, single failure of any dynamic mechanical component does not prevent the delivery of the safety function.

(2) Independence

In order to satisfy LLRC2 and ensure the delivery of SFC1 and SFC4, the three divisions of the RHR are independent and separately arranged in different locations to prevent failure of a component in one of the divisions from leading to a common cause failure of all divisions.

6.3.5. System Interfaces

As claimed in LLRC3, the interfaces between SSCs of different safety classes and with the pressure

boundary are appropriately designed to ensure that any failure in a lower class item will not propagate to an item of a higher class. As a general rule, equipment providing the function to prevent the propagation of failures is assigned to the higher class. When SSCs of different classes are connected, design requirements equivalent to those for higher class are applied to the lower class. Alternatively, adequate functional isolation by means of, for example, isolation devices equivalent to higher class are considered so that the safety functions of the SSCs of higher class are not impaired of the failure of the lower SSCs.

6.3.6. Qualification

Qualification provisions are put in place to ensure that the RHR SSCs are capable of delivering the performance and reliability claimed throughout their respective operational lives and under the environmental and operational conditions claimed in order to satisfy RC2 and LLRC4.

The RHR is first designed with adequate materials, design pressure and temperatures to withstand the operational and environmental conditions upon which SFC1 and SFC4 are required without sustaining damage that could lead to the loss of the safety function. In addition, qualification procedures (prototype tests, factory acceptance tests, commissioning tests, etc.) to physically demonstrate that individual items can deliver their safety function under the required conditions with the performance and reliability claimed are implemented.

6.3.7. Hazards Protection

As claimed in LLRC5 and LLRC6, design provisions against the effects of hazards that could affect the delivery of SFC1 and SFC4 are put in place.

(1) Internal Hazards

RHR components necessary to deliver SFC1 and SFC4 are protected with specific countermeasures against the effects of internal flooding, internal fire, dropped loads, internal missiles, failure of pipes, tanks, pumps and valves (pipe whip, etc.) and internal explosions as applicable. An example of the main provisions to satisfy LLRC5 is given as follows.

(a) Piping Whip

Piping is routed as close as practicable to the building structural walls in order to protect the pipes from piping whip and other flying missiles.

(b) Fire

RHR components and containing structures are in conformance with the fire prevention specifications requirements. The RHR consists of three divisions strategically arranged in different locations and physically separated as a countermeasure against fire hazards.

(c) Internal Flooding

The RHR consists of three divisions strategically arranged in different locations and physically separated as a countermeasure against internal flooding.

(2) External Hazards

An example of the main provisions to satisfy LLRC6 is given as follows.

(a) Seismic Design

RHR Class 1 components are designed with the seismic resistance corresponding to Seismic Category 1 assigned to ensure the reliability required by SFC1 and SFC4 under design basis earthquake conditions.

(b) Design against LOOP

As described in 6.3.3 (2), each division of the RHR is automatically connected to the corresponding division of the independent Emergency Diesel Generators that provide power for all RHR components in the corresponding division which require electrical supply in the event of LOOP.

6.3.8. Examination, Maintenance, Inspection and Test (EMIT)

As claimed in LLRC7, the RHR is designed to facilitate test, maintenance and surveillance (monitoring) tasks during operation or shutdown periods to ensure the performance and reliability claimed without compromising the availability for the delivery of SFC1 and SFC4. An example of some EMIT provisions is given as follows.

(1) On-line and Outage Tests

(a) The RHR flow rate verification test is performed by drawing water from the S/P and returning it into the S/P through the test lines provided during normal operation. The system is provided with interlocks to switch to automatic control upon RHR automatic start signal during the test.

(b) Reactor water is drawn from the shutdown cooling suction lines during reactor shutdown for the functional tests and flow monitoring of the operating modes injecting water into the reactor.

(2) Maintenance

(a) RHR components inside the drywell are designed such that maintenance is facilitated during plant shutdown periods. The components outside the drywell are designed such that maintenance can be performed easily and within the minimum time during normal plant operation.

(b) The layout of RHR facilities are designed to facilitate operator's access to the maintenance and repair areas. Plant layout design considers the handling of removed parts of heavy components and machinery for maintenance and repair.

(3) Surveillance (Monitoring)

(a) An example of monitoring provisions is given in section 6.3.3 (1) (a).

(b) Reactor containment penetrations, process piping, valves and RPV outboard major equipments are arranged such that personnel and equipment required for integrity tests and surveillance can access into the area as close as possible.

(c) All active components are arranged on the external side of the PCV to allow surveillance during operation.

6.3.9. Codes and Standards

Codes and standards are selected to satisfy LLRC8 and thus ensure the reliability claimed. Mechanical equipment is designed in accordance with ISO, BS and European Standards in principle.

6.4. System Design Evaluation

As explained in section 6.3, the claims raised in 6.2 are supported with arguments, which will be further developed during Step 3. The evidence substantiating the arguments and demonstrating the achievement of the claims will be developed during Step 4 and Step 4.

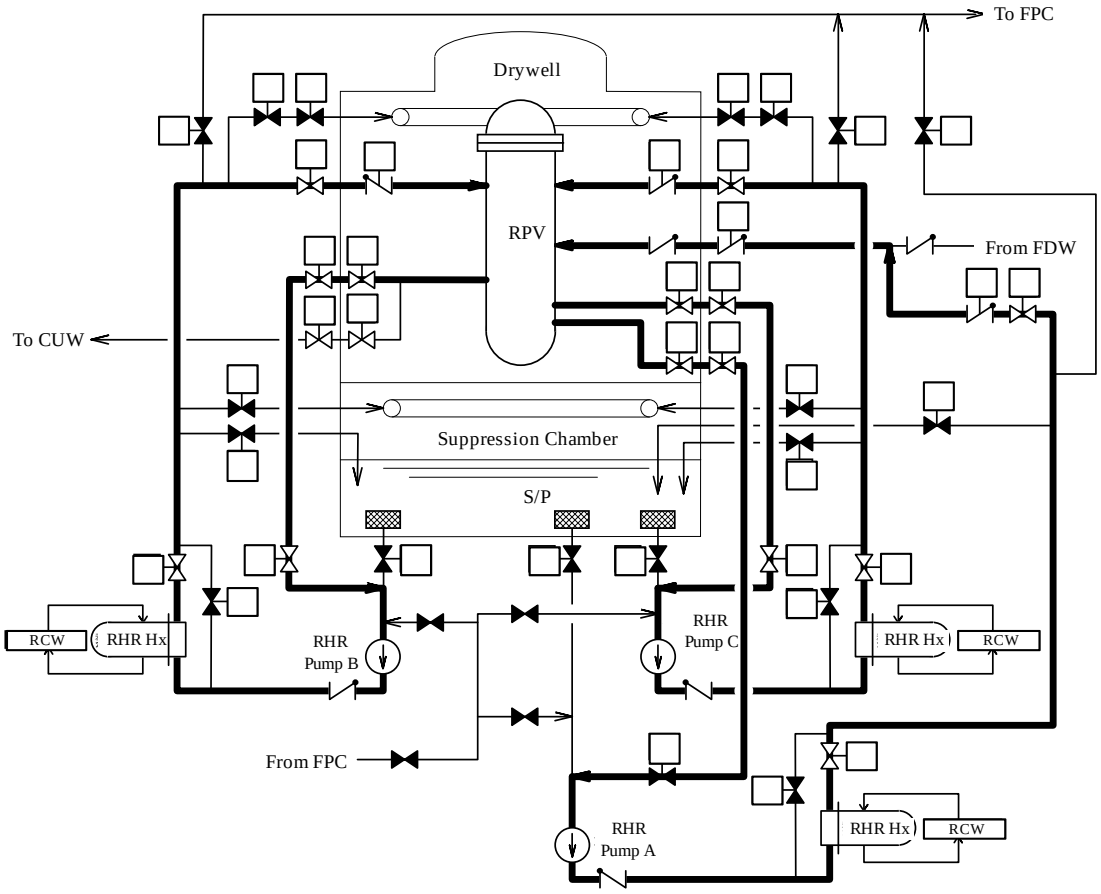


Figure 6-1 Outline of the Reactor Shutdown Cooling Mode

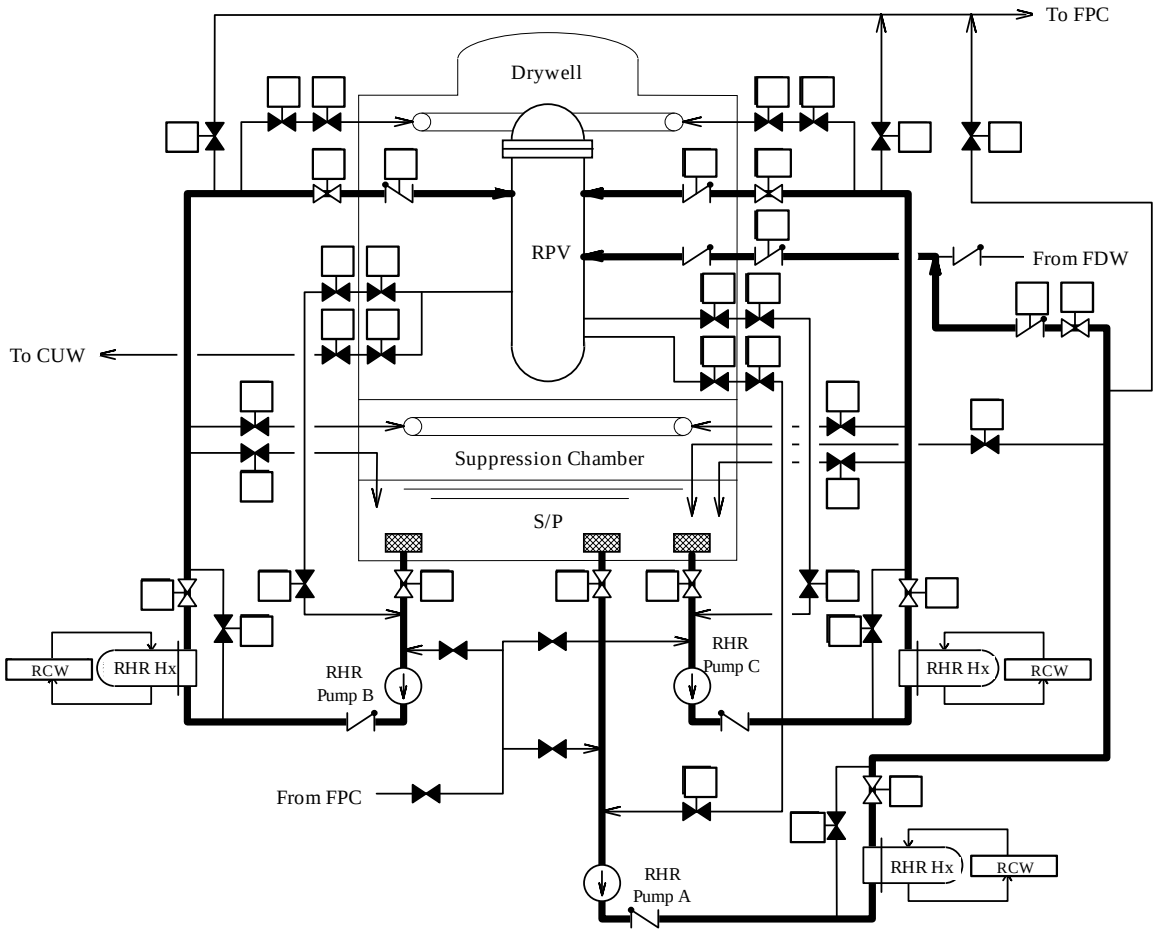


Figure 6-2 Outline of the Low Pressure Core Flooder Mode

7. Nuclear Boiler System Preliminary Safety Case

7.1. System Summary Description

This section is a general introduction to the Nuclear Boiler System (NB) where the system roles, system functions, system configuration and modes of operation are briefly described.

7.1.1. System Roles

The main roles of the NB are to transfer steam generated in the Reactor Pressure Vessel (RPV) to the turbine system for power generation and the condensed steam as feedwater back into the RPV to close the cycle; to provide isolation of the main steam to prevent radioactive releases without restriction; and to maintain the pressure of the reactor system below specified limits.

7.1.2. Functions Delivered

The NB is designed to perform the following functions:

(1) The NB transfers steam generated in the Reactor Pressure Vessel (RPV) to the turbine system to drive the turbines and generate electrical power.

(2) The NB transfers the feedwater from the turbine system into the RPV.

(3) The NB main steam lines limit the loss of coolant and the release of radioactive material from the RPV following a main steam line rupture outside the PCV.

(4) The NB provides isolation of the main steam lines to prevent radioactive releases to the surrounding areas without restriction in the event of transients and postulated accidents.

(5) The NB depressurises the RPV under transient and accident conditions for overpressure protection of the Reactor Coolant Pressure Boundary (RCPB).

(6) The NB provides reactor core cooling as part of the Emergency Core Cooling System (ECCS) as follows:

  (a) The NB depressurises the RPV through the Automatic Depressurisation System (ADS).

  (b) The NB in conjunction with the Residual Heat Removal System (RHR) provides low pressure core flooding function through the piping of RHR division A, which is connected to feedwater line A to inject water into the RPV.

  (c) The NB supplies steam through a branch from the main steam lines to the steam-driven turbine of the Reactor Core Isolation Cooling System (RCIC) pump which supplies water into the RPV through feedwater line B.

(7) In the event of Main Condenser isolation, the NB through the Safety Relief Valves provides residual heat removal after reactor shutdown in conjunction with the RCIC until the necessary pressure for RHR Reactor Shutdown Cooling Mode is reached.

(8) The NB in conjunction with the Reactor Water Clean-up System (CUW) provides clean-up of reactor coolant by returning reactor coolant into the RPV through the feedwater lines connected to the CUW.

7.1.3. Basic Configuration

The NB is divided into two subsystems, the Main Steam System (MS) and the Feedwater System (FDW). The NB subsystems should be differentiated from the Main Steam System and the Condensate and Feedwater System, which are continuation of the MS and FDW beyond the Reactor Building (R/B) and up to and including the Turbine Building (T/B).

(1) Main Steam System (MS)

The steam generated in the nuclear reactor is transferred from the RPV steam outlet nozzle to the turbine system through four main steam lines. These four main steam lines join at the upstream header of the turbine Main Stop Valve (MSV) in the T/B. The MS consists of the following major components:

(a) Four MS lines
(b) Four MS Flow Restrictors (one on each MS line)
(c) Main steam drain system
(d) 16 Safety Relief Valves (SRVs)
(e) SRV discharge lines
(f) Eight Main Steam Isolation Valves (MSIVs) (two on each MS line)
(g) Instrumentation and controllers

Figure 7-1 shows an outline of the MS.

(2) Feedwater System (FDW)

The water discharged by the FDW Pumps is transferred to the nuclear reactor through the two feedwater lines. Each feedwater line branches into three pipelines inside the PCV, with a total of six feedwater pipelines connected to the Feedwater Sparger in the RPV to equally supply water into the reactor. The FDW consists of the following major components:

(a) Two feedwater lines with their associated valves
(b) Instrumentation and controllers

Figure 7-2 shows an outline of the FDW.

7.1.4. Modes of Operation

Relevant modes of operation of the SRVs are summarised as follows:

(1) Automatic Relief Valve Function

The SRVs are forced to open by the piston actuator upon high reactor pressure signal to control excessive pressure increases in the RCPB. All 16 SRVs are provided with this function.

(2) Safety Valve Function

As a backup of the relief valve function to control excessive pressure increases in the RCPB, the SRVs are designed to open automatically after overcoming the spring force depending on the increase of pressure so that the RCPB pressure does not exceed 1.1 times the maximum design pressure in the event of abnormal transients and 1.2 the maximum design pressure in the event of accidents. All 16 SRVs are provided with this function.

(3) Automatic Depressurisation System (ADS)

As part of the ECCS, the SRVs of the ADS are forced to open by the piston actuator which is driven by the simultaneous signal of low reactor water level (water level1) and high drywell pressure to in order to quickly reduce the nuclear reactor pressure upon small and medium piping breaks. Thus, feed-water from the RHR can be injected into to the RPV as the Low Pressure Flooder Mode. Seven valves out of the 16 SRVs are provided with this function.

(4) Manual Relief Valve Function

The piston is actuated to forcibly open the SRVs by remote manual action from the Main Control Room (MCR) in order to discharge the steam generated in the RPV due to residual and decay heat into the Suppression Pool (S/P) for heat removal after reactor shutdown in the event the main condenser could not be used as the source to remove heat for any reason.

7.2. Design Bases

This section describes the claims put on the NB, from high level safety functional claims (common to the NB and all the rest of systems that in conjunction with it deliver the safety function) to low level performance claims and reliability claims that apply only to the NB in this case.

7.2.1. Safety Functional Claims

The NB has been designed to meet the following Safety Functional Claims (SFCs) (SAP EKP. 1~5):

Normal Operation:

SFC1. The MS is a principal means to deliver residual heat removal after reactor shutdown following hot standby operation in conjunction with the RCIC and RHR in the event of unavailability of the main condenser. From this perspective, the NB delivers a Category A (provisional) mitigation function, and as a principal means, the components necessary to deliver heat removal function are classified as Class 1 (provisional) safety components according to the safety categorisation and classification of UK ABWR.

SFC2. Part of the NB forms the Reactor Coolant Pressure Boundary (RCPB). Therefore, the components within the RCPB ensure the pressure integrity of the boundary and preserve reactor coolant, loss of which would lead to consequences above the BSL. From this perspective, the NB delivers a Category A preventive function and the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC3. Part of the NB forms the Primary Containment Vessel Boundary (PCV Boundary). Therefore, the components within the PCV boundary form a barrier to maintain the integrity of the boundary and thus prevent the dispersion of radioactive substances. From this perspective, the NB delivers a Category A mitigation function (containment) and the components necessary to deliver this function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC4. During normal operation the MS transfers steam generated in the RPV to the turbine side for power generation through the MS lines which contain reactor coolant beyond the RCPB limits. Rupture of these piping could lead to a loss of reactor coolant. From this perspective, the NB delivers a Category B (provisional) preventive function, and therefore, the components necessary to deliver this function are classified as Class 2 (provisional) safety components according to the safety categorisation and classification of UK ABWR.

SFC5. The FDW also operates as a normal operation system to supply feedwater into the RPV for power generation the failure of which would result into loss of feedwater flow. From this perspective, the NB delivers a Category B (provisional) preventive function, and therefore, the components necessary to deliver this function are classified as Class 3 (provisional) safety components according to the safety categorisation and classification of UK ABWR.

Fault Conditions:

SFC6. The MS is a principal means to limit the loss of coolant and the release of radioactive material from the RPV following a main steam line rupture outside the PCV to the extent that the RPV water level does not drop below the top of the active fuel until closure of the

MSIVs. From this perspective, the NB delivers a Category A mitigation function, and as principal means, the components necessary to deliver this containment function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC7. The MS is the principal means to close the MS lines to limit the release of reactor coolant and radioactive material to the surroundings in the event of a MS pipe rupture. From this perspective, the NB delivers a Category A mitigation function, and as principal means, the components necessary to deliver this containment function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC8. The MS is the principal means to deliver overpressure protection of the Reactor Coolant Pressure Boundary (RCPB) under abnormal transients and accident conditions that could put excessive pressure on the boundary. From this perspective, the NB delivers a Category A mitigation function, and as a principal means, the components necessary to deliver overpressure protection are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC9. The MS is a principal means to depressurise the RPV in order to provide reactor core cooling as part of the ECCS so that significant damage to the fuel is prevented and the reaction between the fuel cladding and the reactor coolant is sufficiently minimised in the event of infrequent faults such as Loss of Cooling Accident (LOCA). From this perspective, the NB delivers a Category A mitigation function, and as a principal means, the components necessary to deliver reactor core cooling are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

The categorisation and classification above described also applies to the support systems and components necessary to deliver the claimed safety functions unless failure does not prejudice the successful delivery. The Safety Categorisation and Classification is addressed in Step S2b document [Ref.10].

For this particular example, only claims SFC6 (limit the loss of coolant and the release of radioactive material) and SFC7 (limit the release of coolant and radioactive material) are developed. Safety functional claims SFC6 and SFC7 are high level claims that derive into lower level performance and reliability claims on the mechanical SSCs of the NB to design them so as to satisfy the high level claims.

7.2.2. Performance Claims

The following Performance Claims PC1 and PC2 are derived from safety functional claims SFC6 and SFC7 in order to ensure heat removal after reactor shutdown, limit the loss of coolant and the release of radioactive material and close the MS lines:

Fault Conditions:

SFC6. The MS is a principal means to limit the loss of coolant and the release of radioactive material from the RPV following a main steam line rupture outside the PCV to the extent that the RPV water level does not drop below the top of the active fuel until closure of the MSIVs. From this perspective, the NB delivers a Category A mitigation function, and as principal means, the components necessary to deliver this containment function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

PC1. The MS is capable of limiting the main steam flow through damaged pipes up to a 200% of the rated flow such that the RPV water level does not drop below the top of active fuel within the time required to close the MSIVs in the event of MS pipe rupture outside the PCV.

SFC7. The MS is the principal means to close the MS lines to limit the release of reactor coolant and radioactive material to the surroundings in the event of a MS pipe rupture. From this perspective, the NB delivers a Category A mitigation function, and as principal means, the components necessary to deliver this containment function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

PC2. The MS is capable of closing the MS lines within 5 seconds (including 0.5 seconds of delay to receive the closure signal) in order to control the release of reactor coolant and radioactive material in the event of damage to the pipes. At the same time, the MS is capable of closing the MS lines slowly enough so that simultaneous closure of all lines does not lead to transients that increase the pressure in the RCPB excessively.

7.2.3. Reliability Claims

The following Reliability Claims RC1 and RC2 are derived from safety functional claims SFC6 and SFC7:

SFC6. The MS is a principal means to limit the loss of coolant and the release of radioactive material from the RPV following a main steam line rupture outside the PCV to the extent that the RPV water level does not drop below the top of the active fuel until closure of the

MSIVs. From this perspective, the NB delivers a Category A mitigation function, and as principal means, the components necessary to deliver this containment function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

SFC7. The MS is the principal means to close the MS lines to limit the release of reactor coolant and radioactive material to the surroundings in the event of a MS pipe rupture. From this perspective, the NB delivers a Category A mitigation function, and as principal means, the components necessary to deliver this containment function are classified as Class 1 safety components according to the safety categorisation and classification of UK ABWR.

RC1. NB Class 1 SSCs are designed with the highest reliability to deliver SFC6 and SFC7 (SAP Paragraph 166, ERL.1).

RC2. NB SSCs not subjected to replacement are designed and qualified to be capable to deliver the performance and reliability claimed throughout an operational life of 60 years (SAP EQU.1).

In order to satisfy RC1, the following Lower Level Reliability Claims LLRC1~LLRC9 are derived from it:

RC1. NB Class 1 SSCs are designed with the highest reliability to deliver SFC6 and SFC7.

LLRC1. NB Class 1 SSCs are designed with redundancy against single failure of any dynamic component under the worst permissible system availability state so that single failure does not prevent the delivery of SFC6 and SFC7 (SAP EDR.2, EDR.4).

LLRC2. NB Class 1 SSCs are designed with independence and separation such that failure of one dynamic component does not lead to a common cause failure that could prevent the delivery of SFC6 and SFC7 (SAP EDR.2, EDR.3).

LLRC3. The mechanical interfaces between SSCs of different safety classes and the mechanical interfaces with the pressure boundary are designed such that failure in a lower class item will not propagate to NB Class 1 items and jeopardise the delivery of SFC6 and SFC7 (SAP paragraph 155).

LLRC4. NB Class 1 SSCs are designed and qualified to deliver SFC6 and SFC7 under the environmental and operational conditions in the PCV and the R/B during normal operation, during and after transient and accident conditions with the reliability claimed throughout their respective operational lives (SAP EQU.1, paragraph 163).

LLRC5. NB Class 1 SSCs are protected or designed to withstand the effects of internal hazards so that they do not affect the delivery of SFC6 and SFC7 (SAP ESS.18).

LLRC6. NB Class 1 SSCs are protected or designed to withstand the effects of external hazards so that they do not affect the delivery of SFC6 and SFC7 (SAP ESS.18).

LLRC7. NB Class 1 SSCs are designed with the capability for being tested, maintained and monitored during operation or refuelling outages to ensure the reliability claimed without compromising the availability to deliver SFC6 and SFC7 (SAP EMT.1, EMT.2, EMT.5, EMT.6).

LLRC8. NB Class 1 SSCs are designed manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to appropriate nuclear-specific codes and standards or equivalent leading to a conservative design commensurate with Class 1 reliability (SAP ECS.3, paragraph 148, 159).

LLRC9. No human intervention is necessary for approximately 30 minutes following the start of the requirement for closure of the MS lines (SAP ERL.3, ESS.8, paragraph 344).

7.3. System Design Description

This section describes the design of the NB with arguments to support the performance and reliability claims derived from SFC6 and SFC7.

7.3.1. Equipment Design and Operation

(1) Main Steam Flow Restrictors

(a) Configuration

One flow restrictor is provided on each one of the four MS lines (four in total) to limit the loss of coolant and the release of radioactive material from the RPV following a main steam line rupture outside the PCV (claim SFC6). The flow restrictors are venturi type nozzles integrated with the main steam nozzles in the RPV and without dynamic parts.

The flow restrictors are also used to measure the steam flow to initiate closure of the MSIVs when the steam flow exceeds the preselected operational limits. The RPV dome pressure and the venture throat pressure are used as the high and low pressure sensing locations for differential pressure measurements.

(b) Performance

The restrictors are designed to limit the coolant blowdown rate from the RPV in the event that a MS pipe break occurs outside the PCV to a flow rate equal to or less than 200% of the rated steam flow at 7.07 MPa [gage] upstream pressure to prevent RPV water level from dropping below the top of active fuel within the time required to close the MSIVs and thus satisfy the performance claim PC1 as described as follows.

The flow restrictors are designed with a venturi throat diameter not greater than 355mm, which is determined to satisfy the flow restriction claimed. This design limits the steam flow in a damaged MS line to less than 200% rated flow.

(2) Main Steam Isolation Valves (MSIVs)

(a) Configuration

Two MSIVs are welded in series on each of the four MS lines (eight MSIVs in total) to close them and thus limit the release of reactor coolant and radioactive material in the event of a MS pipe rupture (claim SFC7). The inboard MSIV is mounted as close as possible to the inside of the drywell, and the outboard MSIV is just outside the PCV.

Each MSIV is a Y-pattern, globe valve which permits the inlet and outlet passages to be streamlined and thus minimize the pressure drop during normal steam flow. This configuration is such that normal steam flow tends to close the valve, and higher inlet pressure tends to hold the valve closed.

The MSIV is operated by pneumatic pressure (nitrogen or gas) and by the action of compressed springs.

Attached to the upper end of the stem is a pneumatic cylinder that opens and closes the valve and a hydraulic dashpot that controls its speed. The pneumatic cylinder is supported on the valve bonnet by actuator support and spring guide shafts. Helical springs around the spring guide shafts close the valve if gas (nitrogen or air) pressure is not available.

The MSIVs automatically close when they receive one of the isolation signals indicated in section 7.3.2 (1), which indicate MS pipe damage or rupture. In addition, remote manual switches in the control room enable the operator to manually operate the valves. Operating gas is constantly supplied to the valves from the High Pressure Nitrogen Gas Supply System (HPIN) or the Instrument Air System (IA). Inboard MSIVs are supplied nitrogen gas from the HPIN and outboard MSIVs are supplied air from the IA. A pneumatic accumulator between the control valve and a check valve provides backup operating gas.

(b) Performance

The Y-pattern globe valve design is such that it allows the MSIVs to close within 5 seconds after a MS pipe break in order to satisfy the performance claimed in PC2.

The MSIVs are designed to quickly and automatically close within 3~4.5 seconds when N2 or air is admitted to the upper piston compartment to limit nuclear reactor coolant leakage and prevent damage to the reactor core if a large quantity of steam was released out of the system due to a rupture accident, etc. on the MS lines outside the PCV.

Furthermore, analysis and qualification procedures are carried out to demonstrate the closing speed and that the quickest closing time of 3 seconds is enough so that simultaneous closure of all MS lines does not lead to transients that increase the pressure in the RCPB excessively.

7.3.2. Main Support Systems

The main systems supporting mechanical SSCs for the delivery of SFC6 and SFC7 are briefly described as follows.

(1) Instrumentation and Control

The main instrumentation and control provisions related to NB operation from the performance and reliability points of view are summarised as follows.

(a) Instrumentation

As claimed in LLRC7, instrumentation is provided to measure and monitor the operating conditions of the NB components necessary for the delivery of SFC6 and SFC7 and thus ensure their performance and reliability. An example of some provisions for instrumentation is given as follows.

(i) MS flow rate is displayed and recorded in the MCR and transmitted to the feedwater control system.

(ii) Lamps are provided to indicate the position (open/closed) of all isolation valves in the MCR.

(b) Control

The signals for automatic closure of the MSIVs in order to isolate the MS lines (delivery of SFC7) are indicated here below:

(i) Low reactor water level (water level 1.5)

(ii) MS line high radioactivity

(iii) MS line high flow rate

(iv) MS line tunnel room high temperature

(v) Main condenser low vacuum level

(vi) MS line low pressure

(2) Power Supply System

The configuration of the power supply system necessary to deliver SFC7 is summarised as follows.

(a) The two solenoid pilot valves for MSIV closing are supplied power by two independent AC uninterruptible power sources (A and B). The MSIVs are fail-safe valves that in the event of loss of both power supplies close (however, they remain open if only one power source is lost).

(3) Heating Ventilating and Air Conditioning System (HVAC)

The HVAC maintains the temperature range in the R/B outside the PCV within 20°C (provisional) and 40°C (provisional) to keep the environmental conditions necessary to ensure components operability.

(4) Drywell Cooling System (DWC)

The DWC cools the atmosphere within the drywell where MS valves, FDW valves and piping within the RCPB are installed to maintain it at the specified temperature and humidity levels in order to ensure the adequate operating conditions for normal operation.

7.3.3. System Architecture

(1) Redundancy

(a) Main Steam Flow Restrictors

With regard to limiting the loss of coolant and the release of radioactive material from the RPV following a MS line rupture outside the PCV until closure of the MSIVs (SFC6), the flow restrictors are static components, and therefore, redundancy against failure is not applicable (LLRC1).

(b) MSIVs

With regard to closure of the MS lines under a pipe rupture outside the PCV (SFC7), the MS is provided with redundancy to satisfy LLRC1. Each MS line consists of two MSIVs with their respective accumulators and control units. The MSIVs are passive components to fail close in the event of loss of power or air/nitrogen pressure. The only single failure that could prevent isolation of the MS line would be the mechanical failure of one MSIV to fail close, which is the reason why two MSIVs are installed in series.

(2) Independence

(a) Main Steam Flow Restrictors

With regard to limiting the loss of coolant and the release of radioactive material from the RPV following a MS line rupture outside the PCV until closure of the MSIVs (SFC6), the flow restrictors are static components, and therefore, independence against common cause failure is not applicable (LLRC1).

(b) MSIVs

With regard to closure of the MS lines under a pipe rupture outside the PCV (SFC7), each MS line is provide with one inboard MSIV and one outboard MSIV independently arranged and physically separated by the PCV. In addition, the gas supply to keep them open is independent from two different support systems (IA and HPIN). With regard to the power supply, the valves are designed to fail safe such that common cause failure of the power sources leads to safe closure of the MSIVs.

7.3.4. System Interfaces

As claimed in LLRC3, the interfaces between SSCs of different safety classes and with the pressure boundary are appropriately designed to ensure that any failure in a lower class item will not propagate to an item of a higher class. As a general rule, equipment providing the function to prevent the propagation of failures is assigned to the higher class. When SSCs of different classes are connected, design requirements equivalent to those for higher class are applied to the lower class. Alternatively, adequate functional isolation by means of, for example, isolation devices equivalent to higher class are considered so that the safety functions of the SSCs of higher class are not impaired of the failure of the lower SSCs.

7.3.5. Qualification

Qualification provisions are put in place to ensure that the NB SSCs are capable of delivering the performance and reliability claimed throughout their respective operational lives and under the environmental and operational conditions claimed in order to satisfy RC2 and LLRC4.

The NB is first designed with adequate materials, design pressure and temperatures to withstand the operational and environmental conditions upon which SFC6 and SFC7 are required without sustaining damage that could lead to the loss of the safety function. In addition, qualification procedures (prototype tests, factory acceptance tests, commissioning tests, etc.) to physically demonstrate that individual items can deliver their safety function under the required conditions with the performance and reliability claimed are implemented.

7.3.6. Hazards Protection

As claimed in LLRC5 and LLRC6, design provisions against the effects of hazards that could affect the delivery of SFC6 and SFC7 are put in place.

(1) Internal Hazards

NB components necessary to deliver SFC6 and SFC7 are protected with specific countermeasures against the effects of internal flooding, internal fire, dropped loads, internal missiles, failure of pipes, tanks, pumps and valves (pipe whip, etc.) and internal explosions as applicable. An example of the main provisions to satisfy LLRC5 is given as follows.

(a) The MS piping is protected from potential damage due to fluid jets, missiles, reaction forces, pressures, and temperatures resulting from pipe breaks.

(2) External Hazards

An example of the main provisions to satisfy LLRC6 is given as follows.

(a) Seismic Design

NB Class 1 components are designed with the seismic resistance corresponding to Seismic Category 1 assigned to ensure the reliability required by SFC6 and SFC7 under design basis earthquake conditions.

(b) Design against LOOP

As described in 7.3.1 and 7.3.2, with regard to the delivery of SFC6, the MS Flow Resctrictors are static components that do not require power supply, and therefore, they are not affected by the occurrence of LOOP. With regard to the delivery of SFC7, the MSIVs are fail-safe valves that isolate the MS lines in the event of loss of power supply.

7.3.7. Examination, Maintenance, Inspection and Test (EMIT)

As claimed in LLRC7, the NB is designed to facilitate test, maintenance and surveillance (monitoring) tasks during operation or shutdown periods to ensure the performance and reliability claimed without compromising the availability for the delivery of SFC6 and SFC7. An example of some EMIT provisions is given as follows.

(1) On-line and Outage Tests

(a) The MSIVs can be functionally tested for operability during plant operation and refuelling outages. During refuelling outages, the MSIVs can be functionally tested and leak-tested.

(2) Maintenance

(a) Inboard MSIVs are designed such that maintenance is facilitated during plant shutdown periods. Outboard MSIVs are designed such that maintenance can be performed easily and within the minimum time during normal plant operation.

(b) The layout of NB facilities are designed to facilitate operator's access to the maintenance and repair areas. Plant layout design considers the handling of removed parts of heavy components and machinery for maintenance and repair.

(3) Surveillance (Monitoring)

(a) The MSIVs are designed such that abnormalities can be checked during operation.

(b) The MSIVs can be visually inspected during refuelling outages.

7.3.8. Codes and Standards

Codes and standards are selected to satisfy LLRC8 and thus ensure the reliability claimed. Mechanical equipment is designed in accordance with ISO, BS and European Standards in principle.

7.4. System Design Evaluation

As explained in section 7.3, the claims raised in 7.2 are supported with arguments, which will be further developed during Step 3. The evidence substantiating the arguments and demonstrating the achievement of the claims will be developed during Step 3 and Step 4.

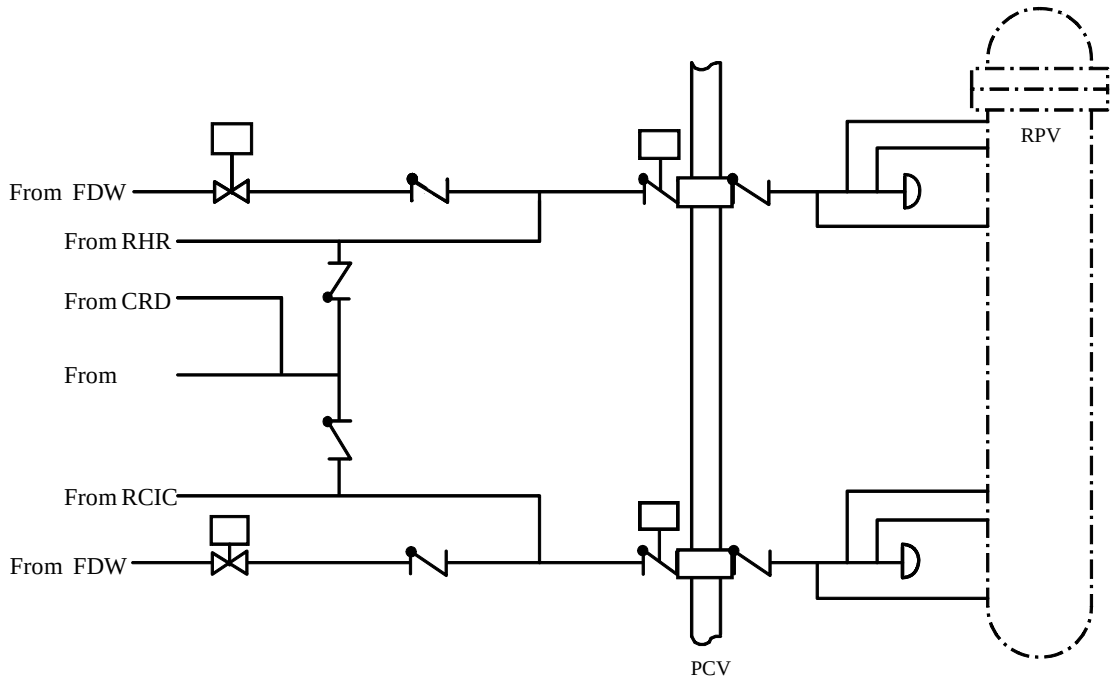


Figure 7-1 Outline of the Feedwater System

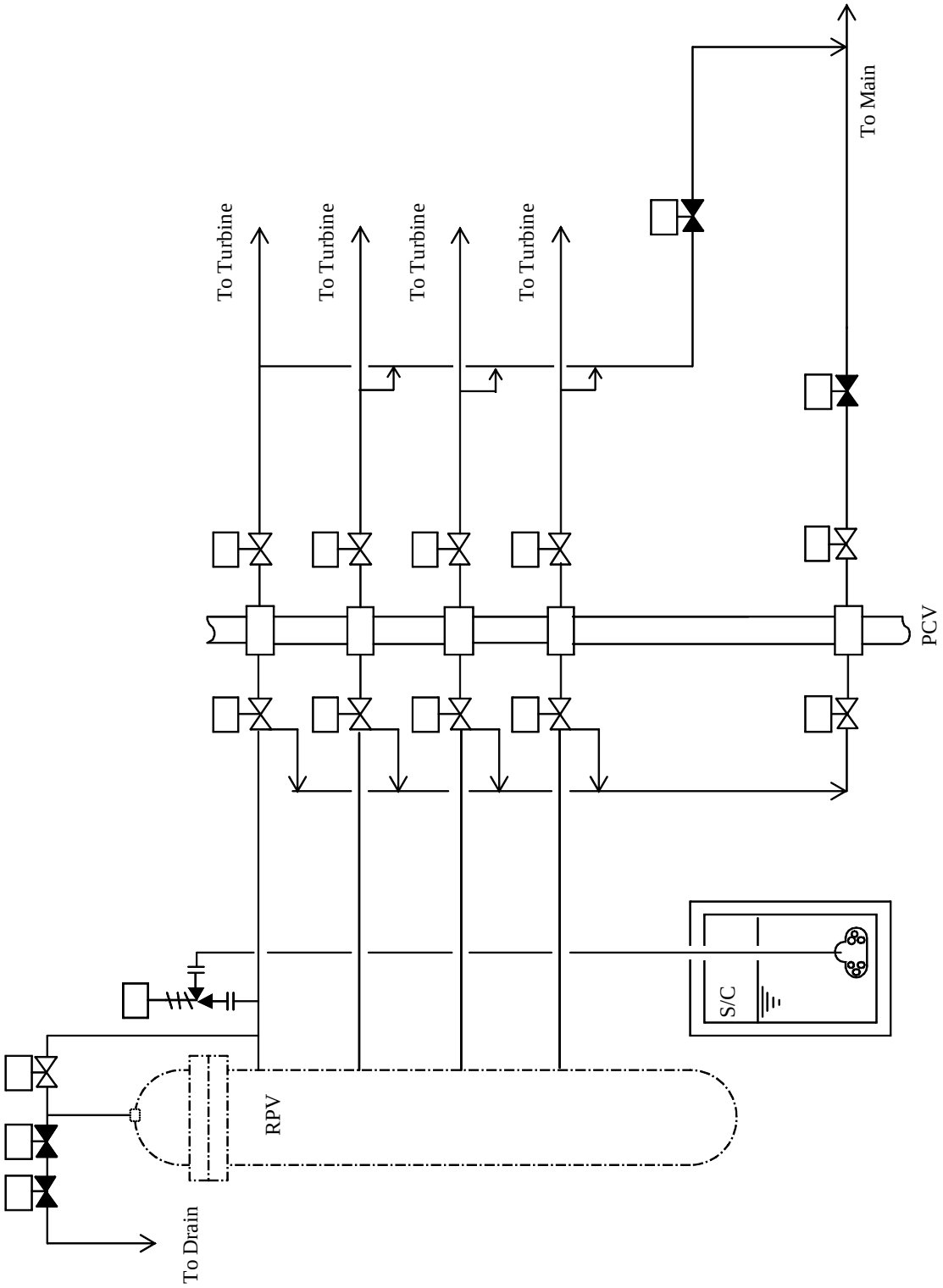


Figure 7-2 Outline of the Main Steam System

8. UK Applicable Regulations and Guidance

The nature of mechanical engineering discipline generally drives the safety case down to the component level. The safety case at this component level can be extremely wide ranging given the very large number of components, the numerous interfaces across many plant systems and disciplines. As a consequence numerous regulations and guidance can be applicable to the safety case. Therefore, in order to develop the safety case effectively, a comprehensive list of key applicable regulations and guidance in relation to specific mechanical engineering aspects will be elaborated. The following lists include some of the key applicable regulations and guidance to the mechanical engineering safety case.

8.1. Act of Parliament

(1) Health and Safety at Work etc Act 1974

(2) Nuclear Installation Act 1965

8.2. Statutory Instrument (SI)

(1) Statutory Instrument 1974 c. 37 The Health and Safety at Work etc. Act 1974

(2) Statutory Instrument 1999 No. 3242 The Management of Health and Safety at Work Regulations 1999

(3) Statutory Instrument 2007 No. 320 The Construction (Design and Management) Regulations 2007

(4) Statutory Instrument 1992 No. 3004 The Workplace (Health, Safety and Welfare) Regulations 1992

(5) Safe work equipment 1998 No. 2306 The Provision and Use of Work Equipment Regulations 1998

(6) Statutory Instrument 1998 2307 The Lifting Operations and Lifting Equipment Regulations 1998

(7) Statutory Instrument 1992 No. 2793 The Manual Handling Operations Regulations 1992 (as amended)

(8) Statutory Instrument 1997 No. 1713 The Confined Spaces Regulations 1997

(9) Statutory Instrument 2005 No. 1643 Control of Noise at Work Regulations 2005

(10) Statutory Instrument 2005 No. 1093 Control of Vibration at Work 2005

(11) Statutory Instrument 1989 No. 635 The Electricity at Work Regulations 1989

(12) Statutory Instrument 2000 No. 128 The Pressure System Safety Regulations 2000

(13) Statutory Instrument 2008 No. 1597 The Supply of Machinery (Safety) Regulations 2008 as amended 2011

(14) Statutory Instrument 1999 No. 2001 Pressure Equipment Regulations 1999
(15) Statutory Instrument 1994 No. 3260 The Electrical Equipment (Safety) Regulations 1994
(16) Statutory Instrument 1997 No. 831 Lift Regulations 1997
(17) Statutory Instrument 1996 No. 192 Equipment and Protective Systems Intended for Use in Potentially Explosive Atmospheres Regulations 1996 as amended 2001 & 2005
(18) Statutory Instrument 2006 No. 3418 Electromagnetic Compatibility Regulations 2006
(19) Statutory Instrument 1999 No. 3232 The Ionising Radiations Regulations 1999

8.3. Safety Assessment Principles for Nuclear Facilities (SAPs)

The Safety Assessment Principles (SAPs) [Ref-2] constitute the regulatory principles against which duty holders' safety cases are judged, and therefore, they are the basis for mechanical engineering safety case. General principles applicable to mechanical engineering are listed below:

Table 8.3-1 Applicable SAPs to Mechanical Engineering Safety Case (1/2)

SAP Number	SAP Title
FP	Fundamental principles
MS	Leadership and management for safety
SC	The regulatory assessment of safety cases
ST	The regulatory assessment of siting
EKP	Key engineering principles
ECS	Safety classification and standards
EQU	Equipment qualification
EDR	Design for reliability
ERL	Reliability claims
ECM	Commissioning
EMT	Maintenance, inspection and testing
EAD	Ageing and degradation
ELO	Layout
EHA	External and internal hazards
EPS	Pressure systems
EMC	Integrity of metal components and structures
ESS	Safety systems and safety-related instrumentation
ESR	Control and instrumentation of safety-related systems
EES	Essential services

Table 8.3-1 Applicable SAPs to Mechanical Engineering Safety Case (2/2)

SAP Number	SAP Title
EHF	Human factors
ENM	Control of nuclear matter
ECV	Containment and ventilation
ERC	Reactor core
EHT	Heat transport systems
ECR	Criticality safety
RP	Radiation protection
FA	Fault analysis
NT	Numerical targets and legal limits
AM	Accident management and emergency preparedness
RW	Radioactive waste management
DC	Design and operation

However, in order to develop the safety case effectively, the most appropriate SAPs in relation to specific mechanical engineering aspects are selected. A selection (not limited) of relevant SAPs to be considered for mechanical engineering safety case during Step 2 is included in Attachment-2.

For compliance with SAPs refer to Step 1 S1a Document "SAP/WENRA compliance statement" [Ref. 7].

8.4. Technical Assessment Guides (TAGs)

Technical Assessment Guides (TAGs) issued by ONR provide guidance on the interpretation and application of SAPs. Therefore, UK ABWR mechanical engineering safety case is being developed by taking TAGs into consideration.

Relevant TAGs to be considered for the mechanical engineering safety case during Step 2 are indicated in [Ref. 3].

9. Relevant International Practice

9.1. WENRA Reference Levels

ONR is a member of the Western Regulators Nuclear Association (WENRA). WENRA has developed Reference Levels, which represent good practices for existing nuclear power plants, and Safety Objectives for new reactors.

UK ABWR mechanical engineering safety case is being developed by taking into consideration WENRA good international practices. Relevant WENRA references to be considered for the mechanical engineering safety case during Step 2 are indicated in [Ref.5].

For compliance with WENRA reference levels refer to Step 1 S1a Document "SAP/WENRA compliance statement" [Ref. 7].

9.2. IAEA Standards

Since IAEA standards represent good international practice, UK ABWR mechanical engineering safety case is being developed by taking into consideration good practice reflected in IAEA standards.

Relevant IAEA standards to be considered for the mechanical engineering safety case during Step 2 are indicated in [Ref. 4].

10. Relevant Codes and Standards

Codes and standards are addressed in Step 1 S1b Document "Codes and Standards Report" [Ref.9]. The following is a summary of the relevant codes and standards applied in the mechanical engineering safety case of UK ABWR.

Mechanical equipment will be designed in accordance with ISO, British Standards (BS) and European standards in principle, or designed to standards which will be demonstrated as equivalent to ISO, BS and European standards. Pumps, diesel engine, lift equipment, etc. will be designed to ISO standards basically. However, for some ABWR specific equipment such as the Fine Motion Control Rod Drives, Hydraulic Control Units and Reactor Internal Pumps there are no dedicated standards, so this equipment will be designed to manufacturer's standards, which will be demonstrated as equivalent to the relevant nuclear standards for the class of equipment. The following table shows a list of the main mechanical codes and standards.

Table 10-1 Main Mechanical Codes and Standards

SSCs Type	Applicable Codes and Standards
Fine Motion Control Rod Drive	Manufacturer's Standards
Hydraulic Control Unit	Manufacturer's Standards
Reactor Internal Pump	Manufacturer's Standards
Fuel Handling Machine	Manufacturer's Standards
Pumps	BS EN ISO 13709 Hydraulic Institute Standards BS Pump Manufacturers Association API 610
Valves	ASME BPVC Sec. III Div. 1 ASME QME-1
Diesel Engine	ISO 8528 (series) Reciprocating internal combustion engine driven alternating current generating sets
MCR Emergency Ventilation (HVAC)	NVF/DG001 Issue 1 An Aid to the Design of Ventilation of Radioactive Area

11. References

Ref.1 New Nuclear Reactors: Generic Design Assessment Guidance to Requesting Parties, Revision 0 (2013), ONR (ONR-GDA-GD-001)

Ref.2 Safety Assessment Principles for Nuclear Facilities, Revision 1 (2006), HSE

Ref.3 Office for Nuclear Regulation Technical Assessment Guides:

1. Design Safety Assurance; TAST/057; Issue 2;
2. Safety Systems; T/AST/003; Issue 6;
3. Guidance on the demonstration of ALARP (as low as Reasonably Practicable); NS-TAST-GD-005; Rev 6;
4. Nuclear Lifting Operations; T/AST/056; Issue 002;
4. Maintenance, Inspection & Testing of Safety Systems, Safety Related Structures and Components; NS-TAST-GD-009; Rev 2;
5. Diversity, Redundancy, Segregation and Layout of Mechanical Plant; NS-TAST-GD-036; Rev 2;
6. Ventilation; NS-TAST-GD-022; Rev 2;
7. Integrity of Metal Components and Structures; NS-TAST-GD-016; Rev 4;
8. Criticality Safety; NS-TAST-GD-041; Rev 3; and
9. Containment: Chemical Plants; NS-TAST-GD-021; Rev 2.

Ref.4 IAEA Safety Standards:

1. Safety of Nuclear Power Plants: Design, Specific Safety Requirements; SSR-2/1; (2012);
2. Safety Assessment for Facilities and Activities General Safety Requirements Part 4; GSR Part 4; (2009);
3. Seismic Design and Qualification for Nuclear Power Plants Safety Guide; NS-G-1.6; (2003);
4. Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants Safety guide; NS-G-1.9; (2004);
5. Commissioning for Nuclear Power Plants Safety Guide; NS-G-2.9; (2003);

Design of Reactor Containment Systems for Nuclear Power Plants Safety Guide; NS-G-1.10; (2004);

6. A System for the Feedback of Experience from Events in Nuclear Installations Safety Guide; NS-G-2.11; (2006);
7. Aging Management for Nuclear Power Plants Safety Guide; NS-G-2.12; (2009);

8. Design of Fuel Handling and Storage Facilities for Nuclear Power Plants Safety Guide; NS-G-1.4; (2003); and
9. Maintenance, Surveillance and In-service Inspection in Nuclear Power Plants Safety Guide; NS-G-2.6; (2002).

Ref.5 WENRA Reference Levels and Safety Objectives:
1. Reactor Safety Reference Levels January 2008;
2. Safety Objectives for New Power Reactors; Study by WENRA Reactor Harmonization
3. Working group; December 2009;
4. Statement on Safety Objectives for New Nuclear Power Plants; November 2010;
5. Working Group on Waste and Decommissioning (WGWD); Waste and Spent Fuel Storage Safety Reference Levels Report; Version 2.1; February 2011; and
6. Working Group on Waste and Decommissioning (WGWD); Decommissioning Safety Reference Levels Report; Version 2.0; November 2011.

Ref.6 Step 2 Assessment Plan for Mechanical Engineering, Revision 0, ONR (ONR-GDA-AP-13-008)

Ref.7 Step 1 S1a Document “SAP/WENRA compliance statement”, Revision A, Hitachi-GE, (XE-GD-0086)

Ref.8 Step 1 C2a document “Genesis of ABWR design”, Revision A, Hitachi-GE, (XE-GD-0136)

Ref.9 Step 1 S1b Document “Codes and Standards Report”, Revision A, Hitachi-GE, (XE-GD-0103)

Ref.10 Step 1 S2b Document “Categorisation and Classification of Systems, Structures and Components”, Revision A, Hitachi-GE, (XE-GD-0104)

Ref.11 Step 1 S3b Document “Fault Studies to Discuss Deterministic Analysis, PSA and Fault Schedule Development”, Revision A, Hitachi-GE, (XE-GD-0105)

Ref.12 Step 1 S11b Document “Preliminary Safety Report on Structural Integrity”, Revision A, Hitachi-GE, (XE-GD-0113)

Ref.13 Step 1 S4b Document “Generic Site Envelope”, Revision A, Hitachi-GE, (XE-GD-0106)

Ref.14 Step 1 S10b Document “Preliminary Safety Report on Civil Engineering and External Hazards”, Revision A, Hitachi-GE, (XE-GD-0112)

Ref.15 Step 1 S6b Document “Internal Hazards Report”, Revision A, Hitachi-GE, (XE-GD-0108)

Ref.16 Step 1 S5b Document “C&I Design and Preliminary Safety Case”, Revision A, Hitachi-GE, (XE-GD-0107)

Ref.17 Step 1 S12b Document “Preliminary Safety Report on Electrical Engineering”, Revision A, Hitachi-GE, (XE-GD-0114)

Ref.18 Step 1 S9c Document “Preliminary Safety Report on Reactor Core and Fuels”, Revision A, Hitachi-GE, (XE-GD-0156)

Ref.19 Step 1 S4c Document “Preliminary Safety Report on Reactor Chemistry”, Revision A, Hitachi-GE, (XE-GD-0152)

Ref.20 Step 1 S5c Document “Preliminary Safety Report on Radioactive Waste Management System”, Revision A, Hitachi-GE, (XE-GD-0153)

Ref.21 Step 1 S6c Document “Preliminary Safety Report on Decommissioning”, Revision A, Hitachi-GE, (XE-GD-0154)

Ref.22 Step 1 S2c Document “Preliminary Safety Report on Radiation Protection Section 1 Definition of Radioactive Sources”, Revision A, Hitachi-GE, (XE-GD-0150)

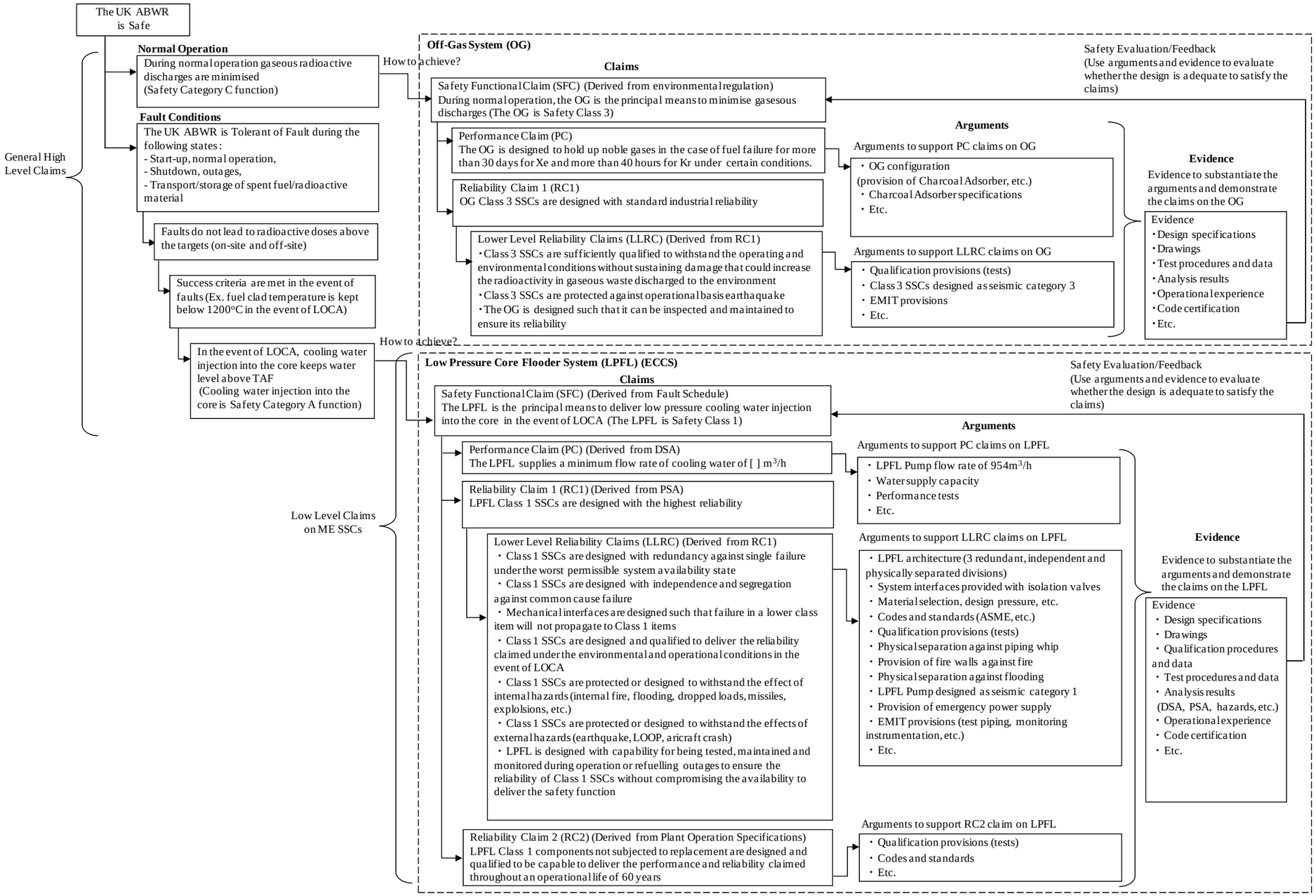
Ref.23 Step 1 S3c Document “Preliminary Safety Report on Radiation Protection Section 2 Strategy to ensure that the exposure is ALARP”, Revision A, Hitachi-GE, (XE-GD-0151)

12. Attachments

Attachment-1 Sample of CAE Flow Process

Attachment-2 Relevant SAPs for ME Safety Case during Step 2

12.1. Attachment-1 Sample of CAE Flow Process



12.2. Attachment-2 Relevant SAPs for ME Safety Case during Step 2

SAP Number	SAP Title
EKP	Key engineering principles
EKP.1	Inherent safety
EKP.2	Fault tolerance
EKP. 3	Defence in depth
EKP.4	Safety function
EKP.5	Safety measure
ECS	Safety Classification and standards
ECS.1	Safety categorisation
ECS.2	Safety Classification of structures, systems and components
ECS.3	Standards
ECS.4	Codes & standards
EQU	Equipment qualification
EQU.1	Qualification procedures
EDR	Design and Reliability
EDR.1	Failure to safety
EDR.2	Redundancy, diversity and segregation
EDR.3	Common cause failure
EDR.4	Single failure criteria
ERL	Reliability claims
ERL.1	Form of claims
ERL.3	Engineered safety features
EMT	Maintenance, inspection and testing
EMT.1	Identification of requirements
EMT.2	Frequency
EMT.5	Procedures
EMT.6	Reliability claims
ELO	Layout
ELO.1	Access
EPS	Pressure systems
EPS.1	Removal closures
EPS.3	Pressure Relief

SAP Number	SAP Title
EPS.4	Overpressure protection
EMC	Integrity of metal components and structures
EMC.1	Safety case and assessment
EMC.5	Defects
EMC.7	Loadings
EMC.11	Failure Modes
EMC.12	Brittle behaviour
EMC.22	Material compatibility
EMC.25	Leakage
EMC.26	Forewarning of failure
EMC.29	Redundancy and diversity
ESS	Safety systems and safety-related instrumentation
ESS.8	Automatic initiation
ESS.18	Failure independence
ECV	Containment and ventilation
ECV.1	Prevention of leakage
ECV.2	Minimisation of releases
ECV.3	Means of confinement
ECV.4	Provision of containment barriers
ECV.5	Minimisation of personnel access
ECV.6	Monitoring devices
ECV.7	Leakage monitoring
ECV.8	Minimising of provisions
ECV.9	Standards
ECV.10	Safety standards