Revision	Approved by	Number of Pages
000		231
Approval Date	12/11 2018	

General Nuclear System Ltd.

UK HPR1000 GDA Project

Document Reference:	**HPR/GDA/PCSR/0007**

Title:

Pre-Construction Safety Report

Chapter 7

Safety Systems

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

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

DISTRIBUTION LIST

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

MODIFICATION RECORD

Revision	Section	Page	Modification
000	ALL	ALL	First Issue

TABLE OF CONTENTS

7.1 List of Abbreviations and Acronyms

AAD	Startup and Shutdown Feedwater System [SSFS]
ACC	Accumulator
ALARP	As Low As Reasonably Practicable
APG	Steam Generator Blowdown System [SGBS]
ARE	Main Feedwater Flow Control System [MFFCS]
ASG	Emergency Feedwater System [EFWS]
ASP	Secondary Passive Heat Removal System [SPHRS]
ATWS	Anticipated Transient without Scram
BEJ	Extra Cooling System and Fire-fighting System Building
BFX	Fuel Building
BRX	Reactor Building
BSA	Safeguard Building A
BSB	Safeguard Building B
BSX	Safeguard Buildings
DBC	Design Basis Condition
DCS	Digital Control System
DEC	Design Extension Condition
DEC-A	Design Extension Condition A
DEC-B	Design Extension Condition B
DEL	Safety Chilled Water System [SCWS]
DER	Operational Chilled Water System [OCWS]
DiD	Defence in Depth
DXE	Extra Cooling Water and NI Firefighting Building Ventilation System [ECW&FFB VS]
EAU	Containment Instrumentation System [CIS]
EBA	Containment Sweeping and Blowdown Ventilation System [CSBVS]

ECS	Extra Cooling System [ECS]
EDE	Annulus Ventilation System [AVS]
EDG	Emergency Diesel Generator
EHR	Containment Heat Removal System [CHRS]
EMIT	Examination, Maintenance, Inspection and Testing
EPP	Containment Leak Rate Testing and Monitoring System [CLRTMS]
EUF	Containment Filtration and Exhaust System [CFES]
EUH	Containment Combustible Gas Control System [CCGCS]
F&B	Feed and Bleed
FLB	Feedwater Line Break
GCT	Turbine Bypass System [TBS]
HBSC	Human-Based Safety Claim
HFE	Human Factors Engineering
HPR1000 (FCG3)	Hua-long Pressurised Reactor under construction at Fangchenggang nuclear power plant unit 3
HVAC	Heating, Ventilation and Air Conditioning System
I&C	Instrumentation and Control
IB-LOCA	Intermediate Break (Loss of Coolant Accident)
ISI	In-Service Inspection
IRWST	In-containment Refuelling Water Storage Tank
IVR	In-Vessel Retention
JPI	Fire-fighting Water System for Nuclear Island [FWSNI]
KDS	Diversity Actuation System [DAS]
KRT	Plant Radiation Monitoring System [PRMS]
LB-LOCA	Large Break (Loss of Coolant Accident)
LCD	Low Pressure Full Cooldown
LHSI	Low Head Safety Injection
LOCA	Loss of Coolant Accident

LOOP	Loss of Offsite Power
MCD	Medium Pressure Rapid Cooldown
MCR	Main Control Room
MCS	Maintenance Cold Shutdown
ME	Mechanical Engineering
MHSI	Medium Head Safety Injection
MSIV	Main Steam Isolation Valve
MSL	Main Steam Line
MSLB	Main Steam Line Break
MSRCV	Main Steam Relief Control Valve
MSRIV	Main Steam Relief Isolation Valve
MSSV	Main Steam Safety Valve
NDT	Non-Destructive Testing
NI	Nuclear Island
NPSH	Net Positive Suction Head
NPSHa	Net Positive Suction Head Available
OPEX	Operating Experience
PARs	Passive Autocatalytic Recombiners
PCSR	Pre-Construction Safety Report
PSA	Probabilistic Safety Assessment
PSI	Pre-Service Inspection
PSV	Pressuriser Safety Valve
PTCN	Periodic Test Completeness Note
PTR	Fuel Pool Cooling and Treatment System [FPCTS]
PWR	Pressurised Water Reactor
RBS	Emergency Boration System [EBS]
RCD	Reactor Complete Discharge
RCP	Reactor Coolant System [RCS]

RCPB	Reactor Coolant Pressure Boundary
RCV	Chemical and Volume Control System [CVCS]
REA	Reactor Boron and Water Makeup System [RBWMS]
REN	Nuclear Sampling System [NSS]
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RIS	Safety Injection System [SIS]
RPE	Nuclear Island Vent and Drain System [VDS]
RPR	Reactor Protection System [RPS]
RPV	Reactor Pressure Vessel
RRB	Boron Heating System [BHS]
RRI	Component Cooling Water System [CCWS]
SA	Severe Accident
SAT	Service Compressed Air Distribution System [SCADS]
SB-LOCA	Small Break (Loss of Coolant Accident)
SBO	Station Black Out
SDM	System Design Manual
SEC	Essential Service Water System [ESWS]
SED	NI Demineralised Water Distribution System [DWDS(NI)]
SEO	Station Sewage System [SSS]
SEP	Potable Water System [PWS (NI)]
SER	CI Dematerialised Water Distribution System [DWDS (CI)]
SFC	Single Failure Criterion
SG	Steam Generator
SGN	Nitrogen Distribution System [NDS]
SGTR	Steam Generator Tube Rupture
SI	Safety Injection
SIH	NI Chemical Reagents Distribution System [CDS]

SLB	Steam Line Break
SSCs	Structures, Systems and Components
SSE	Safe Shutdown Earthquake
SSE1	Seismic Category 1
TEG	Gaseous Waste Treatment System [GWTS]
TLOCC	Total Loss of Cooling Chain
TLOFW	Total Loss of Feedwater
TSP	Tri-Sodium Phosphate
UK HPR1000	The UK version of the Hua-long Pressurised Reactor
VCT	Volume Control Tank
VDA	Atmospheric Steam Dump System [ASDS]
VVP	Main Steam System [MSS]

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

7.2 Introduction

The main objective of Pre-Construction Safety Report (PCSR) Chapter 7 is to present the design information of safety systems in the UK version of the Hua-long Pressurised Reactor (UK HPR1000) nuclear power plant (the general description of safety systems is presented in Sub-chapter 2.7). The safety systems in UK HPR1000 include the following:

a) Containment and Related Safety Systems;

The containment and related safety systems mainly includes the containment, Containment Heat Removal System (EHR [CHRS]), Containment Filtration and Exhaust System (EUF [CFES]), Containment Combustible Gas Control System (EUH [CCGCS]), Containment Leak Rate Testing and Monitoring System (EPP [CLRTMS]) and the Containment isolation system and Annulus Ventilation System (EDE [AVS]).

b) Engineered Safety Systems;

The engineered safety systems include the Safety Injection System (RIS [SIS]), Emergency Boration System (RBS [EBS]), Atmospheric Steam Dump System (VDA [ASDS]) and Emergency Feedwater System (ASG [EFWS]).

c) Secondary Passive Heat Removal System (ASP [SPHRS]);

d) Extra Cooling System (ECS [ECS]).

7.2.1 Chapter Route Map

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

Five high level claims and a number of level 2 claims are developed and presented in Chapter 1 to achieve the objective. This chapter supports ***Claim 3.3***.

Claim 3: *The design and intended construction and operation of the UK HPR1000 will protect the workers and the public by providing multiple levels of defence to fulfil the fundamental safety functions, reducing the nuclear safety risks to a level that is as low as reasonably practicable.*

Claim 3.3: *The design of the processes and systems has been substantiated and the safety aspects of operation and management have been substantiated.*

Claim 3.3 can be broken down into several level 3 claims; the third level claim relevant to the safety systems is ***claim 3.3.3***.

Claim 3.3.3**:** *The design of the Safety Systems has been substantiated.*

Chapter 7 will present the design information of the safety systems in the UK HPR1000 nuclear power plant. The design information is used to support ***Claim 3.3.3***. The route map for Chapter 7 is identified and presented in Appendix 7A (in Appendix 7A, X is 2 to 6 for containment and related safety systems(Sub-chapter 7.4) and 5 to 10 for other safety systems(Sub-chapter 7.5 to 7.10), the detailed information about System Design Manual (SDM) is presented in Sub-chapter 7.14) .

7.2.2 Chapter Structure

The general structure of this chapter is presented as below:

a) Sub-chapter 7.1 - Abbreviations and Acronyms- lists all the abbreviations and acronyms presented in this chapter;

b) Sub-chapter 7.2 – Introduction- introduces the route map, chapter structure, interfaces with other chapters, production strategy and general requirements of this chapter;

c) Sub-chapter 7.3 - Applicable Codes and Standards- presents the relative codes and standards to be adopted in the safety systems and its components design;

d) Sub-chapter 7.4-7.10 - All safety systems design introductions - introduces the design information of the safety systems, including design requirements, design basis, system description and operation and design substantiation etc.

e) Sub-chapter 7.11 - presents the As Low As Reasonably Practicable (ALARP)

assessment for safety systems;

f) Sub-chapter 7.12 - presents the general conclusion for the safety system and component design;

g) Sub-chapter 7.13 - Lists all identified forward action plans;

h) Sub-chapter 7.14 - Lists all the supporting references of this chapter.

The functional diagram of the safety systems is presented in Appendix 7B.

7.2.3 Interfaces with other Chapter

The Chapter 7 contains various design information. To help understand the relationship between Chapter 7 and the other chapters, the relevant interfaces are identified and are presented in Table T-7.2-1.

T-7.2-1 Interfaces between Chapter 7 and Other Chapters

PCSR Chapter	Interface
Chapter 1 Introduction	Chapter 1 provides the fundamental objective, Level 1 Claims and Level 2 Claims. Chapter 7 provides claims and arguments to support the Level 2 Claim 3.3 that is addressed in Chapter 1.
Chapter 2 General Plant Description	Chapter 2 provides a brief introduction to the safety systems. Chapter 7 provides the detailed description of the safety systems.
Chapter 3 Generic Site Characteristics	PCSR Chapter 3 provides a brief description of the heat sink associated with ECS [ECS] Chapter 7 provides the detailed description of the ECS [ECS].
Chapter 4 General Safety and Design Principles	Chapter 4 provides the general safety and design principles including the concept of Defence in Depth (DiD), safety classification of SSCs, engineering substantiation, etc. These principles will be considered in the Chapter 7 safety systems design.
Chapter 6 Reactor Coolant System	Chapter 6 provides the description of the Reactor Coolant System RCP [RCS]. Chapter 7 provides the interface information with the RCP [RCS].
Chapter 8 Instrumentation and Control	Chapter 7 provides the control function requirement that will be fulfilled by the I&C systems. Chapter 8 provides design substantiation relevant to

PCSR Chapter	Interface
	these control functions.
Chapter 9 Electric Power	Chapter 9 provides the design information relevant to the electrical power systems. General power supply information is described in Chapter 9. The power supply requirements of the safety systems are described in Chapter 7.
Chapter 10 Auxiliary Systems	Chapter 7 provides supporting functional requirements relevant to safety and operation functions for interfacing the auxiliary system. Chapter 10, the auxiliary system supports the operation of the safety systems.
Chapter 11 Steam and Power Conversion System	Chapter 7 provides supporting functional requirements relevant to safety and operation functions for interfacing Steam and Power Conversion System. Sub-chapter 11.3 , Steam and Power Conversion System supports the operation of the safety systems.
Chapter 12 Design Basis Condition Analysis	Chapter 12 provides the justification of current safety systems design in terms of the Design Basis Condition (DBC) -2/3/4 analyses. Chapter 7 provides the specific design of safety systems, which takes into consideration the fault analysis.
Chapter 13 Design Extension Conditions and Severe Accident Analysis	Chapter 13 provides the justification of current safety systems design in terms of the design extension conditions and severe accident analysis. Chapter 7 provides the specific design of safety systems, which takes into consideration the fault analysis.
Chapter 14 Probabilistic Safety Assessment	Chapter 7 provides the specific design of safety systems for the Probabilistic Safety Assessment (PSA) analysis. Chapter 14 provides the estimate feedback showing whether potential enhancement areas are presented or not.
Chapter 15 Human Factors	Chapter 15 provides the principles and methodology of Human Factor integration that will be considered in the system and component design. Chapter 7 provides the specific design of safety systems, which is taken into account for further estimates in human factors assessment.
Chapter 16 Civil Works & Structures	Chapter 16 provides the detailed description of the containment structure.

PCSR Chapter	Interface
	Chapter 7 provides the description of the containment general functional design.
Chapter 17 Structural Integrity	Chapter 17 provides the structural integrity classification and demonstration of the safety system components. Chapter 7 provides detailed design information of the safety systems and equipment.
Chapter 18 External Hazards	Chapter 18 provides an assessment of the external hazards relevant to the UK HPR1000 as well as the design principles. Chapter 7 provides the safety systems design substantiation of applied external hazard protection design principles, which is used for external hazards assessment.
Chapter 19 Internal Hazards	Chapter 19 provides an assessment of the internal hazards relevant to the UK HPR1000 as well as the design principles. Chapter 7 provides the safety systems design substantiation of applied internal hazard protection design principles, which is used for internal hazards assessment.
Chapter 20 MSQA	The organisational arrangements and quality assurance arrangements set out in Chapter 20 are implemented in the design process of the safety systems and the production of PCSR Chapter 7. Chapter 7 will meet these requirements during development of the safe case.
Chapter 21 Water Chemistry	Chapter 21 provides the water chemistry related to the safety systems. This information is related to the material selection of the safety systems. Chapter 7 will meet water chemistry requirements for material selection with regards to the safety system.
Chapter 22 Radiological Protection	Chapter 22 provides radiological protection design considerations relevant to the safety systems substantiation. Chapter 7 provides the safety systems design information used in the radiological protection design.
Chapter 24 Decommissioning	Chapter 24 provides decommissioning design considerations relevant to the SSCs of UK HPR1000 Chapter 7 provides the design information about decommissioning.

PCSR Chapter	Interface
Chapter 30 Commissioning	Chapter 30 provides the arrangements and requirements for commissioning. Chapter 7 considers the arrangements and requirements which are presented in Chapter 30.
Chapter 31 Operational Management	Chapter 31 provides the principles, requirements, and methodology for the procedures of periodic testing, inspection, maintenance and ageing and degradation. Chapter 7 provides the design substantiation relevant to periodic testing.
Chapter 33 ALARP Evaluation	Chapter 33 provides methodology for demonstrating ALARP. Chapter 7 provides the ALARP demonstration for safety systems based on these ALARP methodologies, which supports the overall ALARP evaluation for the UK HPR1000.

7.2.4 General design requirements

The design requirements are mainly derived from Chapters 4, 15, 18, 19, 30 and 31 (Including general safety and design principles, human factor and hazard protection etc.). Other requirements / principles are presented in References [1], [3] and [4].

This sub-chapter lists the design requirements to be considered in the design of the safety systems. These requirements / principles mainly include:

a) Safety Classification

The classification aims to help ensure that the item is designed, manufactured, constructed, commissioned and operated according to appropriate requirements to achieve good quality under all expected operating conditions and realise the safety functions.

The safety classification principles (including the seismic categorisation principle) presented in Chapter 4 and in Reference [1] and [3] shall be applied to the design of safety systems since the safety systems are required to perform safety functions.

b) Engineering Design Requirements

1) Reliability requirements

- Single Failure Criterion (SFC)

According to Reference [1], the reliability of items important to safety is commensurate with their safety significance. The single failure criterion

is a criterion (or requirement) applied to a system such that it must be capable of performing its task in the presence of any single failure.

The single failure includes active and passive failures. An active single failure is defined as a failure which is sufficient to invalidate the relevant safety function of a component, including the malfunction of a mechanical or electrical component which relies on mechanical movement to complete its intended function upon demand, and the malfunction of an I&C component. A passive single failure is defined as a failure which could occur in a component that does not change its state while realising its function.

The single failure criterion is applied to each safety group considered in the fault analysis. A single failure of an active component within systems that deliver FC1 or FC2 safety functions is required to be able to be tolerated at or after the postulated initiating event, when system action is demanded. A single failure of passive components within systems that deliver FC1 or FC2 safety functions needs to be assessed at the start of a transient in an appropriate manner.

The SFC and redundancy shall be applied to the safety systems components performing FC1 and FC2 safety functions.

- Independence

  According to Reference [1], independence can be accomplished in the design of systems by using functional isolation and/or physical separation. Functional isolation is used to reduce adverse effects between the elements of connected systems or systems redundantly designed. Normal operation, abnormal operation or failure of any part of these systems can arouse adverse effects.

  Physical separation shall be applied in the layout of systems as far as reasonably practicable, to reduce the potential of common cause failure due to a localised initiating event. The choice of isolation measures (compartmentalisation, distance, orientation etc.) shall take the nature of the initiating events into account.

  The safety systems shall consider the requirement of independence described in Chapter 4 and Reference [1].

- Diversity

  The concept of diversity is taken into consideration in the realisation of the safety function to reduce the risk of loss of the main protection line. Diversity should be realised by incorporating different attributes into redundant systems or components that perform the same safety function.

Such attributes can be different operating principles, different physical variables, different operating conditions, different manufacturers, etc.

In the UK HPR1000 design, failure of the main protection line is assumed in the analysis for frequent faults. Therefore, a diverse protection line should be established to achieve the nuclear safety objective.

The safety systems shall consider the requirement of diversity described in Chapter 4 and Reference [1].

- Fail-safe Design

  According to Reference [1], the fail-safe requirements shall be considered and incorporated, as appropriate, into the design of systems and components important to safety, so that the failure of them or a support feature will not invalidate the performance of the intended safety function. This principle shall be considered in safety systems design.

- Ageing and Degradation

  The general design requirements and management of ageing and degradation are shown in Chapter 4 and Chapter 31.

  Ageing and degradation (asset management) includes several aspects, such as equipment qualification, state monitoring, pre-service inspection, commissioning testing, operating and Examination, Maintenance, Inspection and Testing (EMIT) and decommissioning etc.

  According to Reference [1], the design life of items important to safety at a nuclear power plant shall be determined. Appropriate margins shall be provided in the design to take due account of relevant mechanisms of ageing, neutron embrittlement and wear out and of the potential for age related degradation. To ensure the capability of items important to safety to perform their necessary safety functions throughout their design life, measures shall be considered in the design including testing, maintenance, maintenance outages, plant states during a postulated initiating event and plant states following a postulated initiating event. This principle shall be considered in the safety systems design.

  Provisions shall be made for monitoring, testing, sampling and inspection to assess ageing mechanisms predicted at the design stage and to help to identify unanticipated behaviour of the plant or degradation that might occur in service.

  The ageing effects concerning individual components have been taken into consideration in the system design:

- Sufficient margin has been allowed for to avoid failures caused by ageing effects in the component design;
- Practical examining measures are planned to address the ageing effect during plant operation (examination, inspection, maintenance and tests);
- For replaceable parts of components, replacement plans and layout designs are properly considered.

c) Human Factors

According to Reference [1], a systematic approach needs to be applied to identify the factors which affect human performance and minimise the potential for human error throughout the entire plant lifecycle.

The design shall allocate functions properly and support personnel in fulfilling their responsibilities and performing tasks. The design also needs to identify human actions that may affect safety, analyse all tasks important to safety proportionately, and limit the likelihood of operational errors and their impact on safety.

A systematic approach on human factor integration is established and applied throughout the entire lifecycle of the UK HPR1000, especially at the design stage. Adequate consideration of human factors is given to ensure that risks from human interactions are managed to a level that is ALARP.

Human factor integration covers the plant locations where operations and maintenance activities take place. To comply with the requirements set above, the following elements will be met:

1) The design should allocate functions properly to minimise the dependence on human actions;
2) Human actions that could affect safety during normal operation, fault and accident conditions should be identified systematically. These human actions important for safety are known as Human-Based Safety Claims (HBSC);
3) Appropriate human factor analysis, including task analysis and human reliability analysis, should be performed on the HBSC to identify improvements to systems, procedures or trainings;
4) All HBSC should be classified either based on their risk significance or on the significance of the safety system affected;
5) The design should support personnel in the fulfilment of their responsibilities and in the performance of tasks by providing suitable and sufficient user interfaces and workspace.

The design of safety system (including component, layout etc.) will meet the human factors requirements presented in Chapter 15 and the relative human factors principles and specifications documents, for general plant and process operation, monitoring and control during normal operations, faults and accident conditions. In addition, the design will be assessed through a Human Factors Engineering (HFE) task analysis; especially operator actions identified as initiating events or as safety measures in the fault schedule impose specific requirements and expectations on the HMI design.

d) Autonomy

According to Reference [1], autonomy can be separated into:

1) Autonomy in respect to operators

If the plant parameters exceed the set points, the protection system shall come into action, providing automatic scram and initiation of post-trip cooling. The plant shall be designed in such a way that it meets the following autonomy objectives:

- The numerical targets of DBC-2/3/4 and DEC-A can be met without operator action from the Main Control Room (MCR) in less than 30 minutes from the first significant signal;
- The numerical targets of DBC-2/3/4 and DEC-A can be met without action outside the MCR in less than 1 hour from the first significant signal;
- No site-based light mobile equipment shall be required in less than 6 hours from accident initiation, for core damage prevention actions in the Design Extension Condition (DEC);
- No site-based light mobile equipment shall be required in less than 12 hours from accident initiation, for containment performance assurance in DEC;
- No offsite or onsite heavy mobile equipment is required in less than 72 hours in both DBC-2/3/4 and DEC;
- In addition, the containment system shall be designed in such a way that it can withstand any of the severe accidents considered in DEC, without operator action during the first 12 hours from the beginning of the severe accident conditions.

When extending the timescale in which no operator action is required, the overall safety and practicality of any provisions required should be considered and the emergency response performance that can be expected from operators should be assessed, based on information including

performance achieved in actual major emergencies. When considering extending the autonomy times, this should not be achieved by excessive complication of automatic controls.

Indications of the plant state shall be provided to the operator. It shall be assessed by the designer on a case by case basis whether or not an operator overriding of any particular automatic action should be prevented.

The time period from the initiation of any incident condition or accident condition to any serious consequences resulting from the absence of operator intervention (including local actions) shall be as long as practicable.

2) Autonomy in respect of the heat sink

Design provisions shall ensure adequate decay heat removal under DBC-2/3/4 and DEC, for 72 hours without external support. The initial means ensuring decay heat removal shall last at least 24 hours.

The design shall include provisions allowing additional means to ensure decay heat removal after 72 hours.

3) Autonomy in respect to power supply systems:

- Electrical Power Supply
  - The period of independence of the installation in relation to external electrical power supplies shall be at least 72 hours; this applies to DBC-2/3/4 and DEC;
  - The plant shall have an available power supply unit which is independent of the electrical power supply units designed for operational conditions and postulated accidents. It shall have sufficient capacity to support the following functions at the same time: remove decay heat, ensure primary circuit integrity, maintain reactor sub-criticality and monitor the unit state;
  - The batteries which perform FC1 and FC2 functions shall be sized so that their expected autonomy is at least 2 hours following any DBC-2/3/4, without recharging;
  - The batteries which perform significant safety functions shall be sized so that their expected autonomy could be 12 hours in severe accidents without recharging.
- Compressed Air

  Where required to support essential systems, the availability of compressed air reserves should be sufficient to be consistent with the timescale for the availability of the equipment.

The principles of autonomy shall be considered in safety systems design.

e) Other design requirements

1) Prevention of Harmful Interactions of Systems Important to Safety

According to Reference [1], the potential for harmful interactions of systems important to safety at the nuclear power plant that might be required to operate simultaneously shall be evaluated, and the effects of any harmful interactions shall be prevented. Protection of interfacing systems shall be considered in the safety systems design.

In the analysis of the harmful interactions, due account shall be taken of physical interconnections and of the possible effects of one system's operation, mal-operation or malfunction under local environmental conditions, to ensure that changes in environmental conditions do not affect the reliability of systems or components in functioning as intended.

If two fluid systems important to safety are interconnected, either the systems shall both be designed to withstand the higher pressure, or provision shall be made to prevent the lower pressure system from overpressure.

2) Considerations Related to the Electrical Power Grid

According to Reference [1], the functionality of items important to safety at the nuclear power plant shall not be compromised by the disturbances in the electrical power grid. This requirement shall be considered in the safety systems design.

f) Equipment Qualification

According to Reference [1], equipment qualification is implemented to verify that items important to safety are capable of performing their intended functions when necessary, and in the environmental conditions including the variations in ambient environmental conditions that are anticipated in the design for the plant. In order to achieve this objective, the operating conditions considered for equipment qualification include DBC-2/3/4 and DECs.

Equipment qualification includes:

1) Environmental qualification: to verify the performance of the equipment in the normal and accidental environmental conditions;

2) Seismic qualification: to verify the performance of the equipment during or after an earthquake.

Considering the results of fault analysis and the safety classifications, the equipment shall be qualified as follows:

1) Equipment required for environmental qualification:

   All normal operational and accident conditions are considered in the equipment qualification process. Normal operational conditions consider the lifetime of the equipment and the normal environment of the equipment locations. The variation of environmental condition arising from the accident conditions is considered in the environmental qualification.

   - Mechanical equipment and electrical equipment that perform FC1 or FC2 functions;
   - Mechanical equipment and electrical equipment that perform FC3 functions are required:
     - To maintain a safe state;
     - To protect against DEC-A and mitigate DEC-B.

2) Equipment required for seismic qualification:

   The equipment that performs the following functions should be seismically qualified: operability (O), functionality (F), integrity (I) or stability (S).

The parameters, which are related to the environmental conditions, and their impact on equipment are presented below:

1) Temperature

   Temperature can indirectly change the performance of the equipment by gradual chemical and physical processes, which is also called thermal aging.

2) Pressure

   Pressure and its rapid changes can affect the performance of equipment by exerting additional forces on the equipment. High increase of external or internal pressure may cause structural failure of the fully sealed equipment. The rapid increase of pressure may cause structural failure of the imperfectly sealed equipment.

3) Radiation

   Nuclear radiation could induce changes in the atomic and molecular structure of matter through excitation, oxidation, crosslinking, degradation and shearing process resulting in the change of equipment performance. Some changes improve the performance of the equipment, but most of the changes cause a decline in the performance.

   There exist four main types of radiation (α, β, γ and neutron) in nuclear power plants. γ radiation possesses a very strong capacity for penetration. On the contrary, the penetration capacity of β radiation is low, 1mm steel or a

10mm water layer can shield most of the β radiation. The penetration capacity of α radiation is even lower than β radiation. Neutron radiation is considered for equipment near the reactor pit.

4) Humidity

Humidity (high humidity) can directly lead to equipment performance degradation, and can make other environmental conditions worse. For example, moisture could lead to corrosion and current effects at the interfaces of different metals. Moisture could directly reduce the performance of organic materials, degrading their physical, mechanical and electrical performance and deforming them. Moisture on the surface can significantly reduce the insulation resistance and breakdown voltage of the insulation surface.

The methods of equipment qualification are presented below:

1) Type test under representative conditions, in accordance with an appropriate test standard;

2) Qualification by analysis:

- Calculation (design analysis), usually structural load analysis and mechanical analysis in accordance with an appropriate design code;
- Operating experience based;
- Analogy - by comparison with similar qualified equipment.

This requirement shall be considered in safety systems design.

g) Protection against Internal and External Hazards

According to Chapter 4 and Reference [4], the necessary capability, reliability and functionality of items important to safety shall be ensured in the conditions arising from internal and external hazards to deliver relevant safety functions. The design principles relevant to the hazards are presented in Chapter 18 and Chapter 19. These principles shall be considered in safety systems design.

The types of hazards are identified in Reference [4] for both internal hazards and external hazards. The following applicable type of hazards shall be considered in safety systems design:

1) Applicable types of internal hazards:

- Internal Fire;
- Internal Flooding;
- Internal Explosion;

- Internal Missile;
- Dropped Load;
- High Energy Pipe Failures.

2) Applicable types of external hazards:

- Earthquakes;
- External Flooding;
- Man-made and Industrial Hazards (including aircraft crash, etc.);
- Extreme Meteorological Conditions

The hazard assessment in Chapter 18 and 19 demonstrates that the safety systems are effectively protected against the identified hazards if those hazards challenge the safety objectives.

h) Commissioning

The equipment which performs safety functions in safety systems shall be effectively demonstrated via commissioning before service.

The system commissioning programme shall be established to guide the commission tests onsite. The commission content, phased approach and scope are shown in Chapter 30. The requirements and approach of commissioning presented in Chapter 30 shall be considered in safety systems design.

i) Examination, Inspection, Maintenance and Testing

According to the requirements defined in Chapter 4, the design shall facilitate the examination, maintenance, inspection and testing to ensure that the SSCs important to safety are capable of performing essential safety functions and satisfying the reliability requirement.

The above activities are commensurate with the safety class of the system since they have taken the design code requirements, reliability analysis and potential degradation mechanisms into account.

1) Examination and Inspection

According to Chapter 31, In-Service Inspection (ISI) is a preventive maintenance process involving the use of Non-destructive Testing (NDT) for nuclear pressure mechanical components at scheduled intervals during operation. The ISI shall be used to detect the anticipated degradation in good time before it compromises the structural integrity, and confirm the absence of unanticipated degradation that could lead to failure.

Pre-Service Inspection (PSI) is carried out prior to reactor start-up, and

performed with the same NDT techniques and equipment as for the future In-Service Inspection (ISI). PSI provides the baseline for the future full and partial ISI performed during outage.

The ISI requirements shall be considered in safety systems design.

2) Maintenance

According to Chapter 31, the maintenance programme for the UK HPR1000 shall cover all preventive and corrective measures, both administrative and technical. The measures are necessary to detect and mitigate degradation of functioning SSCs or to restore to an acceptable level the performance of design functions in a failed SSC.

The purpose of maintenance activities is also to enhance the reliability of equipment. The range of maintenance activities includes servicing, overhaul, repair and replacement of parts, and often, as appropriate, tests, calibration and inspection.

The maintenance types, safety requirements and maintenance strategy are presented in Chapter 31. These requirements / principles shall be considered in safety systems design.

3) Periodic Testing

According to Chapter 31, the goal of the periodic tests design is to define a comprehensive list of the periodic tests to be performed in a given system. Each periodic test defines:

- The test content and scope;
- The test frequency;
- The operating mode during which the test is to be performed.

The types of periodic tests, relevant requirements and the methodology of analysing completeness are presented in Chapter 31. These requirements / principles shall be considered in safety systems design.

j) Special Thermal-hydraulic Phenomena

Based on feedback from the operating plant, there may be some special thermal-hydraulic phenomena during the standby or operation of the system. These thermal-hydraulic phenomena may induce potential risks for the safe operation of the facility.

The thermal-hydraulic phenomena are identified and shall be considered in the system design. These thermal-hydraulic phenomena are presented below (but not limited to):

1) Phenomenon regarding the dead leg;

2) Phenomenon regarding the hot water and cold water mixing;

3) Phenomenon regarding the thermal stratification;

4) Phenomenon regarding the water hammers;

5) Phenomenon regarding the boiler effect.

The specific system design addressing these phenomena will be presented in the design substantiation sub-chapter of each system.

k) Material Selection

Material selection of systems and equipment is one of the most significant factors for the safety and economy to the nuclear power plant. Therefore, special attention shall be paid to material selection at the design stage for SSCs to carry out their duties with high reliability throughout the design life of the plant.

The principles and the approach of material selection are presented in Reference [2]. According to Reference [2], the general principles relevant to the material selection of safety systems are summarised below:

1) Material selection shall be consistent with the functional objectives of the system and equipment;

2) Material selection shall be performed in a manner in which the classification shall be reflected; different requirements shall be commensurate with the classification;

3) Materials selected for use in safety systems shall be compatible with the full range of environmental conditions which may be encountered over the plant design life;

4) Materials selected for use in safety systems shall present high functional reliability and good resistance to aging and degradation throughout the design life to mitigate the risk of performance degradation and failure of SSCs;

5) Materials selected for use in safety systems shall possess excellent manufacturability, and shall be convenient for performing processing sequences such as forging or casting, machining, heat treatment, welding and inspection;

6) Operating Experience (OPEX) and feedback shall be taken into account for material selection of safety systems;

7) Generation and transportation of source terms shall be specially considered when selecting the material to be used in safety systems, intended to

minimise the radiological dose to the workers and public when performing in-service inspection, maintenance, replacement and decommissioning.

In addition to the above factors, the selection of materials also needs to consider the influence of the reactor chemistry.

l) Insulation

During the equipment and piping system insulation design, the following issues must be paid attention to:

1) During plant normal operation without any maintenance work to be carried out, the insulation design shall reduce the heat loss as much as possible to reduce energy loss;

2) During plant maintenance or refuelling, the insulation design shall protect the workers from being scalded;

3) During plant maintenance or refuelling, the insulation design shall ensure the convenience of installation or replacement, especially for the equipment or piping systems containing radioactive material;

4) The principles of material selection presented in Sub-chapter k) shall be considered in insulation design. Moreover, flammable materials are prohibited to prevent potential internal hazards.

m) Decommissioning

Decommissioning shall be considered during design stage for the UK HPR1000. At the current stage, the general considerations of decommissioning are stated in Chapter 24 and mainly include:

1) Consideration of facilitating decommissioning;

2) Consideration of the decommissioning strategy; and,

3) Consideration of the preliminary decommissioning plan for the UK HPR1000.

The impact on decommissioning will be considered during the design of the safety systems.

7.3 Applicable Codes and Standards

The general principle relevant to the selection of appropriate standards is presented in PCSR Chapter 4. Moreover, the detailed principles are presented in Reference [1] and [5].

Wherever possible, the standards applied for engineering substantiation should be:

a) Internationally recognised in the nuclear industry;

b) The latest or currently applicable approved standards; and

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

Based on the above principles, the applicable codes and standards which are intended to be selected and used in Mechanical Engineering (ME) design are identified in Reference [6]. Therefore, the main applicable codes and standards for safety systems and components design are presented in Table T-7.3-1; more detailed information about codes and standards is contained in Reference [6] and [64].

T-7.3-1 Applicable Codes and Standards for Chapter 7

Codes and Standards	Title
IAEA, NO. SSR-2/1 (2016)	Safety of Nuclear Power Plants: Design, IAEA Specific Safety Requirements
IAEA, NO. NS-G 1.10 (2004)	Design of Reactor Containment Systems for Nuclear Power Plants
IAEA, NO. NS-G 1.9 (2004)	Design of the Reactor Coolant System and Associated Systems in Nuclear Power Plants
RCC-M 2007 Edition	Design and construction rules for mechanical components of PWR nuclear islands
RCC-M 2007 Volume H	Design and construction rules for mechanical components of PWR nuclear islands Volume H
RSE-M 2010 edition and 2012 addendum	In-service inspection rules for mechanical components of PWR nuclear islands

7.4 Containment and Related Safety Systems

7.4.1 Containment General Functional Design

7.4.1.1 Containment Safety Functions

During design basis accidents or severe accidents, the containment shall ensure the integrity of the containment structure, and maintain the general safety functions. The purpose of the containment design is to withstand the mechanical stress and thermal stress produced in accidents, and therefore to prevent radioactive releases into the environment.

The containment systems are designed to ensure the following safety functions:

a) Confinement of radioactive substances in operational states and in accident conditions;

b) Protection of the plant against external natural and human induced events;

c) Radiation shielding in operational states and in accident conditions.

7.4.1.1.1 Confinement of Radioactive Substances

The structural integrity of the inner and outer containment envelope is designed to be maintained. The specified maximum leak rate of the inner containment is not to be exceeded in any condition pertaining to design basis accidents.

7.4.1.1.2 Protection against External Events

The containment structures and systems are designed to ensure that all those components of the reactor coolant pressure boundary, that cannot be safely isolated from the reactor core and the safety systems located inside the containment necessary to keep the core in a safe state, are protected against the external events included in the design basis.

The outer containment structures can prevent the impact on internal systems due to external hazards such as aircraft crashes and explosion shock waves.

7.4.1.1.3 Biological Shielding

In operational states and accident conditions, the containment structures are designed to protect the plant personnel and the public from undue exposure due to direct radiation from radioactive material contained within the containment and containment systems.

7.4.1.1.4 Summary of Description

The UK HPR1000 containment systems consist of the containment structure and associated sub-systems and features required to operate under specific accident conditions. Depending on the plant state, the containment systems and equipment contributing to the containment function include:

a) EHR [CHRS]

   The EHR [CHRS] ensures containment heat removal.

b) EUF [CFES]

   The EUF [CFES] performs active pressure relief to lower the pressure inside the containment and maintain the integrity of the containment only during severe accident in the event of active function failure of the EHR [CHRS] and reduces the release of radionuclides to the environment.

c) EUH [CCGCS]

   The EUH [CCGCS] provides hydrogen containment and control, and reduces the risk of hydrogen combustion.

d) EPP [CLRTMS]

   The EPP [CLRTMS] ensures collection and recovery of potential leaks at

containment.

e) Containment Isolation

The containment isolation valves provide the containment isolation function during normal plant operation and postulated accidents.

f) EDE [AVS]

The EDE [AVS] ensures the sub-atmospheric pressure is maintained in the containment annulus.

The UK HPR1000 containment is a double-walled structure including an inner containment and an outer containment. The inner containment is a pre-stressed concrete structure with a steel liner. The inner containment is designed with a large free volume which ensures the necessary open space required for accident conditions, and provides a sufficient space for the lifting of main equipment (e.g., steam generator). The internal surface of the inner containment, covered by the sealing steel liner, prevents the leakage of radioactive substances. The pre-stressed system can resist the internal pressures caused by accident conditions and pressure tests.

The outer containment is located outside the inner containment. It is a reinforced concrete structure composed of a cylindrical wall and a dome.

The inner and outer containment walls are separated by an annulus. The annulus is maintained at sub-atmospheric pressure by the EDE [AVS] to enable collection and filtration of any substance leakage through the inner containment before being vented into the environment.

The detailed description of the containment structure is presented in Chapter 16.

7.4.1.2 Design Bases

a) General Parameters

The inner containment with its leak-tight steel liner and internal wall provides the main component to perform the containment function. The leak-tight steel liner on the inner containment wall provides the containment leak-tightness function and the pre-stressed concrete containment structure provides the resistance to pressure.

The general parameters of the containment are as follows:

1) The inner containment design pressure and temperature are 0.52MPa and 145°C respectively;

2) The maximum leak rate from the inner containment is 0.3% vol/day at design pressure and temperature;

3) The free volume of the inner containment is designed to accommodate the

temperature and pressure resulting from design basis accidents. For the design reference plant of UK HPR1000, the free volume of the inner containment is approximately 73500m^3, the free volume of the UK HPR1000 inner containment will be review according to the analysis results of design basis accidents.

The containment is designed to meet the safety functions. The containment is required to withstand the environmental and dynamic effects associated with both normal plant operation and postulated accidents. The containment is designed to accommodate the temperature and pressure resulting from a Loss of Coolant Accident (LOCA) and a Main Steam Line Break (MSLB).

b) Definition of the Containment Load Combinations

The containment is designed to withstand the mechanical stresses and thermal stresses produced in DBCs. Containment load combinations for the DBC sequences of LOCA and Steam Line Break (SLB) are calculated. The references related to containment load combinations in the case of LOCA and SLB are now under development and are yet to be issued.

7.4.2 Containment Heat Removal System (EHR [CHRS])

7.4.2.1 Safety Requirements

The EHR [CHRS] is required to perform the following safety functions, Reference [7] and [8]:

7.4.2.1.1 Control of Reactivity Requirements

The EHR [CHRS] is not required to perform this safety function.

7.4.2.1.2 Removal of Heat Requirements

The EHR [CHRS] shall transfer residual heat from the In-containment Refuelling Water Storage Tank (IRWST) and the containment to the ultimate heat sink during the following conditions through water spraying:

a) Small Break (Loss of Coolant Accident) (SB-LOCA) with total loss of the Low Head Safety Injection (LHSI) (during power operation) (State A);

b) SB-LOCA with total loss of the LHSI (during shutdown) (State C\D);

c) Loss of Residual Heat Removal (RHR) or failure of recovery of RHR after a Loss of Offsite Power (LOOP) accident(during shutdown) (State C\D);

d) Reactor coolant sealing leakage caused by total loss of the cooling chain (in power state) (State A);

e) Total loss of the cooling chain (during shutdown) (State D);

f) Station black out (during maintenance cold shutdown state) (State D).

Moreover, the EHR [CHRS] shall remove the residual heat from the core to the containment under Severe Accident (SA) through reactor pit flooding and injection.

7.4.2.1.3 Confinement Requirements

The EHR [CHRS] shall limit the pressure of the containment to maintain its integrity. The EHR [CHRS] transfers residual heat from the containment atmosphere to the IRWST and in the end, to the ultimate heat sink via the Component Cooling Water System (RRI [CCWS]) or the Extra Cooling System (ECS [ECS]) under conditions stated in Sub-chapter 7.4.2.1.2, to limit the containment pressure below required values and thus to maintain its integrity.

The EHR [CHRS] shall perform the containment isolation function during conditions when the EHR [CHRS] is not required.

The part of the EHR [CHRS] located outside of the containment shall prevent potential high radioactive fluid leaks after a severe accident.

7.4.2.1.4 Extra Safety Function Requirements

During refuelling of the plant, the EHR [CHRS] supplies borated water to the IRWST to maintain the inventory of the IRWST.

When the Volume Control Tank (VCT) of the Chemical and Volume Control System (RCV [CVCS]) reaches a lower level unexpectedly, the charging pump of the RCV [CVCS] takes water from the IRWST via the pipelines of the EHR [CHRS].

When one strainer of the EHR [CHRS] suction is clogged unexpectedly, the strainer can be back-flushed by itself after being switched to draw water from the adjacent RIS [SIS] strainer or from the other train of the EHR [CHRS].

Following an accident, the key parameters, such as the containment pressure, reactor pit temperature and water level, system parameters important to safety, etc. are monitored to ensure fulfilment of the required safety functions.

7.4.2.2 Design Requirements

The general design requirements of the safety systems to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to the EHR [CHRS]:

a) Fail-safe: There is no fail-safe requirement on the EHR [CHRS].

b) Autonomy in Respect to the Heat Sink: The EHR [CHRS] is not a heat sink system; therefore the autonomy of the heat sink is not applicable to the EHR [CHRS].

The substantiation analysis of EHR [CHRS] to other design requirements is shown in

Sub-chapter 7.4.2.5.

7.4.2.3 Design Bases

This Sub-chapter aims to provide the main design assumptions considered in the system design, Reference [8].

7.4.2.3.1 General Assumptions

a) Safety Classification

The EHR [CHRS] is designed to reach and maintain the final state in DEC sequence, so the spraying, back-flushing, reactor pit flooding and injection functions are classified as Function Category 3 (FC3).

The containment isolation function is used to reach a controlled state under DBC-2/3/4, whose failure will lead to serious consequences. Therefore, the containment isolation function is classified as Function Category 1 (FC1).

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment important to safety is taken into account.

The design life of the main equipment of the EHR [CHRS] is 60 years. In addition, some parts of the main equipment need to be replaced regularly during the design life.

c) Autonomy

There is no quantitative autonomy requirement for the EHR [CHRS].

d) Equipment Qualification

Active components of the EHR [CHRS] performing FC1 safety functions shall be qualified.

Active components of EHR [CHRS] performing FC3 safety functions required under DEC conditions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

Grid fluctuation is considered in the design of the EHR [CHRS]. The fluctuation of the electrical power grid may affect the ability of safety functions, especially performance of active equipment, such as the containment heat removal pumps.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in EHR [CHRS] equipment design, such as internal flooding, fire, earthquake, etc.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions such as the confinement function shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.4.2.3.2 Design Assumptions

The EHR [CHRS] transfers residual heat from the IRWST and the containment to the ultimate heat sink through spraying, reactor pit flooding and injection under DEC conditions. The requirements for the EHR [CHRS] are as follows:

a) Control of Reactivity Assumptions

There is no design assumption on the control of reactivity since the EHR [CHRS] is not required to perform this safety function.

b) Removal of Heat Assumptions

1) Heat Removal Capacity

The EHR [CHRS] is designed to remove residual heat to keep the pressure of containment below the design pressure. The required thermal load of one heat exchanger is { }when the IRWST water temperature is{ } taking into account a conservative temperature for the cooling water.

If only one train of the EHR [CHRS] is available, the IRWST temperature is maintained below { }with a thermal load of { }taking into account a conservative temperature for the cooling water.

The minimum flowrate for containment spray is { } for each train.

2) Reactor Pit Passive Flooding

During severe accidents, the EHR [CHRS] can passively flood the reactor pit with sufficient borated water. The water volume of the reactor pit flooding tank is required to guarantee continuous water flooding for at least { } after accidents.

The system is required to fill the reactor pit in { }, and then a small flowrate is required to compensate for evaporation loss in the reactor pit. The small flowrate varies over time, and the minimum flowrate is about{ }.

3) Reactor Pit Active Injection

In the long-term, the EHR [CHRS] pump takes borated water from the IRWST, flowing through the EHR [CHRS] heat exchanger, where it is cooled, and injects the water into the reactor pit. It also maintains the water level in the reactor pit taking evaporation into consideration. The minimum flowrate

is{ }.

c) Confinement Assumptions

1) Short-term Function Criteria

The EHR [CHRS] is not required to start within the 12-hour grace time after an accident. The large free volume of the containment can ensure that the containment integrity is not challenged by a design basis accident or severe accident.

Two trains of the EHR [CHRS] can reduce the containment pressure below { } within 24 hours after activation of the EHR [CHRS] spraying.

One train of the EHR [CHRS] is able to maintain the containment pressure below the design pressure of the containment.

The minimum flowrate for containment spray is { } for each train.

2) Long-term Function Criteria

During long-term operation of the EHR [CHRS], one train of the EHR [CHRS] is sufficient to maintain the containment pressure below { }.

3) Leak Tightness of the System

During the operation the EHR [CHRS], highly radioactive fluid is circulated in the system. Leak tightness is required to prevent potential leak of the radioactive fluid. The pump is provided with seal injection to prevent seal leak to the environment.

d) Extra Safety Function Assumptions

During refuelling of the plant, the borated water in the reactor pit flooding tank is discharged to the IRWST after an equivalent quantity of water has been transferred to the reactor cavity.

During operation of the EHR [CHRS], a filtration system filters the debris generated in the accident to protect the pump from debris damage.

The design of the filtration system, which is described Sub-chapter 7.5, can ensure the function and prevent clogging of the strainer. Nevertheless, back-flushing is provided as a defence in depth measure to ensure reliability of the strainer under severe accidents.

7.4.2.4 System Description and Operation

7.4.2.4.1 General System Description

The EHR [CHRS] consists of two parts: the active part and the passive part.

As introduced in Reference [7], the active part of the EHR [CHRS] has two identical trains, which are physically separated. Each train mainly consists of:

a) An intake line from the IRWST;

b) One pump;

c) One heat exchanger;

d) Three discharge lines (for spraying, reactor pit injection and strainer back-flushing).

The passive part of the EHR [CHRS] performs passive reactor pit flooding function and mainly consists of:

a) One reactor pit flooding tank;

b) Associated valves in pipelines connected to the reactor pit.

7.4.2.4.2 Description of Main Equipment

a) Containment Heat Removal Pumps

The EHR [CHRS] pumps are horizontal centrifugal pumps. The motors of the pumps are cooled by the RRI [CCWS] or ECS [ECS]. The EHR [CHRS] pumps can provide sufficient flow in the spraying modes, back-flushing mode and active reactor pit water injection mode, Reference [9].

The main parameters of the EHR [CHRS] pump are listed in Table T-7.4-1.

T-7.4-1 Main Design Characteristics of the EHR [CHRS] Pump

Parameters	**Value**	**Unit**
Type	Horizontal centrifugal pump	
Design Life	60	yr.
Nominal Flowrate	330	m^3/h
Discharge Head at Nominal Flowrate	140	mWc
Material	Stainless Steel	

b) EHR [CHRS] Heat Exchangers

The EHR [CHRS] heat exchangers are of the horizontal shell and tube type, Reference [9]. The main parameters of the EHR [CHRS] heat exchanger are

listed in Table T-7.4-2.

T-7.4-2 Main Design Characteristics of the EHR [CHRS] Heat Exchanger

Parameters	**Value**		**Unit**
Type	Shell & Tube		
	Hot Side	Cold Side	
Design Thermal Load	9.2		MW
Medium	Boric water	Demineralised Water	
Design Pressure	2.5	2.9	MPa (g)
Design Temperature	160	90	°C
Design Flowrate	330	360	m3/h
Material	Stainless Steel	Carbon Steel	

c) Reactor Pit Flooding Tank

The reactor pit flooding tank is used to discharge water passively to the reactor pit during severe accidents. The tank is made of concrete with a stainless steel liner. The tank capacity can meet the flow requirements of pit flooding for 10 hours after severe accidents. The effective volume of the reactor pit flooding tank is about 730m^3, Reference [9]. The main design characteristics of the reactor pit flooding tank are listed in T-7.4-3.

T-7.4-3 Main Design Characteristics of the Reactor Pit Flooding Tank

Parameters	**Value**	**Unit**
Type	Concrete Tank with Steel Liner	
Medium	Boric Acid	
Design Pressure	0.7	MPa (g)
Design Temperature	170	℃

Parameters	Value	Unit
Usable Volume	730	m^3
Max. Volume	750	m^3
Material	Concrete with a stainless steel liner	

7.4.2.4.3 Description of the Main Layout

The pumps, heat exchangers and connected piping on train A and B of the EHR [CHRS] are located in the Safeguard Buildings A (BSA) and B (BSB) respectively. The other parts are located in the Reactor Building (BRX), Reference [10].

In addition, the EHR [CHRS] is mainly located in the control zone due to considering the high radioactivity after the accident.

The reactor pit flooding tank is located at a high position in the BRX to meet the flow requirements of passive reactor pit flooding by gravity.

The containment spray rings are located at the dome of the containment.

There is sufficient elevation difference between the pump suction and the IRWST bottom to provide enough net positive suction head to ensure the safe operation of the EHR [CHRS] pumps.

7.4.2.4.4 Description of System Interfaces

The EHR [CHRS] interfaces with the following systems, Reference [9]:

a) Component Cooling Water System (RRI [CCWS])

   The RRI [CCWS] system provides cooling water for the EHR heat exchangers, and the motors and bearing of the EHR pumps.

b) Extra Cooling System (ECS [ECS])

   The ECS [ECS] system, as a diverse independent cooling system, provides cooling water for the EHR [CHRS] heat exchangers, and the motors and bearing of the EHR [CHRS] pumps when the RRI [CCWS] system is unavailable.

c) Safety Injection System (RIS [SIS])

   The RIS [SIS] supplies water and sump strainer for the EHR [CHRS]. The EHR [CHRS] can also take water through the sump strainer of the adjacent RIS [SIS] for back flushing.

d) Nuclear Sampling System (REN [NSS])

The REN [NSS] is used to take samples and monitor downstream of the EHR [CHRS] heat exchanger.

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

The PTR [FPCTS] is required to mix the reactor pit flooding tank by using the purification pump periodically, and is also required to purify the IRWST.

In Refuelling Cold Shutdown (RCS) condition, the PTR [FPCTS] draws water from the IRWST through the EHR [CHRS] and RCV [CVCS] pipes to fill the reactor pool.

f) NI Demineralised Water Distribution System (SED [DWDS (NI)])

The SED [DWDS (NI)] provides demineralised water for pipe flushing and the sealing the water tank of the pump.

g) Chemical and Volume Control System (RCV [CVCS])

When the volume control tank of the RCV [CVCS] has a lower level, the charging pump of the RCV [CVCS] takes water from the IRWST via the intake line provided by the EHR [CHRS], and returns water to the IRWST via the back flush line of train B of the EHR [CHRS].

h) Nuclear Island Vent and Drain System (RPE [VDS])

The RPE [VDS] is required to receive the drainage and venting of the EHR [CHRS].

i) Safeguard Building Controlled Area Ventilation System (DWL [SBCAVS])

The DWL [SBCAVS] is required to collect the discharge of the relief valve which is arranged at the outlet line of the sealing water tank of the pump. And also, the DWL [SBCAVS] is required to ensure appropriate environmental conditions for the EHR [CHRS].

More detailed interface information related to the EHR [CHRS] is detailed in the system design, Reference [9].

7.4.2.4.5 Description of Instrumentation and Control

To realise the fundamental safety functions, the EHR [CHRS] control requirements include reactor pit flooding, containment spraying, back-flushing and containment isolation, Reference [11].

a) Reactor Pit Water Flooding

Passive reactor pit flooding of the EHR [CHRS] will be manually started by the operator during severe accidents and when reactor core outlet temperature exceeds 650°C. It is designed to avoid spurious activation while the passive

reactor pit flooding subsystem is not required. In the long-term, when the reactor pit injection flooding tank generates a low water level alarm, reactor pit flooding will be switched from the passive flooding mode to the active injection mode manually.

b) Containment Spraying

Under DEC-A conditions, the operator will manually start the containment spraying mode of the EHR [CHRS] according to the water temperature of the IRWST.

Under DEC-B conditions, the operator will manually start the containment spray mode of the EHR [CHRS] following a containment high pressure signal.

c) Back-flushing

If the strainer of the EHR [CHRS] is blocked, there will be a high differential pressure alarm. The EHR [CHRS] will be switched to the back-flushing mode manually.

d) Containment Isolation

The EHR [CHRS] shall not be in operation during accidents, while containment isolation is needed. The EHR [CHRS] will receive the containment isolation signal from the Reactor Protection System RPR [RPS] and the containment isolation valves will be closed automatically.

7.4.2.4.6 System Operation

a) Plant Normal Condition

The EHR [CHRS] is in the standby state during the normal operation of the power plant.

During refuelling, the isolation valves in the line between the tank and the IRWST will be opened and will supply borated water to the IRWST to avoid a low water level. After refuelling, the borated water will be filled back in to the flooding tank from the IRWST, Reference [11].

When the volume control tank of the RCV [CVCS] is low or unavailable, the RCV [CVCS] can switch suction from the volume control tank to the IRWST through the lines provided by the EHR [CHRS].

b) Plant Accident Conditions

The system is designed to operate in the following conditions, Reference [11]:

1) SA;

2) SB-LOCA with total loss of LHSI;

3) Loss of the RHR system;

4) TLOCC;

5) SBO.

The system performs the following functions during accident conditions:

a) Reactor Pit Flooding

During severe accidents, the isolation valves at the outlet of the reactor pit flooding tank shall be opened manually to discharge water to the reactor pit by gravity, when the reactor core outlet temperature exceeds 650^{o}C. This is done to cool the reactor melt-down substances by cooling the RPV, and retain the reactor melt-down substances inside the RPV.

Small flowrate injection mode shall be switched to when the reactor pit water level reaches the required level. In the long term, the EHR [CHRS] pump will take water from the IRWST, and inject the water cooled by the EHR [CHRS] heat exchanger to the reactor pit.

b) Containment Spraying

Within the 12-hour grace time of severe accidents, the pressure and temperature in the containment can be maintained below the design limits even when the containment spray of the EHR [CHRS] is not initiated. The operator starts one or both trains of the EHR [CHRS] manually according to the containment pressure or the IRWST temperature.

Water is drawn from the IRWST and cooled by the heat exchangers before spraying to reduce the pressure and temperature in the containment.

c) Back-flushing

The EHR [CHRS] can still operate in the back-flush mode to flush the strainer, even if the strainer is blocked.

7.4.2.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). Review of consistency of the system design against the design principles is currently being undertaken. Detailed information on the system is presented in Reference [7], [8], [9], [10] and [11]. Furthermore, the design substantiation of the EHR [CHRS] will be evaluated in the fault study in Chapter 13.

7.4.2.5.1 Compliance with Safety Requirements

a) Compliance with Control of Reactivity Requirements

The EHR [CHRS] does not contribute to this safety function directly.

b) Compliance with Removal of Heat Requirements

After DEC accidents, the EHR [CHRS] can transfer residual heat from the IRWST to the ultimate heat sink, with the cooling of the EHR [CHRS] heat exchanger via the RRI [CCWS] or ECS [ECS] system.

The severe accident condition is the bounding condition of the EHR [CHRS]. The temperature of the hot side of heat exchanger is no more than { }, and the rated flow is { }. The temperature of the cold side inlet of heat exchanger is { }, and the flowrate is { }

If one train of the EHR [CHRS] operates, the water temperature of the IRWST does not exceed { }.
When the EHR [CHRS] operates in the containment spraying together with the small flow active reactor pit injection mode, it will remove a heat load of { } to maintain containment pressure and temperature below the design value.

The design of the reactor pit flooding tank is based on the safety analysis results which require the reactor pit to be quickly filled within { }, and then compensate for the evaporation loss in the small flow passive reactor pit flooding mode. The mobile devices of the plant will be ready after { }, so from a conservative point of view, the passive reactor pit flooding mode can be maintained for at least { } after the flooding activation. The available water volume and flow rate are able to guarantee the demand of filling the reactor pit within half an hour and providing continuous flooding for { } after the flooding activation. The usable volume of the reactor pit flooding tank is about { }.

In the long-term phase, the EHR [CHRS] pump injects borated water into the reactor pit. The designed flowrate is no less than { }which maintains the water level in the reactor pit while taking evaporation into consideration.

If the passive reactor pit flooding mode is not available, the reactor pit level is less than { }, or the water level of flooding tank cannot meet the requirements of the safety function, the active reactor pit injection mode can be started manually, and the flow rate shall be set according to the level measurement and specific situation.

c) Compliance with Confinement Requirements

The EHR [CHRS] can transfer the containment heat to the IRWST and finally to the ultimate heat sink to limit pressure in the containment and ensure the containment integrity through containment spraying. The containment integrity is ensured during this 12h-period even without containment spray by the EHR [CHRS] system. The 12h-period grace time is substantiated in Sub-chapter 13.6.

The designed minimum flowrate for containment spray is 300m^3/h for each train.

Under the DEC conditions, activating two containment spray trains of the EHR [CHRS] after a 12h grace period can decrease the pressure of the containment below 0.2MPa abs within 24 hours, and activating one containment spray train of the EHR [CHRS] after a 12h grace period can keep the pressure of the containment below the containment design pressure (0.52MPa abs).

During long-term operation of the EHR [CHRS], one train of the EHR [CHRS] can keep the pressure of the containment below 0.2MPa abs.

The EHR [CHRS] can be isolated by the motor-driven containment isolation valve outside of the containment and the check valve inside of the containment during accidents in which the EHR [CHRS] is not required to operate.

The part of the EHR [CHRS] located outside of the containment can be a part of the containment to maintain the containment integrity and contain the radioactive substances during accidents. For the EHR [CHRS] pump, seal injection with a pressurised tank is provided for the pump to prevent pump seal leak to the environment. The heat exchangers are of the tube-shell type with a higher pressure in the shell side, which can prevent the radioactive fluids in the tube side from releasing to the environment. The isolation valves in the EHR [CHRS] are equipped with bellow seals for the valve stems to prevent potential leaks. Moreover, water level sensors are provided in the pump rooms to monitor potential leaks in the area and to remind the operator to isolate the damaged EHR [CHRS] train.

d) Compliance with Extra Safety Function Requirements

A gravity draining pipeline to the IRWST with a motor-drive valve and manual valve is provided for the reactor pit flooding tank. In order to ensure the water volume of the IRWST when refuelling, the reactor pit flooding tank is discharged to the IRWST by opening the isolation valve downstream of the draining pipeline, Reference [11].

The filtration system for the EHR [CHRS] is described in Sub-chapter 7.5, which can ensure to protect the pump from debris clogging.

The back-flushing pipes for the strainers are provided in the EHR [CHRS] as a defence in depth measure. In case of strainer clogging, the back-flushing line can take water from the RIS [SIS] strainer (or the other train of EHR [CHRS] strainer) to back-flush the strainer, Reference [11].

7.4.2.5.2 Compliance with Design Requirements

The system is described in the basis of the design of the HPR1000 (FCG3). A review of consistency of the system design against the design principles is currently being undertaken.

a) Compliance with Safety Classification

The safety categorisation of EHR [CHRS] functions is listed in Table T-7.4-4 and the safety classification of the main components in Table T-7.4-5.

The EHR [CHRS] is designed to withstand a Safe Shutdown Earthquake (SSE). The main components are classified as SSE1 and the seismic category is shown in T-7.4-5.

T-7.4-4 System Function Categorisation for EHR [CHRS]

System Function	**Function Category**
Containment Spray	FC3
Reactor pit flooding	FC3
Back-flushing	FC3
Containment Isolation	FC1

T-7.4-5 Component Classification for EHR [CHRS]

Component	**Function Class**	**Design Provision Category**	**Design Provision Class**	**Seismic Category**
Containment Isolation Valves	F-SC1	DPA	B-SC2	SSE1
Isolation Valve	F-SC3	DPA	B-SC2	SSE1
Containment Heat Removal Pump	F-SC3	DPA	B-SC2	SSE1
Heat Exchanger (Hot Side)	F-SC3	DPA	B-SC2	SSE1
Isolation Valve of RRI [CCWS]	F-SC1	DPL	B-SC3	SSE1
Isolation Valve of ECS [ECS]	F-SC3	DPL	B-SC3	SSE1

b) Compliance with Reliability

1) Redundancy and SFC

The principle of SFC is presented in Sub-chapter 7.2.4.

Equipment that performs an FC1 function (containment isolation) in the EHR [CHRS] meets the SFC. One motor-driven isolation valve and one check valve can isolate the containment penetration in a SFC.

The intake line between the IRWST and the angular globe valve is designed with double-layer casing pipe (safety guard tube).

2) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The EHR [CHRS] consists of two independent trains, and each of them is located in a separate safeguard building. Therefore, the design of the EHR [CHRS] meets the requirements of independence. More layout information is provided in Reference [10].

3) Diversity

The principle of diversity is presented in Sub-chapter 7.2.4.

The cooling system and heat sink of the EHR [CHRS] is diversely designed to ensure the reliability of the EHR [CHRS]. The heat exchangers and pumps of the EHR [CHRS] can be cooled by the RRI [CCWS] or ECS [ECS] during accidents.

The reactor pit can be passively flooded or actively injected to ensure In-Vessel Retention (IVR).

4) Fail-safe Design

There is no fail-safe designed equipment in the EHR [CHRS] system.

5) Ageing and Degradation

The plant design life is 60 years. Some components may need replacing at the end of their individual design life. The management of equipment ageing and degradation follows the arrangement of asset management stated in Sub-chapter 7.2.4.

The performance of equipment is guaranteed through life examination, inspection maintenance and testing, as well as through monitoring during normal operation. Thus it can be ensured that ageing effects will not compromise safety performance. The detailed design arrangement around EMIT and equipment monitoring is presented in Reference [11].

The system layout design as part of the detailed design stage can ensure the

accessibility and requirements for safety equipment in-service inspection and periodic tests including the necessary Non-Destructive Testing (NDT). This includes the requirements of emergency and scheduled maintenance on the SSCs as well. Detailed layout information is presented in Reference [10].

7.4.2.5.3 Compliance with Human Factors

The design requirements relevant to the human factors are stated in Chapters 4. The principles and methodology are stated in Chapter 15.

Neither system design nor control function design of the EHR [CHRS] requires short term operator intervention. No operator action is required within 30 minutes after the initial event. The large free volume of the containment allows a 12-hour grace time without operation of containment spraying.

To avoid spurious actuation of the reactor pit passive flooding, the isolation valves for flooding are closed and the motors of the valves are disconnected from power during plant normal operation.

To avoid spurious containment spraying, the isolation valves for containment spraying are closed and disconnected from power during plant normal operation.

It should be noted that there are operator actions occurring during plant normal operation or accident conditions (including plant start-up, shutdown, and maintenance or testing etc.). Relevant human actions important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of Chapter 15. Relevant evaluated reports will be provided as references of Chapter 15.

7.4.2.5.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in Reference [1]. The EHR [CHRS] system satisfies the requirements through the following design:

1) No operator intervention is required in the first 30 minutes under accident conditions;

2) All valves performing safety functions are electric valves which can be operated from the MCR; no human operation is required outside of the MCR in less than 1 hour from the first significant signal.

The design of the EHR [CHRS] fulfils the principles via control function design, Reference [11].

b) Autonomy in Respect to the Heat Sink

This is not applicable since the EHR [CHRS] is not a heat sink system.

c) Autonomy in Respect to Power Supply Systems

All of the electrical equipment supporting the safety functions can be powered by appropriately qualified emergency power provisions.

Each EHR [CHRS] train is supplied by an electrical division and backed-up by the Emergency Diesel Generators (EDGs). Besides, the EHR [CHRS] are powered with Station Black Out (SBO) diesel generators when the EDGS fails.

The EHR [CHRS] is also supplied by mobile diesel generators to ensure its function under extreme accidents such as Fukushima.

The isolation valves of the passive flooding and containment penetrations are also supplied by 12h battery.

7.4.2.5.5 Compliance with Other Design Requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

1) Provide adequate isolation (e.g. using double isolating valves) between the EHR [CHRS] and interfacing systems;

2) The design pressure of the isolation valves between the EHR [CHRS] and the interface systems adopts the larger pressure.

b) Considerations Related to the Electrical Power Grid

According to Reference [1], the functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid.

The fluctuation of the electrical power grid mainly affects the functional capability of EHR [CHRS] pumps. The pumps flow will change with the fluctuation of the power grid. As a result, the design of EHR [CHRS] pumps considers the influence of grid fluctuation, Reference [9].

Based on UK context relevant to the electrical power grid, an evaluation will be carried out during the GDA progress.

7.4.2.5.6 Compliance with Equipment Qualification

All components required to perform the safety functions shall be capable of operating under normal conditions and accident conditions, which requires the components to withstand the most adverse ambient environment.

Each safety classified component, as shown in Table T-7.4-4, is qualified in accordance with the requirements described in Chapter 4.

The documents relevant to the equipment qualification will be developed during Step

4 of GDA.

7.4.2.5.7 Compliance with Hazard Protection

Reference [10] provides the measures to protect the EHR [CHRS] against internal and external hazards. The hazard analysis in Chapter 18 and 19 demonstrates that the EHR [CHRS] is effectively protected during the hazards identified.

7.4.2.5.8 Compliance with Commissioning

Commissioning is carried out for the EHR [CHRS] to valid its functionality. The following tests need to be validated:

a) System flushing;

b) Instrumentation and control channel tests;

c) Valve tests;

d) Containment heat removal pumps and motors test;

e) Containment heat removal heat exchangers test;

f) The EHR [CHRS] system overall function test.

A supporting document will be produced to further describe the commissioning of the EHR [CHRS].

7.4.2.5.9 Compliance with Examination, Inspection, Maintenance and Testing

a) System Surveillance

The main monitoring methods of the EHR [CHRS] are as follows:

1) Reactor pit spurious injection;

2) Status of the reactor pit flooding tank;

3) Leakage of the safeguard building;

4) Status of the pump sealing water tank;

5) Status of the containment heat removal pump.

b) Maintenance and Replacement

Preventive maintenance of the EHR [CHRS] is scheduled during the operation of the power plant to ensure the availability of the system.

The EHR [CHRS] can be repaired in the long term after a severe accident and the pipeline that needs repairing can be flushed and decontaminated before maintenance to ensure the safe access of personnel.

c) Periodic Test

Periodic tests to be performed on the EHR [CHRS] are as follows:

1) Containment heat removal pump start-up and flow test

This periodic test aims to confirm that the containment heat removal pump can be started correctly from the main control room and to measure the flowrate of the containment heat removal pump in the back flush mode to verify that the flowrate is not lower than what is required for back flushing. Furthermore, the performance curve of the pump is verified to meet the safety requirements by measuring the flowrate and head of the pump.

2) The operability test of electric isolation valve

This periodic test aims to ensure that the valve is properly switched on and off, and meets the closing time requirements.

d) In-service Inspection

The pumps, some valves, the reactor pit flooding tank and pipelines of the EHR [CHRS] need to be inspected in service to ensure that the pressurised equipment can maintain a satisfactory safety level when it is pressurised continuously.

7.4.2.5.10 Compliance with Special Thermal-Hydraulic Phenomena

As stated in Sub-chapter 7.2.4, the thermal-hydraulic phenomenon in EHR [CHRS] design is considered as follow:

The hydraulic phenomena are considered carefully to ensure function reliability of the system and prevent any challenges in performing the safety function. Especially, the water hammer in the EHR [CHRS] is limited. The bypass line downstream the EHR [CHRS] pump is designed to avoid water hammer phenomena. It needs to close the electric isolation valve downstream of the EHR [CHRS] pump before starting it and water flows through the bypass line to prevent water hammer on the spraying nozzles.

7.4.2.5.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and also engineering experience, the materials selected for the main components is presented in Sub-chapter 7.4.2.4.2.

7.4.2.5.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

The main equipment of the EHR [CHRS] is in a standby state during normal operation and no local operation is required on the EHR [CHRS] after an accident. Therefore, no insulation is provided for the EHR [CHRS].

7.4.2.5.13 Compliance with Decommissioning

The design of the EHR [CHRS] takes into account the impact on decommissioning, including the following measures:

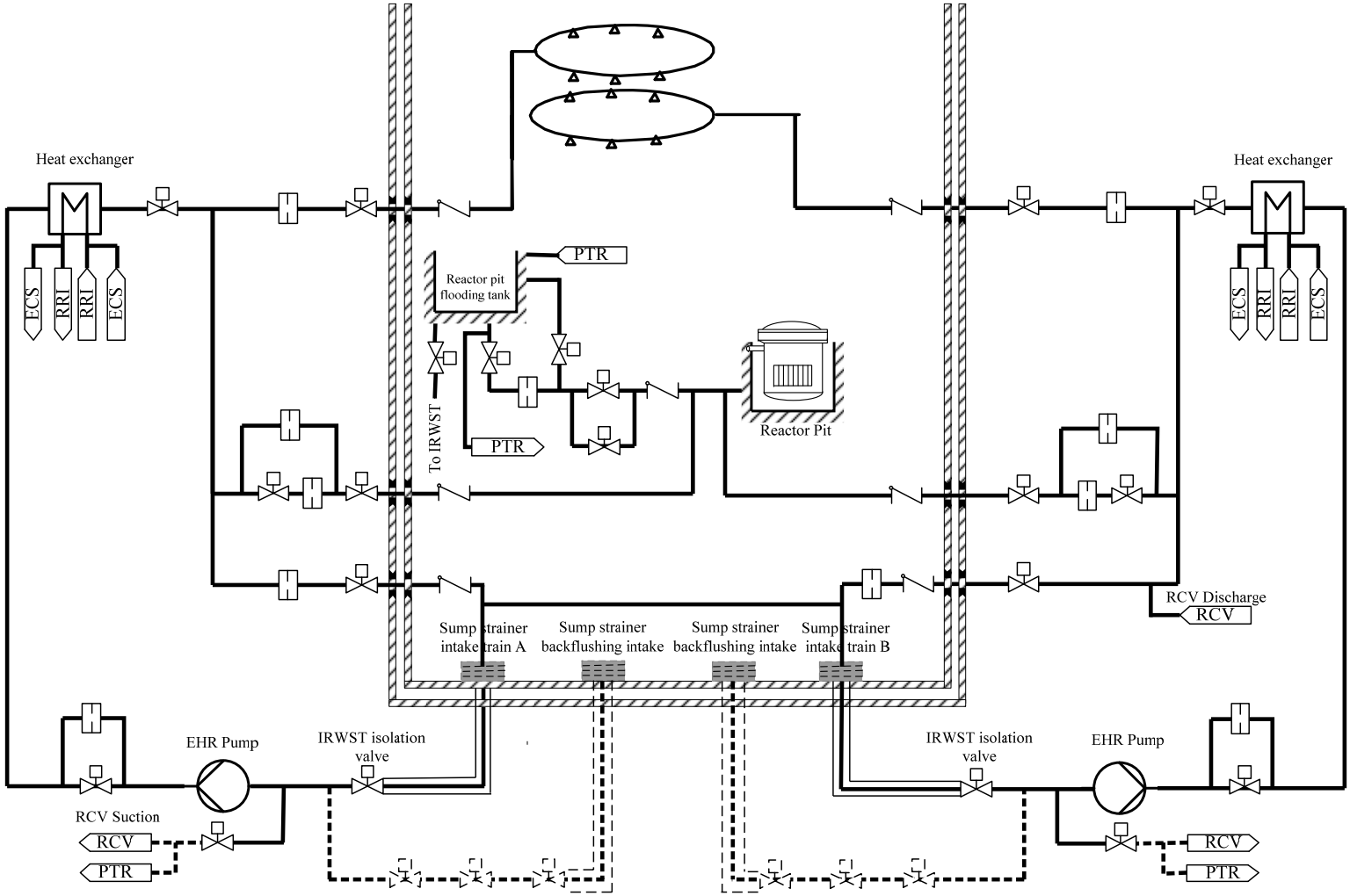
a) The main equipment is equipped with a drainage pipe, which can be used to empty the equipment;

b) The passive flooding tank is equipped with a steel liner to ensure convenience for decontamination;

c) The layout of the EHR [CHRS] considers decommissioning, such as the accessibility of personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.4.2.6 Functional Diagrams

The simplified functional diagram of the EHR [CHRS] is shown in Figure F-7.4-1. The detailed system functional diagrams are presented in Reference [12].



F-7.4-1 Simplified Functional Diagram of EHR [CHRS]

7.4.3 Containment Filtration and Exhaust System (EUF [CFES])

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

7.4.3.1 Safety Requirements

The EUF [CFES] is required to perform the following safety functions, Reference [14]:

7.4.3.1.1 Control of Reactivity Requirements

The EUF [CFES] is not required to perform this safety function.

7.4.3.1.2 Removal of Heat Requirements

The EUF [CFES] is not required to perform this safety function directly, although a small amount of heat is removed by the exhaust function indirectly after a severe accident.

7.4.3.1.3 Confinement Requirements

The EUF [CFES] is required to perform the containment isolation function to confine the radioactive substances released within the containment in normal operation, DBC-2/3/4 and DEC-A conditions, for which the EUF [CFES] is not required to operate.

The EUF [CFES] is required to perform active pressure relief to lower the pressure inside the containment and maintain the integrity of the containment only during a severe accident (in case of the active function failure of EHR [CHRS]).

7.4.3.1.4 Extra Safety Function Requirements

The EUF [CFES] has no extra safety function requirements.

7.4.3.2 Design Requirements

The general design requirements of the safety systems to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to EUF [CFES] system:

a) Fail-safe: There is no fail-safe requirement on the EUF [CFES].

b) Autonomy in Respect to the Heat Sink: The EUF [CFES] system is not a heat sink system; therefore the autonomy of the heat sink is not applicable to the EUF [CFES] system.

c) Considerations Related to the Electrical Power Grid: Not applicable since the EUF [CFES] has no power supply requirement for its safety function.

The substantiation analysis of the EUF [CFES] system to other design requirements is

shown in Sub-chapter 7.2.5.

7.4.3.3 Design Bases

The EUF [CFES] is designed to mitigate the severe accident in which the EHR [CHRS] fails to operate. After 24 hours following a severe accident, the EUF [CFES] is permitted to start manually when the pressure inside containment is higher than its design pressure (0.52MPa abs). The start time of the EUF [CFES] will be determined on site based on the site situation.

This sub-chapter aims to provide the main design assumptions considered in the system design, Reference [14].

7.4.3.3.1 General Assumptions

a) Safety Classification

The containment isolation functions are used to reach a controlled state under DBC-2/3/4, so the part of the EUF [CFES] system that performs containment isolation functions under DBC-2/3/4 is Function Category 1 (FC1).

The part of the EUF [CFES] system that performs filtration and exhaust functions under severe accidenst is Function Category 3 (FC3).

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which is important to safety will be taken into account.

The design life of the main equipment of the EUF [CFES] system is 60 years. In addition, some parts of the main equipment need to be replaced regularly during the design life.

c) Autonomy

There is no quantitative autonomy requirement for the EUF [CFES] system.

d) Equipment Qualification

Active components of the EUF [CFES] system performing an FC1 or FC2 safety function will be qualified.

Active components of EUF [CFES] system performing an FC3 safety function required under DEC conditions will be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

Not applicable since the EUF [CFES] has no power supply requirement for the safety function.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in the EUF [CFES] equipment design, such as internal flooding, high energy pipe failure, and earthquake.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions such as the confinement function shall be performed under an earthquake event. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.4.3.3.2 Design Assumptions

a) Control of Reactivity Assumptions

The EUF [CFES] does not contribute to the safety function of reactivity control.

b) Removal of Heat Assumptions

The EUF [CFES] does not perform the residual heat removal function directly.

c) Confinement Assumptions

After 24 hours of severe accidents, the EUF [CFES] can be permitted to be put into operation for containment depressurisation if the EHR [CHRS] fails and the pressure in the containment exceed the design pressure.

The characteristics of the gaseous mixture inside the containment before filtration are described in Table T-7.4-6. The gas inside the containment is vented through the EUF [CFES] and purified through a filtration vessel after a severe accident.

1) The system starts when the pressure of the containment is approximately 0.52MPa abs, and the mass flowrate is approximately 4kg/s;

2) The isolation valves of the containment can be closed manually by the operator to switch off the system when the finishing operating conditions are met.

The gas in the containment meets the requirements in Table T-7.4-7 after being filtered by the EUF [CFES].

T-7.4-6 Features of In-containment Gas Mixture before Filtration

Composition ---Water vapour, N_2, O_2, H_2, other gases	
Maximum flow of the gas mixture	4 kg/s

Composition ---Water vapour, N_2, O_2, H_2, other gases	
Pressure (absolute)	0.52 MPa
Temperature	140-180°C

T-7.4-7 Requirements after the EUF [CFES] Filtration

d) Extra Safety Function Assumptions

The EUF [CFES] has no extra safety function requirements.

7.4.3.4 System Description and Operation

7.4.3.4.1 General System Description

As introduced in Reference [13], the EUF [CFES] is mainly composed of one set of a filtration assembly, two containment isolation valves, one safety valve, one backwash valve, one restriction orifice, one rupture disk and one set of Plant Radiation Monitoring System (KRT [PRMS]) instrumentation, lines (pipes, equipment and the related instruments) that inject various materials (including demineralised water and nitrogen) into the filtration assembly, lines for the effluent to return to the containment, valves, and water level and pressure instrumentations.

The gas from containment passes through the inlet line of the EUF [CFES] to the two containment isolation valves, then goes through one set of the filtration assembly, the flow restriction orifice and the rupture disk in turn, and then reaches the stack. Figure F-7.4-2 gives the simplified flow diagram of the system.

The filtration assembly is connected to the nitrogen supply line, the supplement water line which comes from chemical liquid tank, the drainage line, and the return line for the radioactive effluents to return to the containment.

The EUF [CFES] is designed to reduce the radioactivity released to the environment to the minimum. Therefore, one set of radiation monitor equipment is arranged to monitor the radiation before the radioactive substances are released to the stack.

The main material of the components in the EUF [CFES] is austenitic stainless steel.

7.4.3.4.2 Description of Main Equipment

a) Containment Isolation Valves

   Two containment isolation valves are arranged in the inlet line of the EUF [CFES] outside of the containment to perform the safety function of containment isolation. The isolation valves of the containment can be driven manually behind the shield wall through a remote transmission mechanism, Reference [15].

b) Filtration Assembly

   One set of the filtration assembly is arranged for the EUF [CFES]. Chemicals in the filtration assembly are used to retain the radioactive aerosol and iodine in the exhaust gas effectively during the discharge of the system, Reference [15].

c) Restriction Orifice

   One restriction orifice is arranged in the outlet line of the filtration assembly to restrict the discharged gas flow of the EUF [CFES], so that the filtration assembly can operate at a relatively broad pressure range of the containment and maintain the best filtration performance, Reference [15].

d) Rupture Disk

   One rupture disk is arranged behind the restriction orifice, the rupture setpoint of which maintains the nitrogen supplying protection function under standby status of the EUF [CFES]. After the system is put into operation, the rupture disk will be opened and the filtered gas is discharged into the atmosphere when the system pressure reaches the setpoint of the rupture disk, Reference [15].

7.4.3.4.3 Description of Main Layout

The main equipment of the EUF [CFES] is located in the Fuel Building (BFX), Reference [16].

The line inlet of the EUF [CFES] inside the containment is arranged to avoid the hydrogen-concentrated zone (at larger spaces of the containment).

The containment isolation valves are physically separated to keep a certain distance from each other and can be operated remotely. That means the operator can operate the valves manually from behind the shield wall. Shield walls are arranged in the equipment room, and the local instrumentations and hand wheels of remote manual valves are installed behind the shield walls.

7.4.3.4.4 Description of System Interfaces

The EUF [CFES] is interfaced with the following systems [9]:

a) Plant Radiation Monitoring System (KRT [PRMS])

   A set of radiation monitors are arranged on the discharge pipes in front of the chimney for monitoring the radioactivity dose in the exhaust gas of the EUF [CFES].

b) Containment Leak Rate Testing and Monitoring System (EPP [CLRTMS])

   It is used for leak recovery of the containment isolation valves in the EUF [CFES].

c) NI Demineralised Water Distribution System (SED [DWDS(NI)])

   Upon internal inspection of combined filter unit during system commissioning and normal operation, the SED [DWDS (NI)] supplies demineralised water to the EUF [CFES].

   After the filtration and exhaust operations, the SED [DWDS (NI)] is used to clean and refill the combined filter unit.

d) Stack

   The end of vent pipe of the EUF [CFES] is open to the atmosphere through the stack.

e) Nuclear Island Vent and Drain System (RPE [VDS])

   During normal operation, it is used to receive the effluent of deteriorated acceptable liquid from the combined filter unit, the discharge from the chemical mixing tank during commissioning tests and dosage.

7.4.3.4.5 Description of Instrumentation and Control

The EUF [CFES] is manually controlled and the pressure and water level are monitored in the EUF [CFES]. More information is provided in Reference [17].

7.4.3.4.6 System Operation

a) Plant Normal Condition

The EUF [CFES] is on standby during plant normal operation, Reference [17].

The operator can carry out periodic sampling of the solution inside the filtration assembly to maintain the proper composition of the mixture. The operating personnel can also add chemicals into the filtration assembly when necessary.

The system is filled with nitrogen, in the lines from the containment isolation valves to the rupture disk and in the space of the vessel during standby periods.

b) Plant Accident Conditions

The isolation valves of the containment can be opened manually to start the system when the containment pressure is higher than the design pressure (0.52 MPa abs) after 24 hours following severe accidents.

The operator can manually open the valves behind the shield wall when the KRT [PRMS] radioactivity sensor confirms the accessibility. The local remote control device is designed to be separate from the high radioactive areas and to provide sufficient protection, Reference [17].

The operator can shut down the system by closing the isolation valves of the containment manually when the shutdown instruction is received or the pressure is decreased to { }.

The solutions with strong radioactivity accumulated in the filtration assembly will represent a potential radioactive source after system shutdown. The high radioactive fluids in the filtration assembly can be transported back to the containment to prevent the diffusion of the potential radioactive pollution source.

7.4.3.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). Detailed design of the system is presented in Reference [13], [14], [15], [16] and [17]. Furthermore, design substantiation of the EUF [CFES] will be estimated in the fault study in Chapter 12 and 13.

7.4.3.5.1 Compliance with Safety Requirements

a) Control of Reactivity Requirements

The EUF [CFES] does not contribute to this safety function.

b) Removal of Heat Requirements

The EUF [CFES] does not perform the residual heat removal function directly.

c) Confinement Requirements

During normal operation of the plant, the EUF [CFES] performs the containment isolation function to confine the radioactive substance in the containment through isolation of the two manual valves in DBC-2/3/4 and DEC-A conditions. The two valves are monitored in the main control room.

The EUF [CFES] can be used to perform active pressure relief to lower the pressure inside the containment and maintain the integrity of the containment after severe accidents. Moreover, the filtration vessel installed in the pressure relief lines can filter the radioactive substances in the discharged gas to ensure that the radioactive substances released into the environment can be maintained at a level that is as low as reasonably practicable.

d) Compliance with Extra Safety Function Requirements

The EUF [CFES] has no extra safety function requirements.

7.4.3.5.2 Compliance with Design Requirements

a) Compliance with Safety Classification

The safety classification of the EUF [CFES] functions is listed in Table T-7.4-8 and the safety classification of main components in Table T-7.4-9. The EUF [CFES] is designed to withstand a SSE. The main components are classified as SSE1 in Table T-7.4-9.

T-7.4-8 System Function Categorisation for EUF [CFES]

System Function	**Function Category**
Containment isolation	FC1
Filtration and discharge	FC3

T-7.4-9 Components Classification for EUF [CFES]

Component	**Function Class**	**Design Provision Category**	**Design Provision Class**	**Seismic Category**
Containment penetration and isolation valves	F-SC1	DPA	B-SC2	SSE1
Filtration instruments	F-SC3	NC	NC	SSE1
Discharge lines/Valve	F-SC3	NC	NC	SSE1

b) Compliance with Reliability

1) Redundancy and SFC

The principle of SFC is presented in Sub-chapter 7.2.4.

Containment isolation is a FC1 function, therefore, the redundancy and SFC shall be applied to the containment isolation valves. Two manual valves with remote control device are provided to ensure containment isolation.

2) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The independence of the location of the containment isolation valves has been considered.

3) Diversity

Not applicable.

4) Fail-safe Design

There is no fail-safe designed equipment in the EUF [CFES] system.

5) Ageing and Degradation

The plant design life is 60 years. Some components may need replacing at the end of their individual design life. The management of equipment ageing and degradation follows the arrangement of asset management stated in Sub-chapter 7.2.5.

The performance of equipment is guaranteed through life examination, inspection maintenance and testing, as well as monitoring during normal operation. Thus it can be ensured that ageing effects will not affect safety performance. The detailed design arrangement on EMIT and equipment monitoring is presented in Reference [17], [11] and [33].

The system layout design as part of the detailed design stage will ensure the accessibility and requirement for safety equipment in-service inspection and periodic tests including the necessary NDT are met. This includes the requirements of emergency and scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [16] and [10].

7.4.3.5.3 Compliance with Human Factors

The design requirements relevant to the human factors are stated in Chapters 4. The principles and methodology are stated in Chapter 15.

Neither system design nor control function design of EUF [CFES] requires short term operator intervention. No operator action is required within 30 minutes after the initial

event. The EUF [CEFS] is only required 24h after a severe accident.

It should be noted that there are operator actions occurring during plant normal operation or accident conditions (including plant start-up, shutdown, and maintenance or testing etc.). Relevant human actions important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of Chapter 15. Relevant evaluated reports will be provided as references of Chapter 15.

7.4.3.5.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

   No operator intervention is required in the first 30 minutes and 1 hour under accident conditions for EUF [CFES] operation.

   The design of the EUF [CFES] fulfils these principles via the control function design, Reference [17] .

b) Autonomy in Respect to the Heat Sink

   Not applicable since the EUF [CFES] is not a heat sink system.

c) Autonomy in Respect to Power Supply Systems

   There is no requirement for the power supply except got the instrumentation used only in normal operation.

7.4.3.5.5 Compliance with Other Design Requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

   Not applicable since the EUF [CFES] has no direct interface with other systems.

b) Considerations Related to the Electrical Power Grid

   Not applicable since the EUF [CFES] has no power supply requirement for the safety function.

7.4.3.5.6 Compliance with Equipment Qualification

Each safety classified component, as shown in Table T-7.4-9, will be qualified in accordance with the requirements described in Chapter 4 with the main considerations being the environmental qualification, irradiation dose qualification and seismic qualification.

The documents relevant to equipment qualification will be developed during Step 4 of GDA.

7.4.3.5.7 Compliance with Hazard Protection

The measures protecting the EUF [CFES] against internal and external hazards are presented in Reference [16]. The hazard analysis in Chapter 18 and 19 demonstrates that the EUF [CFES] is effectively protected during the hazards identified.

7.4.3.5.8 Compliance with Commissioning

The performance of the EUF [CFES] will be validated through the following commissioning tests, Reference [17] :

a) Initial inspection test;

b) Analog Monitoring and Control channel test;

c) Starting test.

A supporting document will be produced to further describe the commissioning of the EUF [CFES].

7.4.3.5.9 Compliance with Examination, Inspection, Maintenance and Testing

a) System Surveillance

The monitoring means of the EUF [CFES] are as follows:

1) Combined filter unit level;

2) System pressure.

b) Maintenance and Replacement

The scheduled maintenance of the EUF [CFES] is performed during the refuelling stage.

c) Periodic Test

Periodic tests of the EUF [CFES] include:

1) Internal and external inspection of the vessel in the combined filter unit;

2) Pressure test for the vessel in the combined filter unit;

3) Visual inspection of the rupture discs;

4) Inspection of the safety valves;

5) The chemical analysis for the solution in the combined filter unit;

6) The functional inspection, including manual operation of remote controls and transmission of alarms to the main control room for the containment isolation valves;

7) Tightness inspection of the containment isolation valves;

8) The functional inspection, including manual operation of remote controls for the effluent backflow isolation valves;

9) The functional inspection for other valves;

10) Leak rate test of containment penetrations.

d) In-service Inspection

The containment penetration pipelines of the EUF [CFES] needs inspecting to ensure that the pressurised equipment can maintain a satisfactory safety level when it is pressurised continuously.

7.4.3.5.10 Special Thermal-Hydraulic Phenomena

Not applicable

7.4.3.5.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and also from engineering experience, the material selected for the main component is presented in Sub-chapter 7.4.3.4.2.

7.4.3.5.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

The main equipment of the EUF [CEFS] is in the standby state during normal operation and local operation is only conducted through a remote control device following a severe accident. Therefore, no insulation is provided for the EUF [CEFS].

7.4.3.5.13 Compliance with Decommissioning

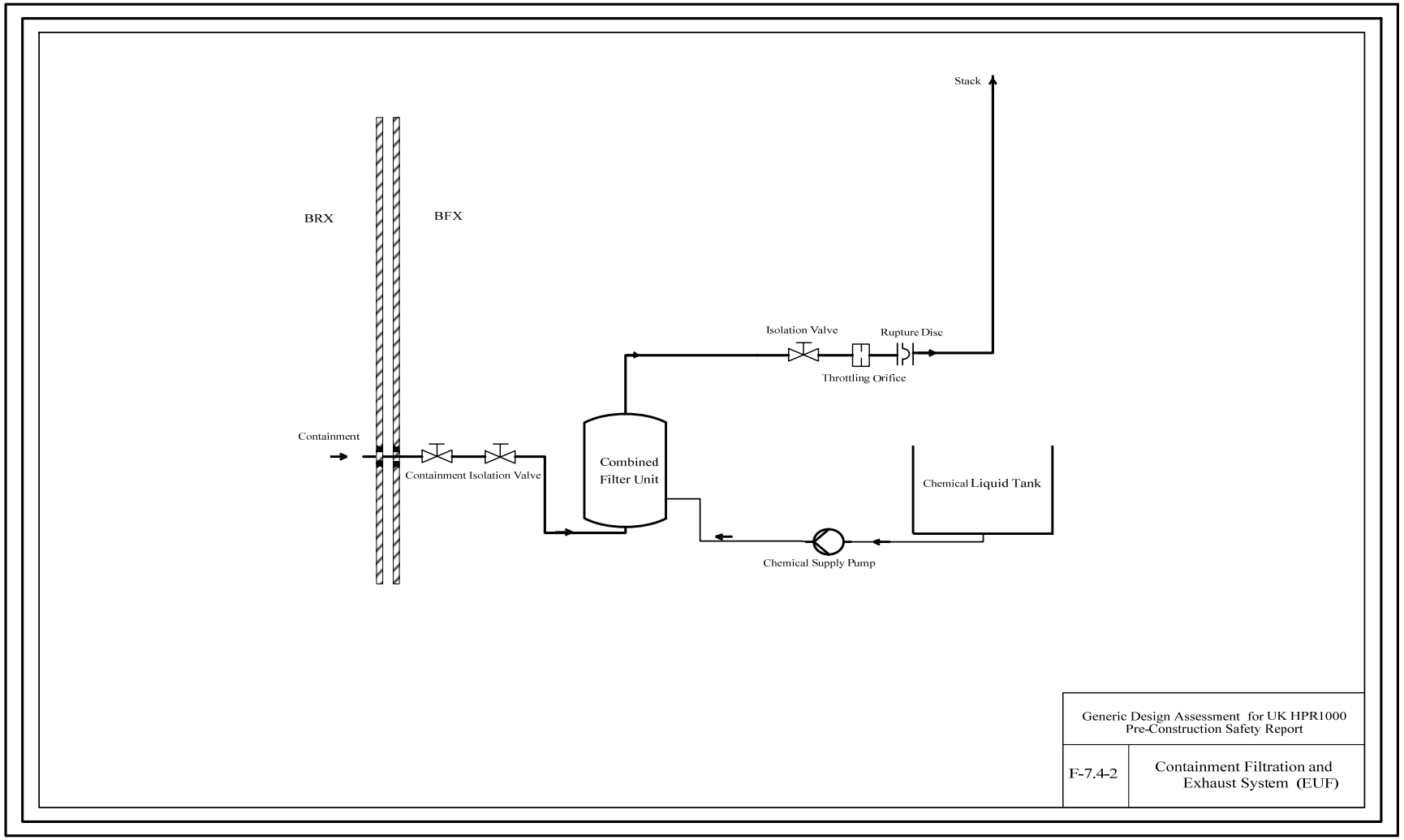
The design of the EUF [CEFS] takes into account the impact on decommissioning, including the following measures:

a) The main equipment is equipped with a drainage pipe, which can be used to empty the equipment;

b) The layout of the EUF [CEFS] considers decommissioning, such as the accessibility of personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.4.3.6 Functional Diagrams

The simplified functional diagram of the EUF [CFES] is shown in Figure F-7.4-2.



F-7.4-2 Simplified Functional Diagram of the EUF [CFES]

7.4.4 Containment Combustible Gas Control System (EUH [CCGCS])

7.4.4.1 Safety Requirements

7.4.4.1.1 Control of Reactivity Requirements

The EUH [CCGCS] is not required to perform this safety function.

7.4.4.1.2 Removal of Heat Requirements

The EUH [CCGCS] is not required to perform this safety function.

7.4.4.1.3 Confinement Requirements

The EUH [CCGCS] is required to meet the safety objective of the confinement of radioactive substances by reducing the hydrogen concentration in the containment. This is to ensure that the containment integrity and leak tightness can be maintained after a LOCA or design extension conditions.

7.4.4.1.4 Extra Safety Function Requirement

The EUH [CCGCS] is required monitor the hydrogen concentration in the containment at different locations during a severe accident.

7.4.4.2 Design Requirements

The general design requirements of the safety systems to be considered are shown in Sub-chapter 7.2.4. The following requirements are not applicable to EUH [CCGCS]:

a) Fail-safe: There are fail-safe requirements on the EUH [CCGCS], so fail-safe is not applicable to the EUH [CCGCS].

b) Autonomy in Respect to the Heat Sink: The EUH [CCGCS] is not a heat sink system; therefore the autonomy of the heat sink is not applicable to the EUH [CCGCS].

c) Considerations Related to the Electrical Power Grid: Not applicable since the EUH [CCGCS] has no active components.

d) Diversity: There is no diversity requirement as the EUH [CCGCS] has no active components.

The EUH [CCGCS] is required to meet the design requirements shown in Sub-chapter 7.2.4.

7.4.4.3 Design Bases

The passive hydrogen recombiners shall be designed to ensure that the average concentration of hydrogen in the containment generated from 100% zirconium-water reaction can be limited to below 4% within 12 hours after severe accidents.

The hydrogen monitoring system can be used to monitor the hydrogen concentration in the containment under severe accident conditions.

This Sub-chapter aims to provide the main design assumptions considered in the system design, Reference [19].

7.4.4.3.1 General Assumptions

a) Safety Classification

In design basis accidents, the hydrogen generated in the containment is removed by two sets of FC2 passive hydrogen recombiners to eliminate the possibility of hydrogen combustion or detonation risk that could cause a loss of containment integrity.

Under Design Extension Condition B (DEC-B), the hydrogen generated from the core melting is removed by 27 sets of FC3 passive hydrogen recombiners to prevent a hydrogen detonation that could cause a loss of containment integrity, Reference [19].

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which is important to safety will be taken into account.

The design life of the main equipment of the EUH [CCGCS] is 60 years. In addition, some parts of the main equipment need to be replaced regularly during the design life.

c) Autonomy

There is no quantitative autonomy requirement for the EUH [CCGCS].

d) Equipment Qualification

Components of the EUH [CCGCS] performing a FC2 safety function shall be qualified.

Components of the EUH [CCGCS] performing a FC3 safety function required under DEC conditions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

Not applicable.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in EUH [CCGCS] equipment design, such as internal flooding, fire, and earthquake, etc.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions such as the confinement function shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.4.4.3.2 Design Assumption

a) Control of Reactivity Assumptions

The EUH [CCGCS] does not perform the safety function of reactivity control.

b) Removal of Heat Assumptions

The EUH [CCGCS] does not perform the safety function of residual heat removal.

c) Confinement Assumptions

After a design basis accident, the EUH [CCGCS] shall limit hydrogen to a global containment concentration of less than 4%, which is lower than the flammability level of hydrogen with oxygen.

After a severe accident event, the EUH [CCGCS] shall control hydrogen concentration levels consistent with the limitations imposed by regulatory requirements. Specifically, the capacity design of Passive Autocatalytic Recombiners (PARs) can guarantee that the average concentration of hydrogen is lower than 10% after a Severe Accident (SA), in which hydrogen is generated by a 100% zirconium-water reaction.

d) Extra Safety Function Assumptions

The hydrogen concentration is monitored for different levels in containment. There are two trains with five sensors on each train to monitor the hydrogen concentration inside the containment.

7.4.4.4 System Description and Operation

7.4.4.4.1 General System Description

As introduced in Reference [18], the EUH [CCGCS] is composed of the passive hydrogen combiner subsystem and hydrogen monitoring subsystem. The passive hydrogen combiner subsystem consists of PARs without any supports. The hydrogen monitoring subsystem consists of hydrogen sensors.

a) Passive Hydrogen Combiner Subsystem

The passive hydrogen combiner subsystem is designed with 29 sets of PARs.

2 sets of PARS are provided for the DBCs (mainly LOCA) to reduce the

hydrogen concentration. The SFC and redundancy are considered in the design. The 2 sets of PARs are located at an elevation of +41m in the containment dome space.

27 sets of PARs are provided for severe accident conditions to reduce the hydrogen concentration. The SFC and redundancy are not considered.

b) Hydrogen Monitoring Subsystem

The hydrogen monitoring subsystem is composed of two redundant trains. Each train includes 5 detection sensors, 1 for the each top platform of 3 steam generators, 1 for the annulus and 1 for the dome.

7.4.4.4.2 Description of Main Equipment

The PAR comprises of a metal housing promoting natural convection between a gas inlet at the bottom and a lateral gas outlet at the top. The horizontal cover of the housing at the top of the recombiner protects the catalyst against direct spraying of water and aerosol deposition. Numerous parallel plates with a catalytically active coating are arranged vertically at the bottom of the housing. Hydrogen and oxygen in gas mixtures are recombined upon contact with the catalyst, Reference [20].

There are two sizes of PARs. In the standard conditions (0.15 MPa abs, 50 ℃ and hydrogen volume concentration of 4%), the hydrogen removal rates of the large recombiners and the small ones are about 5.4 kg/h and 2.4kg/h respectively.

The hydrogen monitoring system has a measurement range: 0-15vol% with an accuracy of { }. The response time is about{ }for the monitoring of the hydrogen, Reference [20].

7.4.4.4.3 Description of Main Layout

The PARs shall be located at the gas flow rising zone which is accessible in the containment, so that they can support the overall convection, facilitate the even distribution of air, and enable the implementation of maintenance, periodic tests and in-service inspections. Sensitive equipment or cabling shall not be deployed on the exhaust window of the hydrogen combiner directly, Reference [21].

The PARs are installed in various parts of the containment (Steam Generator (SG)-compartments, RCP [RCS] pumps compartments, PZR compartments, the containment dome, upper-room of IRWST, etc.).

The hydrogen sensors are located in the upper dome and annular rooms of the containment, whilst the instrumentation modules are located outside the containment. Each train includes 5 detection sensors. The hydrogen sensors cannot be located in the direct path of a hydrogen release. The sensor shall be kept away from the wall and other large surfaces to avoid flow dead zones. In addition, the hydrogen sensors shall be located in an accessible position, in order to facilitate the implementation of

maintenance, periodic tests and in-service inspections, Reference [21].

7.4.4.4.4 Description of System Interface

The EUH [CCGCS] has no supporting systems except for the power supply and I&C systems. The EUH [CCGCS] has no user systems.

7.4.4.4.5 Description of Instrumentation and Control

The hydrogen concentration is monitored through the two trains of transmitting signals to the main control room.

7.4.4.4.6 System Operation

a) Plant Normal Condition

The EUH [CCGCS] is on standby when plant is in normal condition.

b) Plant Accident Conditions

When the plant enters the state described in the severe accident management guideline (power condition), the operator will manually start the hydrogen monitoring subsystem. After a manual start, the system operates automatically without the intervention of the operator. The containment hydrogen concentration, detected online and continuously by the hydrogen monitoring subsystem, is displayed in the main control room and remote shutdown station. An alarm will sound when the hydrogen concentration exceeds the alarm value. The processing cabinet of the hydrogen monitoring system will send the detected hydrogen concentration signal, failure signal and equipment operating status to the severe accident control board and Digital Control System (DCS) in the main control room, to display and give alarm on the severe accident control board and DCS. The operator can start or stop the system from the severe accident control board and DCS, Reference [22].

7.4.4.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). The detailed design of the system is presented in Reference [18], [19], [20], [21] and [22]. Furthermore, design substantiation of the EUH [CCGCS] will be estimated in the fault study in Chapter 12 and 13.

7.4.4.5.1 Compliance with Safety Requirements

a) Compliance with Control of Reactivity Requirements

The EUH [CCGCS] does not contribute to this safety function.

b) Compliance with Removal of Heat Requirements

The EUH [CCGCS] does not contribute to this safety function.

c) Compliance with Confinement Requirements

2 sets of FC2 PARs and 27 sets of FC3 PARs are provided in the EUH [CCGCS] for the DBCs and severe accidents. The PARs are passively self-activated when the hydrogen concentration reaches 1% in volume.

d) Compliance with Extra Safety Function Requirements

Two redundant trains of hydrogen monitoring are provided and each train includes 5 detection sensors. The sensors can provide online and continuously monitoring after being manually started.

7.4.4.5.2 Compliance with Design Requirements

a) Compliance with Safety Classification

The safety categorisation of the EUH [CCGCS] functions is listed in Table T-7.4-10 and the safety classification of main components in Table T-7.4-11.

The EUH [CCGCS] is designed to withstand a SSE. The main components are classified as SSE1 in Table T-7.4-11.

T-7.4-10 System Function Categorisation for EUH [CCGCS]

System Function	**Function Category**
Passive hydrogen combiner subsystem	
PARs for DBC	FC2
PARs for DEC	FC3
Hydrogen monitoring subsystem	FC3

T-7.4-11 Component Classification for EUH [CCGCS]

Component	**Function Class**	**Design Provision Category**	**Design Provision Class**	**Seismic Category**
PARs for DBC	F-SC2	NC	NC	SSE1
PARs for DEC	F-SC3	NC	NC	SSE1
Monitoring sensors	F-SC3	NC	NC	SSE1

b) Compliance with Reliability

1) Redundancy and SFC

The principle of the SFC is presented in Sub-chapter 7.2.4.

Redundancy and the SFC are applied to PARs which provide the FC2 classified safety functions. Two sets of PARs are provided to reduce the hydrogen concentration during design basis conditions.

2) Independence

Independence has been considered for the EUH [CCGCS] through their layout.

Generally, the passive hydrogen recombiners are installed in the containment dome, SG compartment, and containment annulus space to support convection and promote atmospheric homogenisation.

The hydrogen sensors are installed in areas such as containment dome, top platform of the SG, and annulus instead of the path the released hydrogen flows through, and as far from the walls and other large area surfaces as possible to prevent sensor placement in dead zones. Moreover, the hydrogen sensors are set at places which are easily accessible to facilitate maintenance, periodic tests and in-service inspections.

3) Diversity

Not applicable.

4) Fail-safe Design

There is no fail-safe designed equipment in the EUH [CCGCS].

5) Ageing and Degradation

The plant design life is 60 years. Some components may need replacing at the end of their individual design life. The management of equipment ageing and degradation follows the arrangement of asset management stated in 7.2.4.

The performance of equipment is guaranteed through life EMIT, as well as from monitoring during normal operation. Thus it can be ensured that ageing effects will not compromise the safety performance. The detailed design arrangement around EMIT and equipment monitoring is presented in Reference [22].

The system layout design as part of the detailed design stage ensures the accessibility and requirement for safety equipment in-service inspection and periodic tests are met. This includes the requirements of scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [21].

7.4.4.5.3 Compliance with Human Factors

Not applicable since the EUH [CCGCS] is a passive system.

7.4.4.5.4 Compliance with Autonomy

Not applicable since the EUH [CCGCS] is a passive system.

7.4.4.5.5 Compliance with Other Design Requirements

Not applicable since the EUH [CCGCS] is a passive system and does not interface with other systems.

7.4.4.5.6 Compliance with Equipment Qualification

All components required to perform the safety functions shall be capable of operating under accidental conditions, which requires the components to withstand the most adverse ambient environment.

Documents relevant to the equipment qualification will be delivered during Step 4 of GDA.

7.4.4.5.7 Compliance with Hazard Protection

Reference [21] provides the measures protecting the EUH [CCGCS] against internal and external hazards. The hazard analysis in Chapter 18 and 19 demonstrates that the EUH [CCGCS] is effectively protected during the hazards identified.

7.4.4.5.8 Compliance with Commissioning

The performance of the EUH [CCGCS] is validated by the following commissioning tests:

a) Initial inspection test;

b) Analog Monitoring and Control channel test;

c) Starting test and general capability test

7.4.4.5.9 Compliance with Examination, Inspection, Maintenance and Testing

a) System Surveillance

   No surveillance is provided since the EUH [CCGCS] is a passive system.

b) Maintenance and Replacement

   The catalyzing plate for passive hydrogen recombiners is subject to performance inspection by sampling performed by the supplier prior to installation. Therefore, it is confirmed that its performance meets the requirements as stipulated in the technical specification. At the end of installation, visual inspection of the shell and support is needed. During plant operation, the performance of the catalyst for

the passive hydrogen recombiners shall be inspected periodically.

The catalyzing metal plate must be regenerated to recover if there is any decrease in catalyst performance. The hydrogen monitoring system is tested and calibrated after being installed. During plant operation, it is inspected and maintained periodically to ensure that the hydrogen monitoring function can be performed reliably.

c) Periodic Test

Periodic tests are provided for the EUH [CCGCS]. These tests include the capability periodic test of PARs and the periodic test of the hydrogen monitoring system in general.

d) In-service Inspection

See section b) (Maintenance and Replacement of the EUH [CCGCS]).

7.4.4.5.10 Special Thermal-Hydraulic Phenomena

Not applicable.

7.4.4.5.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and also engineering experience, the material selected for the main component is presented in Sub-chapter 7.4.4.4.2.

7.4.4.5.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

The main equipment of the EUH [CCGCS] is in standby during normal operation and is installed in the reactor building, where no personnel access during normal operation is available. Following an accident, the EUH [CCGCS] operates passively. Therefore, no insulation is provided for the EUH [CCGCS].

7.4.4.5.13 Compliance with Decommissioning

The design of the EUH [CCGCS] takes into account the impact on decommissioning, including the following measures:

a) The main equipment is passive equipment with simple structures, which can facilitate the decommissioning of the equipment;

b) The layout of the EUH [CCGCS] considers decommissioning, such as the accessibility of personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.4.5 Containment Leak Rate Testing and Monitoring System (EPP [CLRTMS])

7.4.5.1 Safety Requirements

7.4.5.1.1 Control of Reactivity Requirements

The EPP [CLRTMS] is not required to perform this safety function.

7.4.5.1.2 Removal of Heat Requirements

The EPP [CLRTMS] is not required to perform this safety function.

7.4.5.1.3 Confinement Requirements

The EPP [CLRTMS] is required to confine radioactive substances by limiting potential releases of radionuclides from the containment building to the environment in accident scenarios (DBC3, DBC4 and DEC-A, DEC-B):

a) The EPP [CLRTMS] collects the leakage at penetrations with a high leak risk in the containment bypass;

b) The EPP [CLRTMS] contributes to the containment isolation function by closing containment isolation valves on pressurisation/depressurisation lines, the airlock, equipment hatch, and isolation valves on the containment pressure measurement lines.

c) The penetrations in the EPP [CLRTMS] contribute to containment confinement when they are effectively isolated.

7.4.5.1.4 Extra Safety Function Requirements

There is no extra safety function requirement for the EPP [CLRTMS].

7.4.5.2 Design Requirements

The general design requirements of the safety systems to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to the EPP [CLRTMS]:

a) Diversity: Diversity is not applicable to the EPP [CLRTMS];

b) Fail-safe: There is no fail-safe requirement on the EPP [CLRTMS], therefore fail-safe is not applicable to the EPP [CLRTMS];

c) Autonomy in Respect to the Heat Sink: The EPP [CLRTMS] is not a heat sink system; therefore the autonomy of the heat sink is not applicable to the EPP [CLRTMS].

The substantiation analysis of the EPP [CLRTMS] to other design requirements is shown in 7.4.5.5 section.

7.4.5.3 Design Bases

The EPP [CLRTMS] belongs to the engineered safety systems and consists of the leak recovery sub-system and containment leak test sub-system. The EPP [CLRTMS] performs the safety functional requirement through leak recovery and containment isolation in accident states.

This sub-chapter aims to provide the main design assumptions considered in the system design.

7.4.5.3.1 General Assumption

The EPP [CLRTMS] contributes to the confinement of radioactive substances. The containment structure and associated systems are designed to limit the release of radionuclides to the environment, in accidents involving fission product release.

a) Safety Classification

The containment isolation valves of the EPP [CLRTMS] which perform the function of containment isolation are Function Category 1 (FC1).

The equipment hatch, airlock and emergency airlock in the closed mode are a part of the containment, and they are Function Category 1 (FC1) due to their contribution to the containment isolation function.

The leak recovery sub-system of the EPP [CLRTMS] performs leak recovery under DBC and DEC conditions, and therefore the whole sub-system is Function Category 2 (FC2).

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which is important to safety will be taken into account.

The design life of the main equipment of the EPP [CLRTMS] is 60 years. In addition, some parts of the main equipment need to be replaced regularly during the design life.

c) Autonomy

The containment isolation valves are controlled and powered by different electrical zones, and the Emergency Diesel Generator (EDG) and battery are used as the emergency power supply. The airlock and emergency airlock shall be powered by different electrical zones.

d) Equipment Qualification

The components of the EPP [CLRTMS] performing an FC1 or FC2 safety function will be qualified.

The equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

There is no fluctuation of the electrical power supplied to the EPP [CLRTMS].

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in the EPP [CLRTMS] equipment design, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions such as the confinement function shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety functions.

7.4.5.3.2 Design Assumption

The EPP [CLRTMS] is required to collect the leakage at penetrations with high leak risk in the containment bypass and contributes to the containment isolation function by closing containment isolation valves on pressurisation/depressurisation lines, the airlock, equipment hatch, and isolation valves on containment pressure measurement lines. The requirements for the EPP [CLRTMS] are as follows:

a) Control of Reactivity Assumptions

The EPP [CLRTMS] does not perform the safety function of reactivity control.

b) Removal of Heat Assumptions

The EPP [CLRTMS] does not perform the safety function of residual heat removal.

c) Confinement Assumptions

The potential leaks to the outside environment of the following penetrations are eliminated by the EPP [CLRTMS]:

1) Equipment hatch;

2) Airlock;

3) Emergency airlock;

4) Fuel transfer tube;

5) Fluid penetrations presenting radiological risks;

6) Ventilation penetrations.

The overall leak rate criterion defined for the maximum permissible leak rate under accident conditions is 0.3% per day of the total gas volume inside the containment.

d) Extra Safety Function Requirement Assumptions

There is no extra safety function requirement for the EPP [CLRTMS].

7.4.5.4 System Description and Operation

7.4.5.4.1 General System Description

As introduced in Reference [23], the EPP [CLRTMS] collects potential radioactivity release from containment under accident conditions, and contributes to the containment isolation and integrity. The EPP [CLRTMS] includes the leak recovery sub-system and containment leak tightness test sub-system. The EPP [CLRTMS] is located in the Reactor Building (BRX), Fuel Building (BFX) and Safeguard Buildings (BSX) of the Nuclear Island (NI).

a) Leak Recovery Sub-system

A leak recovery sub-system is provided at the containment penetrations with the high potential risk of leakage into the atmosphere to prevent containment bypass. The leaks are collected by the pipelines discharged into the sump of the annulus. The Annulus Ventilation System (EDE [AVS]) supplies and maintaines the negative pressure in the containment annulus to drive the flow in the leak recovery sub-system.

The leak recovery sub-system is provided in the following penetrations:

1) Equipment hatch, airlock, emergency airlock and fuel transfer tube.

Potential leaks through the double seals are collected and transferred to the containment annulus by the leak recovery sub-system.

2) Pipe penetrations with potential radiological risks.

Potential leaks from the outside isolation valve are collected and transferred to the containment annulus by the leak recovery system.

It applies to the penetrations in which the inside isolation valve is normally connected directly to the containment atmosphere, or primary coolant is transported.

3) Ventilation penetrations.

Potential leaks from the outside isolation valve are collected and transferred to the containment annulus by the leak recovery sub-system.

b) Leak Test Sub-system

Three types of tests are designed to evaluate the leak of the containment with its steel liner and associated penetrations.

1) Type A: Overall test to determine the total leak rate from the inner containment.

   Test Type A assesses and evaluates the containment leak-tightness, which involves pressurising the containment in successive stages gradually and taking measurements at each stage (pressure level).

   The leak rate is evaluated by the absolute pressure method. A monitoring system collects the required data to estimate the total leak rate (thermometers, hygrometers, etc.).

   Measurements are taken at atmospheric pressure to determine measurement system errors at the beginning of the tests.

   Additional measurements are taken at intermediate pressure levels between atmospheric and the maximum test pressure. The measurements are then repeated as the containment pressure is reduced to atmospheric pressure.

   During the Type A tests, containment behaviour is monitored by the Containment Instrumentation System (EAU [CIS]).

2) Type B: Partial test to determine the local leak rate through specific containment penetrations equipped with seals.

   Type B test determines local leaks through the leak seals of the following specific containment penetrations:

   - Equipment hatch.
   - Airlock.
   - Emergency airlock.
   - Electrical penetrations.
   - Fuel transfer tube equipped with closures with a removable plug and gasket seal.

3) Type C: Partial test to determine the local leak rates through the containment isolation valves.

   Type C tests determine the local leaks through the containment isolation valves apart from those of the water/steam secondary system, and those of the circuits considered "enclosed" within the containment.

7.4.5.4.2 Description of Main Equipment

The main equipment of the EPP [CLRTMS] is as follows, Reference [25]:

a) Containment isolation valves

The EPP [CLRTMS] contains four containment isolation valves for containment isolation. Two automatic valves are located in the containment pressurisation/ depressurisation line, and two manual valves in containment pressure monitoring line.

b) Equipment hatch

The equipment hatch is mainly used as the access way for large equipment in to the reactor building.

In the construction phase, the equipment access hatch is used to introduce the main components into the reactor building, such as the reactor vessel, the steam generators, the pressuriser, the primary piping and the primary reactor pump sets, etc.

In the operational phase, the equipment access hatch is used to introduce the necessary components for the execution of outages, such as:the vessel head multi-stud tensioning machine, specific tools for maintenance activities, replacement equipment, etc.

The equipment access hatch is designed to maintain its mechanical integrity and fulfil its basic functions (notably, preservation of internal containment leak tightness) in all normal or accident conditions. The safety function class of equipment access hatch is F-SC1, the barrier class is B-SC2, the code class is RCC-M2, and the seismic class is SSE1.

The equipment access hatch is comprised of the following main components:

1) A cover coupled to the inner sleeve using flanges;
2) A mobile heavy duty floor;
3) A double-seal system located between the cover flange and the sleeve flange which enables the collection and control of leaks;
4) Flange coupling device;
5) Cover guide and lifting device;
6) Control station.

c) Airlock and emergency airlock

The two airlocks (Personnel Airlock and Emergency Airlock) are identical in regards to their function. The personnel airlock and emergency airlock of containment are mainly used for the passage of personnel and small equipment without affecting the leak tightness capability of containment.

The pressure retaining components of personnel access airlocks are designed to maintain the mechanical integrity and fulfil the basic functions (notably, preservation of internal containment leak tightness) in all normal or accident conditions. After an accident, the airlocks must be able to be opened manually. The safety function class of personnel access airlock is F-SC1, the barrier class is B-SC2, the code class is RCC-M2 and the seismic class is SSE1.

Each personnel access airlock consists of personnel access airlocks body, mechanisms for the automatic and manual control of the doors, local instrumentation and control consoles, equivalent equalization device and anti-crush safety system.

d) Containment mechanical penetrations

According to the types of transmission fluid, mechanical piping penetrations can be categorized into the following types:

1) Penetrations for high energy pipes: pipework penetrations carrying high energy fluid;

2) Standard pipe penetrations;

3) Sump extraction penetrations for RIS [SIS] and EHR [CHRS];

4) Spare penetrations;

5) Ventilation penetrations.

The design of penetration considers the requirements from construction and inspection. Dedicated structure is designed for each penetration type.

1) Penetrations for high energy pipes

A penetration for high energy pipes comprises the following elements:

- Cylindrical ferritic steel penetration sleeves are embedded and anchored in the concrete of both Reactor Building containment walls. The internal containment penetration sleeve is elongated through the annulus and beyond the external face of the external containment wall. It is used to prevent pressurisation and/or temperature increase in the annulus when there is a pipework break in this area;
- An integrally forged pipe fitting, which is installed inside the annulus, is used to link the pipework to the internal containment sleeve, in order to prevent the risk of a direct external leak resulting from failure of the weld between the integrally forged pipe fitting and pipework.
- An expansion joint is used to link the integrally forged pipe fitting to the external containment sleeve to adopt the differential displacement.

- At least one flange is needed to prevent leaks between the sleeve and concrete.

The structure of penetrations for steam and feedwater pipes is the same as the penetrations for high energy pipes, except that they have an extra shield tube inside the internal containment sleeve. The shield tube is used to protect the internal containment sleeve by preventing the directly spraying when a break occurs at the weld between the integrally forged pipe fitting and pipework. Cooling flanges are welded to internal sleeve if necessary.

2) Standard pipe penetrations

A standard pipe penetration comprises the following elements (Note: some standard pipe penetrations contain two or more pipework sections in the same penetration.):

- Cylindrical ferritic steel penetration sleeves are embedded and anchored in the concrete of both the Reactor Building containment walls;
- A connection flange located inside the internal containment is welded between the pipework and internal containment penetration sleeve;
- An expansion joint is used to link the pipework to the external containment sleeve to adopt the differential displacement.

3) Sump extraction penetrations (RIS [SIS] and EHR [CHRS] penetrations)

A penetration for sump extraction penetrations comprises the following elements:

- A cylindrical stainless steel penetration sleeve is embedded and anchored in the slab of the Reactor Building；
- A connection flange located at the sump side is welded between the extract pipework and penetration sleeve;
- An expansion joint is used to link the containment sleeve and the shut-off valve on the safeguard building side to adopt the differential displacement.

4) Spare penetrations

A spare penetration comprises the following elements:

- Cylindrical ferritic steel penetration sleeves are embedded and anchored in the concrete of both the Reactor Building containment walls. These sleeves have the same strength and structure as sleeves for high energy penetration.
- The penetration is capped by a solid welded closure on annulus side.

5) Ventilation penetrations

A ventilation penetration comprises the following elements:

- Cylindrical ferritic steel penetration sleeves are embedded and anchored in the concrete of both the Reactor Building containment walls. The internal containment penetration sleeve is elongated through the annulus and beyond the external face of the external containment wall, which is used as a duct penetrated the two containment walls;
- An expansion joint is used to link the internal contaiment penetration sleeve to the external containment sleeve to adopt the differential displacement;

e) Containment electrical penetrations

The electrical penetrations provide gas-tight and pressure-resistant penetration through the containment of one or more electrical circuits. They are designed to withstand the aggregate of operational conditions without loss of containment integrity or assembly structural damage.

The electrical penetrations include:

1) Electrical conductors up to the nearest connecting points within and outside the containment (penetration conductors);
2) Components for electrical insulation of such conductors;
3) Components for the pressure-resistant, gas-tight and temperature-resistant enclosure of this conductor assembly and for connection with the containment wall;
4) Permanently connected devices for monitoring gas leakage.

The electrical penetrations consist of a number of insulated conductor feedthroughs.The conductor feedthoughs are housed in a canister, which is mounted in the containment wall. The canister is welded to a metal embedded sleeve in the concrete of the containment to form a gas-tight seal. Terminal boxes are mounted at either end of this structure.

The fluid penetrations are safety classified and provided with sufficient isolation as described in Sub-chapter 7.4.6.

7.4.5.4.3 Description of Main Layout

Leak recovery sub-system is dedicated to leak collection and is comprised of pipes connected to the inter seal space of various containment devices located in the Fuel Building (BFX) and the safeguard building. The pipes collect leakage and direct it toward the RPE [VDS] sump located in the annulus. The leak collection extraction

network is comprised of isolation valves installed in a vertical position and inclined pipes to facilitate the run-off of the condensates [26].

7.4.5.4.4 Description of System Interface

a) Containment Sweeping and Blowdown Ventilation System (EBA [CSBVS])

The EPP [CLRTMS] recovers the leaks from the EBA [CSBVS] outer containment isolation valves.

b) Annulus Ventilation System (EDE [AVS])

1) The extraction of leakage from drained components via the leak collection system by maintaining a negative pressure in the annulus.

2) Treatment of potentially contaminated air with an absolute filter and an iodine filter before it being released into the environment.

c) Containment Filtration and Exhaust System (EUF [CFES])

The EPP [CLRTMS] collects the potential leakage from containment isolation valves of the EUF [CFES].

7.4.5.4.5 Description of Instrumentation and Control

The parameters of the EPP [CLRTMS] are monitored as follows [27]:

a) Depressurisation flowrate;

b) Stack maximal exhaust pressure;

c) The pressure of containment when testing;

d) The temperature and humidity in commissioning and periodic tests.

7.4.5.4.6 System Operation

a) Plant Normal Operation

This Sub-chapter describes the possible configurations of the EPP [CLRTMS] in normal plant operation (DBC-1).

1) Containment Tests

Containment pressurisation by mobile compression units is either for pre-operational containment resistance and leak tightness tests or for the ten-year containment test.

2) Pressurisation of Containment

The pressurisation of containment can be activated and deactivated by the compressors from the related control panels.

Adjustment of the pressurisation gradient in containment is performed manually by each compressor control panel through regulating the pressurisation rate or by adapting the number of compressors in operation.

The containment leak rate is measured after venting the pressurisation line to consider the leaks through the containment pressurisation/depressurisation penetration.

3) Depressurisation of the Containment

The depressurisation rate is controlled through manual control valves and local flow instruments after the manual valve opens.

The flow meter isolates the containment pressurisation / depressurisation penetration by an automatic closure of the containment isolation valve outside of containment when there is an excessively quick depressurisation in the containment. An alarm in the main control room allows for restarting of the depressurisation.

4) Normal Shutdown of the System

After the test, the containment pressurisation and depressurisation function is isolated by closing related valves. The test equipment is removed.

5) Containment Penetrations Leak Tightness Test

The tests are carried out in a plant status defined by each basic system.

b) Plant Accident Conditions

The leakage is collected by the negative pressure created in the annulus by the EDE [AVS] in accidents. The condensates are recovered in the RPE [VDS] sumps of the annulus. The gas is treated by the filtration of the EDE [AVS] before being released into the atmosphere.

The containment isolation valves of the containment pressurisation and depressurisation penetration are closed automatically according to the containment isolation signals.

7.4.5.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. Detailed design of the system is presented in [23], [24], [25], [26] and [27].

7.4.5.5.1 Compliance with Safety Functional Requirements

a) Compliance with Control of Reactivity Requirements

The EPP [CLRTMS] does not contribute to this safety function.

b) Compliance with Removal of Heat Requirements

The EPP [CLRTMS] does not contribute to this safety function.

c) Compliance with Confinement Requirements

Leakage collection is provided for the penetrations which contain a high risk of leak as described in Sub-chapter 7.4.5.4.

The EPP [CLRTMS] lines that penetrate the containment building are provided with four isolation valves to ensure containment isolation.

The equipment hatch and airlocks are designed with double seals and actuators for opening and closing of the hatch and airlocks to ensure containment isolation and personnel access.

d) Compliance with Extra Safety Function Requirements

There is no extra safety function requirement for the EPP [CLRTMS].

7.4.5.5.2 Compliance with Design Requirements

a) Compliance with Safety Classification

The safety categorisation of the EPP [CLRTMS] functions is listed in Table T-7.4-12 and the safety classification of the main components in Table T-7.4-13.

The EPP [CLRTMS] is designed to withstand a Safe Shutdown Earthquake (SSE). The main components are classified as SSE1 as shown in Table T-7.4-13.

T-7.4-12 System Function Categorisation for the EPP [CLRTMS]

System Function	Function Category
Containment leakage collecting	FC2
Containment isolation	FC1
Equipment Hatch and airlocks	FC1
Containment penetrations	FC1

T-7.4-13Components Classification for the EPP [CLRTMS]

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
Equipment for containment leakage collecting	F-SC2	DPA	B-SC2	SSE1

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
Containment penetrations	F-SC1	DPA	B-SC2	SSE1
Containment Isolation Valves	F-SC1	DPA	B-SC2	SSE1
Equipment Hatch	F-SC1	DPA	B-SC2	SSE1
Airlock and Emergency airlock	F-SC1	DPA	B-SC2	SSE1
Containment penetrations	F-SC1	DPA	B-SC2	SSE1

b) Compliance with Reliability

1) Redundancy and SFC

The principle of SFC is presented in Sub-chapter 7.2.4.

Redundancy and the SFC are applied to the equipment providing the FC1 classified safety functions.

2) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The design of the EPP [CLRTMS] considers the independence requirement. The containment isolation valves located internally and externally of the containment ensure the independence of the system.

3) Diversity

Not applicable for the EPP [CLRTMS].

4) Fail-safe Design

Not applicable for the EPP [CLRTMS].

5) Ageing and Degradation

The plant design life is 60 years. Some components may need replacing at the end of their individual design life. The management of equipment ageing and degradation follows the arrangement of asset management stated in 7.2.4.

The performance of equipment is guaranteed through life EMIT, as well as the monitoring during normal operation. Thus it can be ensured that ageing effects will not compromise safety performance. Detailed design arrangements around EMIT and equipment monitoring is presented in

Reference [27].

The system layout design as part of the detailed design stage will ensure the accessibility and requirement for safety equipment in-service inspection and periodic tests as well as the requirements of scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [26].

7.4.5.5.3 Compliance with Human Factors

The system design and the control function design of the EPP [CLRTMS] do not require short term operator intervention. No operator action within 30 minutes after the initial event is required.

It should be noted that there are operator actions during plant normal operation or accident conditions (including plant start-up, shutdown, and maintenance or testing etc.). Relevant human actions which are important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of Chapter 15. Relevant evaluated reports will be provided as references of Chapter 15.

7.4.5.5.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

No operator intervention is required in the first 30 minutes and 1 hour under accident conditions for EPP [CLRTMS] operation.

The design of the EPP [CLRTMS] fulfils these principles via their control function design, Reference [27] .

b) Autonomy in Respect to the Heat Sink

Not applicable since the EPP [CLRTMS] is not a heat sink system.

c) Autonomy in Respect to Power Supply Systems

The containment isolation valves in containment pressurisation/depressurisation penetrations operate when receiving containment isolation signals.

In order to improve the function reliability, the containment isolation valves are controlled and powered by different electrical zones, and Emergency Diesel Generators (EDG) and batteries are used as an emergency power supply.

The equipment hatch and airlocks will be opened during cold shut down for maintenance to allow for personnel passing and equipment transportation. As a result, the power supply is needed for control. Additionally, the airlock and emergency airlock shall be powered by different electrical zones.

7.4.5.5.5 Compliance with Other Design Requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

Not applicable.

b) Considerations Related to the Electrical Power Grid

Not applicable.

7.4.5.5.6 Compliance with Equipment Qualification

All components required to perform the safety functions shall be capable of operating under normal conditions and accident conditions, which requires the components to withstand the most adverse ambient environment.

The documents relevant to equipment qualification will be developed during Step 4 of GDA.

7.4.5.5.7 Compliance with Hazard Protection

The measures taken to protect the EPP [CLRTMS] against the internal and external hazards are provided in Reference [26]. The hazard analysis in Chapter 18 and 19 demonstrates that the EPP [CLRTMS] is effectively protected during the hazards identified.

7.4.5.5.8 Compliance with Commissioning

The system performance will be validated by commissioning and testing.

a) System flushing;

b) Instrumentation and control channel tests;

c) Valve tests;

d) The global leak rate of the primary containment;

e) The leak rate of electric penetrations, mechanic penetrations, the equipment hatch and airlocks;

f) The visual check of the containment;

g) The strength of the containment.

The detailed description is presented in Reference [27]. Documents related to the commissioning will be submitted.

7.4.5.5.9 Compliance with Examination, Inspection, Maintenance and Testing

a) System Surveillance

The EPP [CLRTMS] is designed for the situation and operation of the system to

be surveyed by a number of means. The main surveillance means of the EPP [CLRTMS] are as follows:

1) The position of automatic containment isolation vales；

2) Closing of the equipment hatch;

3) Closing of the airlock internal and external door;

4) Closing of the emergency airlock internal and external door;

5) The flowrate of pressurisation and depressurisation during containment test.

b) Maintenance and Replacement

The scheduled maintenance of the valves of the containment leak recovery sub-system is performed during maintenance cold shutdown, refuelling cold shutdown and reactor completely discharged modes. No accident risks will be caused to containment pressurisation under such conditions.

The scheduled maintenance of containment isolation valves is performed during maintenance cold shutdown, refuelling cold shutdown and reactor completely discharged modes. There is no requirement on containment integrity under such conditions.

The valve maintenance is conducted only under the conditions of maintenance cold shutdown and refuelling cold shutdown without a required containment test.

c) Periodic Test

Periodic tests for the EPP [CLRTMS] include:

1) Isolation test of containment pressurisation/depressurisation penetrations;

2) Operability of the access hatch in manual mode;

3) Overall test of containment;

4) Leak rate test of containment penetrations.

d) In-service Inspection

The equipment hatch, airlock and emergency airlock shall have in-service inspections performed on them to ensure their safety under high pressure.

7.4.5.5.10 Compliance with Special Thermal-Hydraulic Phenomena

There is no special thermal-hydraulic phenomenon for the EPP [CLRTMS] design.

7.4.5.5.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component of the EPP

[CLRTMS] is stainless steel.

7.4.5.5.12 Compliance with Insulation Design

There is no insulation requirement for the EPP [CLRTMS].

7.4.5.5.13 Compliance with Decommissioning

The design of the EPP [CLRTMS] takes into account the impact on decommissioning, including the following measures:

a) The main line is equipped with a drainage pipe, which can be used to empty the line;

b) The layout of the EPP [CLRTMS] considers decommissioning, such as the accessibility of personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.4.6 Containment Isolation

7.4.6.1 Safety Requirements

7.4.6.1.1 Control of Reactivity Requirements

The containment isolation is not required to perform this safety function.

7.4.6.1.2 Removal of Heat Requirements

The containment isolation is not required to perform this safety function.

7.4.6.1.3 Confinement Requirements

The containment isolation is required to confine the radioactive substances. It shall minimise the radioactive release through the fluid penetrations into the environment in accidents with fission product being released.

7.4.6.1.4 Extra Safety Function Requirement

Not applicable.

7.4.6.2 Design Requirements

Containment isolation is required to meet the design requirements as shown in Sub-chapter 7.2.4. The substantiation analysis of containment isolation to other design requirements is shown in Sub-chapter 7.4.6.5.

7.4.6.3 Design Bases

7.4.6.3.1 General Assumption

The isolation function is not required during normal operation. The position of the isolation valves depends on the operation of the system to which they belong.

All fluid penetrations, except those belonging to safety systems used for post-accident management, are isolated.

Isolation is provided through isolation valves (motorised, manual and/or check valves). Containment isolation must be ensured when needed.

a) Safety Classification

The function of containment isolation is a safety function, which belongs to Function Category 1 (FC1) in DBC or Function Category 3 (FC3) in DEC.

b) Ageing and Degradation

During the design of containment isolation valves, the ageing and degradation of the equipment, which are important to safety, will be taken into account.

The design life of the plant is 60 years. Some containment isolation valves need to be replaced regularly during the life of the plant.

c) Autonomy

The autonomy of the containment isolation function is described in the systems to which the containment isolation valves belong to.

d) Equipment Qualification

The containment isolation valves performing an FC1 safety function shall be qualified.

The containment isolation valves performing an FC3 safety function required under DEC conditions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

The fluctuation of the electrical power grid doesn’t affect the ability of the safety function as no component sensitive to power fluctuations forms part of the containment isolation.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in the design of containment isolation valves, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions such as the confinement function shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.4.6.3.2 Design Assumption

a) Control of Reactivity Requirements

Containment isolation is not required to perform this safety function.

b) Removal of Heat Requirements

Containment isolation is not required to perform this safety function.

c) Confinement Requirements

The containment isolation function is automatically activated by signals from the RPR [RPS] except for the manual containment isolation valves.

Depending on the normal operating position and role in the accident, various containment isolation valves may perform the following functions to:

1) Close at the beginning of the accident,

2) Remain leak tight during the post-accident phase,

3) Remain operable during the post-accident phase if needed.

The containment isolation must ensure these specific functions.

d) Extra Safety Function Requirements

Not applicable.

7.4.6.4 System Description and Operation

7.4.6.4.1 General System Description

For fluid penetrations, isolation is generally carried out by two independent devices in the pipes crossing the containment boundary.

The following are considered as effective barriers provided that they are protected from internal missiles:

a) The metallic pipe walls, tanks and valve bodies, the design pressures and temperatures of which are higher or equal to the bounding conditions in accidents that may occur in the reactor building,

b) An isolation valve which is closed automatically or by operator in main control room,

c) An isolation valve with local manual control, normally closed. The position of this valve is subject to administrative controls or is controlled by a mechanical locking device,

d) A single check valve on a pipe transporting liquid entering the containment provided it is located inside the containment and there is an additional isolation

valve outside the containment.

The systems which are relevant for the containment isolation function of liquid penetrations are provided as follows:

a) Containment Leak Rate Testing and Monitoring System (EPP [CLRTMS]);

b) Steam Generator Blowdown System (APG [SGBS]);

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

d) Containment Heat Removal System (EHR [CHRS]);

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

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

g) Emergency Boration System (RBS [EBS]);

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

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

j) Nuclear Island Vent and Drain System (RPE [VDS]);

k) Nuclear Sampling System (REN [NSS]);

l) Main Feedwater Flow Control System (ARE [MFFCS]);

m) Main Steam System (VVP [MSS]);

n) Atmospheric Steam Dump System (VDA [ASDS]);

o) Secondary Passive Heat Removal System (ASP [SPHRS]);

p) Containment Filtration and Exhaust System (EUF [CFES]);

q) Containment Sweeping and Blowdown Ventilation System (EBA [CSBVS]);

r) Operational Chilled Water System (DER [OCWS]);

s) NI Dematerialised Water Distribution System(SED [DWDS(NI)]);

t) Nitrogen Distribution System (SGN [NDS]);

u) Service Compressed Air Distribution System (SAT [SCADS]);

v) Fire-fighting Water System for Nuclear Island (JPI [FWSNI]);

w) Gaseous Waste Treatment System (TEG [GWTS]);

x) Reactor Coolant System (RCP [RCS]).

Containment isolation is divided into two isolation stages: containment isolation stage A and containment isolation stage B.

Containment isolation stage A includes the penetrating lines in the following systems:

a) The EPP [CLRTMS];

b) The APG [SGBS];

c) The PTR [FPCTS];

d) The EHR [CHRS];

e) The RCV [CVCS];

f) The RRI [CCWS];

g) The RPE [VDS];

h) The REN [NSS];

i) The EBA [CSBVS];

j) The DER [OCWS];

k) The SED [DWDS(NI)];

l) The SGN [NDS];

m) The JPI [NIFPS];

n) The TEG [GWTS].

Containment isolation stage B includes the penetrating lines in the following systems:

a) The RCV [CVCS] (lines of the shaft seals, charging and auxiliary spraying);

b) The RRI [CCWS] (cooling lines of the letdown heat exchangers);

c) The REN [NSS] (sampling lines for the equipment in the primary circuit and gas in the containment).

d) The RBS [EBS] (lines for emergency boration injection).

7.4.6.4.2 Lines Penetrating the Containment Internal and External Walls

The isolation valves shall be configured according to the following criterias:

a) Lines Connecting to the Primary Loop or Directly Connecting to the Containment Atmosphere

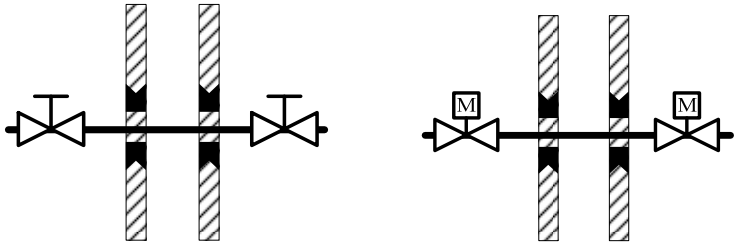
These lines are equipped with one or two isolation valves (one outside the containment and the otherinside) which constitutea double isolation barrier with the corresponding pipe walls at the containment penetration.The safety valve can be used as the isolation valve if the safe pressure set point value is higher than 1.5 times of the containment design pressure.

The SFC can be met by this configuration.

The general design requirements of the isolation valves are as follows:

1) For Systems Used during Shutdown

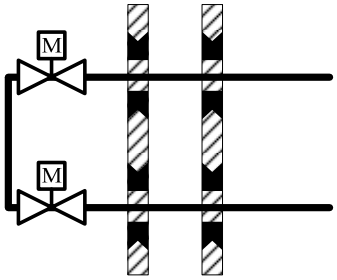
   Two manual valves or power-operated valves controlled from the MCR are required



2) For the System Used in Normal Operating Conditions or Accident Conditions, Parts of the System are Located outside the Containment and Form a Closed Boundary

   - The closed section outside of containment is considered as forming a part of the containment and is designed to withstand the design pressure of the containment.

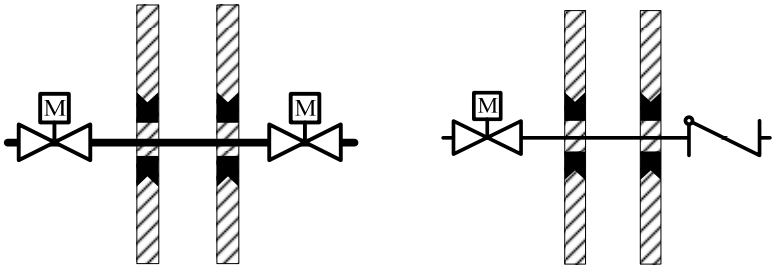
     For each penetration, the part outside of containment needs an automatic isolation valve for containment isolation.



   - For Other Systems Used in Normal Operating Conditions or Accident Conditions

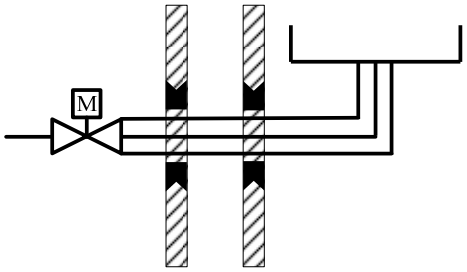
     Two automatic containment isolation valves shall be designed, with one inside the containment, and the other outside (1). For the line transmitting fluid into the containment (2), an automatic isolation valve and a check valve shall be installed, with the check valve installed inside the containment as an isolation valve.

     (1) (2)



- Special Regulations on the RIS [SIS] and EHR [CHRS] Penetrations (from IRWST to Pump)

  Each of these lines only contains one automatic isolation valve installed outside of containment. These valves are not automatic by receiving the containment isolation signal and shall be closed manually in the main control room. The pipes between the sump and the valve are enclosed in a leak tight casing (guard sleeve) and provide a double leak tight penetration barrier.



Bellows-sealed globe valves are used where they are needed to ensure the external leak-tightness of containment isolation valves. The other valves are equipped with a leak recovery system.

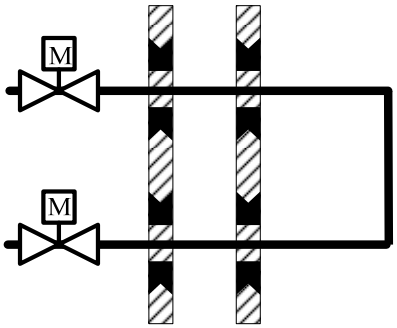
b) Lines Not Directly Connected to the Containment Atmosphere (not Belonging to the Secondary Loop System)

For lines entering the containment, which are connected neither to the containment atmosphere, nor to the primary loop system, or do not belong to the secondary cooling system, (as shown in the following figure) are subject to the following requirements:

1) The integrity of the containment isolation valves shall be maintained after an accident.

2) They must be safe and meet the relevant seismic requirements.

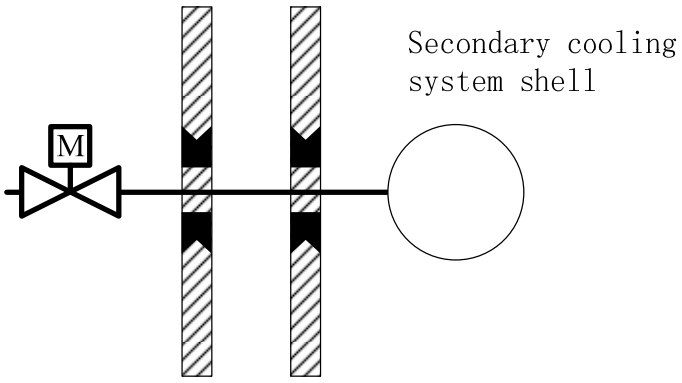
These lines are equipped with an isolation valve outside each penetration, so that a double barrier is provided at the penetration (closed system installed inside the containment and the isolation valve outside the containment).



In general, for the systems used during plant normal operation or accidents, the isolation valves shall be automatically or remotely controlled in the main control room. The isolation valves for other systems are operated manually.

c) Lines that Partially Belong to the Secondary Loop System

As long as the SG tubes are intact, the steam and feedwater line penetrations do not perform a containment function; this is provided by the secondary cooling system boundary.



After a SGTR accident, the following isolation valves of the secondary cooling system contribute to the containment function in the long-term:

1) In the event of SGTR, for the main steam isolation valves and steam generator safety relief valves, the SFC applies to the pilot devices instead of the mechanical parts of the main valves themselves;

2) The normal feedwater and emergency feedwater isolation valves outside the containment, and the normal feedwater check valve inside the containment;

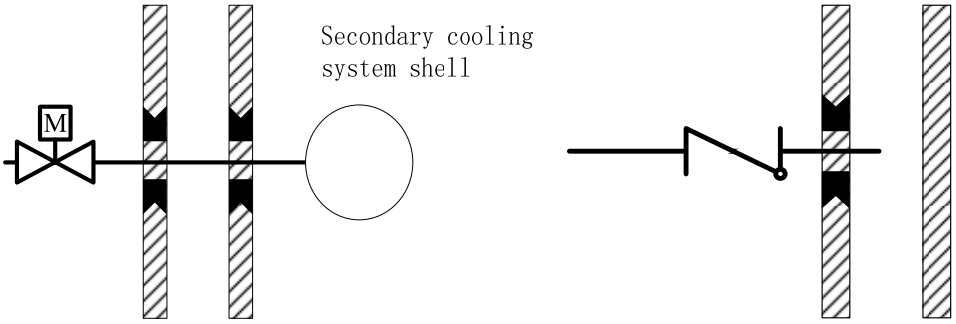
3) The secondary isolation valves from the Steam Generator Blowdown System (APG [SGBS]).

d) Lines Penetrating the External Containment Wall only

1) Lines Penetrating the External Containment Wall only, and Open to the

Containment Annulus Atmosphere

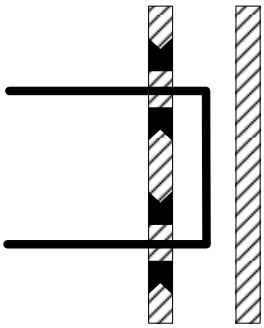
For this type of line, an isolation valve or a check valve is installed outside the containment.



Note: The check valve configuration is acceptable as long as the inter-containment space is at negative pressure.

2) Lines Penetrating the External Containment Wall only, and Closed to the Containment Annulus Atmosphere

This type of lines does not need isolation valves.

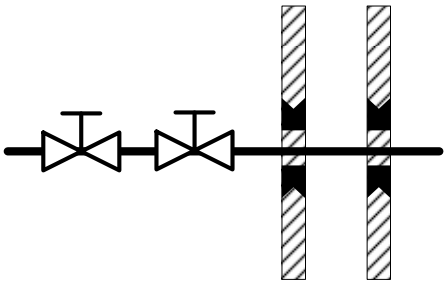


The classification requirement for the pipes in the inter-containment space is the same as the penetrations.

e) Exceptional Lines Penetrating the Containment

This can be an acceptable arrangement if two valves outside the containment structure can provide an equivalent barrier (i.e. can meet all the design requirements) in certain applications. Each valve shall be actuated reliably and independently. Isolation valves shall be located as close as practicable to the structural boundary of the containment.

Therefore, some exceptional ventilation penetrations without lines in the containment can be designed with two containment isolation valves outside the containment, for example, the EUF [CFES] containment isolation valves.



7.4.6.5 Preliminary Design Substantiation

The design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken.

7.4.6.5.1 Compliance with Safety Requirements

a) Compliance with Control of Reactivity Requirements

The containment isolation does not contribute to this safety function.

b) Compliance with Removal of Heat Requirements

The containment isolation does not contribute to this safety function.

c) Compliance with Confinement Requirements

Containment isolation contributes to the confinement of radioactive substances. It minimises the radioactive released through the fluid penetrations into the environment during accidents with fission product release.

Isolation is provided by means of isolation valves (motorised, manual and/or check valves).

d) Compliance with Extra Safety Function Requirements

Containment isolation does not contribute to this safety function.

7.4.6.5.2 Compliance with Design Requirements

a) Compliance with Safety Classification

For the classification of containment, isolation valves are FC1.

Containment isolation valves perform safety functions after a Safe Shutdown Earthquake (SSE).

The containment isolation is designed as SSE1 to withstand the design basis earthquake.

b) Compliance with Reliability

1) Redundancy and the SFC

The principle of the SFC is presented in Sub-chapter 7.2.4.

Redundancy and the SFC applies to all penetrations, with the following exceptions:

The active SFC applies to the pilot devices for these valves instead of the MSIVs (mechanical part of the main valve only) in the event of SGTR.

The passive SFC does not apply to containment penetrations when the isolation function is required. The reasons are as follows:

- The design and construction ensures the quality of the containment penetrations;
- The periodic test and leak rate test prevents the failure of the containment penetrations;
- Current operational experience shows that there is no failure of the containment penetrations.

2) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

Containment isolation is provided with double isolation in different buildings as described in Sub-chapter 7.4.6.4, which can provide independence for containment isolation. The compliance analysis with regards to independence is described in the systems to which the containment isolation valves belong.

3) Diversity

The principle of the diversity is presented in Sub-chapter 7.2.4.

The compliance analysis with regards to diversity is described in the systems to which the containment isolation valves belong.

4) Fail-safe Design

There is no fail-safe design in the containment isolation.

5) Ageing and Degradation

The containment isolation valves and penetrations are designed for the 60-year plant operation. The compliance analysis with regards to ageing and degradation is described in the systems to which the containment isolation valves belong.

7.4.6.5.3 Compliance with Human Factors

The design requirements relevant to the human factors are stated in Chapter 4. The principles and methodology are stated in Chapter 15.

The compliance analysis with regards to the human factors is described in the systems to which the containment isolation valves belong.

7.4.6.5.4 .Compliance with Autonomy

The compliance analysis with regards to the autonomy is described in the systems to which the containment isolation valves belong.

7.4.6.5.5 Compliance with Other Design Requirements

The compliance analysis with regards to other design requirements is described in the systems to which the containment isolation valves belong.

7.4.6.5.6 Compliance with Equipment Qualification

The compliance analysis with regards to the equipment qualification is described in the systems to which the containment isolation valves belong.

7.4.6.5.7 Compliance with Hazard Protection

Containment isolation is protected against hazards. The protection is mainly realised by locating the isolation valves in the reactor building, fuel building and related safeguard buildings.

The measures taken to protect containment isolation against internal and external hazards are provided in the systems to which the containment isolation belongs. The hazard analysis in Chapter 18 and 19 demonstrates that containment isolation is effectively protected during the hazards identified.

7.4.6.5.8 Compliance with Commissioning

The performance of containment isolation valves will be validated by commissioning and testing. The compliance analysis with regards to commissioning is described in the systems to which the containment isolation belongs.

7.4.6.5.9 Compliance with Examination, Inspection, Maintenance and Testing

The containment isolation valves are designed for the 60-year plant operation. The compliance analysis with regards to the EMIT concerning the containment isolation valves is addressed in detail in the related sections of the systems which have containment isolation valves.

7.4.6.5.10 Compliance with Special Thermal-Hydraulic Phenomena

The compliance analysis with regards to the special thermal-hydraulic phenomena is described in the systems to which the containment isolation valves belong.

7.4.6.5.11 Compliance with Material Selection

The compliance analysis with regards to material selection is described in the systems to which the containment isolation valves belong.

7.4.6.5.12 Compliance with Insulation Design

The compliance analysis with regards to insulation is described in the systems to which the containment isolation valves belong.

7.4.6.5.13 Compliance with Decommissioning

The design of the containment isolation valves takes into account the impact on decommissioning. For example, the layout of the containment isolation valves considers the accessibility of personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.4.7 Annulus Ventilation System (EDE [AVS])

The Annulus Ventilation System (EDE [AVS]) is designed to provide negative pressure for the containment annulus during plant normal operation and accident conditions. Detailed information of the EDE [AVS] is presented in Sub-chapter 10.6.

7.5 Safety Injection System (RIS [SIS])

7.5.1 Safety Requirements

The requirements of safety functions on the RIS [SIS] design for the UK HPR1000 are identified in this sub-chapter, Reference [28] and [29].

7.5.1.1 Control of Reactivity Requirements

The RIS [SIS] injects borated water into the Reactor Coolant System (RCP [RCS]) under the conditions of DBC-2/3/4 and Design Extension Condition A (DEC-A) to control the reactivity of the reactor.

7.5.1.2 Removal of Heat Requirements

a) In a loss of coolant accident, the RIS [SIS] contributes to water inventory compensation and the residual heat removal for injecting borated water into the RCP [RCS]. Moreover, LHSI prevents boron crystallization through simultaneous injection of the cold and hot leg.

b) In a Small Break (Loss of Coolant Accident) (SB-LOCA) accident in the RHR mode, the Medium Head Safety Injection (MHSI) pumps shall compensate for the loss of RCP [RCS] water volume (The large minimum flow line of the MHSI pump is in the open state).

c) The RIS [SIS] removes the residual heat from the reactor in the RHR operation mode after DBC-2/3/4 or DEC-A accidents.

d) Under the Total Loss of Cooling Chain (TLOCC) and Station Black Out (SBO) conditions (Reactor Pressure Vessel (RPV) is in the open state), train A and train B of the RIS [RIS] shall compensate for the RCP [RCS] water level drop due to evaporation.

e) In DEC-A accidents, the MHSI pumps and pressuriser safety valves operate in Feed and Bleed (F&B) mode to remove the core decay heat.

f) In accident conditions, the debris entering into the In-containment Refuelling Water Storage Tank (IRWST) is filtered to ensure the uninhibited operation of the RIS [SIS] pump and Containment Heat Removal System (EHR [CHRS]) pump.

7.5.1.3 Confinement Requirements

a) In Intermediate Break (Loss of Coolant Accident) (IB-LOCA) and Large Break (Loss of Coolant Accident) (LB-LOCA) accidents, the heat exchanger downstream of the LHSI pump cools the borated water injected into the core, and limits the steam generated at the breaks by injecting into the cold leg and hot leg simultaneously;

b) As the heat sink in the containment, the IRWST can absorb the heat within the containment. The IRWST together with the LHSI pump and heat exchanger prevent the increase of the containment pressure and temperature;

c) The RIS [SIS] is isolated by the containment isolation valve to prevent radioactive substances from releasing to the environment;

d) In a Steam Generator Tube Rupture (SGTR) accident, MHSI injection pressure is lower than the pressure setting of the Main Steam System (VVP [MSS]) safety valve to prevent radioactive substances from releasing to the environment uncontrollably due to the opening of the main steam safety valve;

e) During cold shutdown, the safety valves on the RHR lines are used to protect the RCP [RCS] against damage under cold overpressure conditions.

7.5.1.4 Extra Safety Function Requirements

The RIS [SIS] shall contribute to supporting the extra functional requirements as follows:

a) Mix and cool IRWST borated water in plant normal operation;

b) Adjust the pH value of the IRWST water source to alkaline after the accident (such as LOCA accident, accidents which require containment spray, etc.);

c) Monitor the pressure and water level of the Accumulator (ACC) in a normal standby state;

d) Monitor the pressure inside the containment after a DBC-2/3/4 accident.

7.5.2 Design Requirements

The general design requirements of the safety systems which need to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to RIS [SIS]:

a) Fail-safe: There is no fail-safe requirement on the RIS [SIS].

b) Autonomy in Respect to the Heat Sink: The RIS [SIS] is not a heat sink system; the autonomy of heat sink is not applicable to the RIS [SIS].

The substantiation analysis of the RIS [SIS] with regards to other design requirements is shown in Sub-chapter 7.5.5.

7.5.3 Design Bases

The RIS [SIS] belongs to the engineered safety systems and consists of three redundant trains. The RIS [SIS] performs its fundamental safety function in all the reactor states. Each LHSI pump of train A and B is equipped with diverse cooling water systems and power supplies, which can cope with SBO and TLOCC conditions.

This sub-chapter aims to provide the main design assumptions considered in the system design.

7.5.3.1 General Assumptions

a) Safety Classification

The LHSI, MHSI and accumulator injection functions are used to reach a controlled state under DBC-2/3/4 conditions (if these functions are not performed, the resulting consequences are high). Therefore, the parts of the RIS [SIS] that perform LHSI, MHSI and accumulator injection functions under DBC-2/3/4 conditions are Function Category 1 (FC1).

The part of the RIS [SIS] that performs RHR functions under DBC-2/3/4 conditions is Function Category 2 (FC2).

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which is important to safety shall be taken into account.

The design life of the main equipment of the RIS [SIS] is 60 years. In addition, some parts of the main equipment need to be replaced regularly during the design life.

c) Autonomy

There is no quantitative autonomy requirement for RIS [SIS].

d) Equipment Qualification

Active components of the RIS [SIS] performing an FC1 or FC2 safety function shall be qualified.

Active components of the RIS [SIS] performing an FC3 safety function required under DEC conditions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

The fluctuation of the electrical power grid may affect the ability of the safety functions, especially performance of the active equipment, such as LHSI and MHSI pumps.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in the RIS [SIS] equipment design, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions such as the confinement function shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.5.3.2 Design Assumptions

The RIS [SIS] injects borated water into the RCP [RCS] under DBC-2/3/4 and DEC-A conditions to compensate for water inventory loss and to remove core residual heat. The requirements for the RIS [SIS] are as follows, Reference [30]:

7.5.3.2.1 Control of Reactivity Assumptions

The RIS [SIS] injects borated water into the RCP [RCS] under the conditions of DBC-2/3/4 and DEC-A to control the reactivity of the reactor.

The requirements for RIS [SIS] injection flow (each train) under accident conditions are listed in Table T-7.5-1 to T-7.5-7.

T-7.5-1 Requirements for LHSI minimum injection flow in the cold leg

T-7.5-2 Requirements for LHSI maximum injection flow in the cold leg

T-7.5-3 Requirements for MHSI minimum injection flow in the cold leg (large miniflow line is closed)

T-7.5-4 Requirements for MHSI maximum injection flow in the cold leg(large miniflow line is closed)

7.5.3.2.2 Removal of Heat Assumptions

a) Safety injection flow and accumulator

In a loss of coolant accident, the RIS [SIS] contributes to water inventory compensation and residual heat removal for injecting borated water into the RCP [RCS]. The MHSI and LHSI injection flow is presented in Sub-chapter 7.5.2.2.1, and the requirements for the accumulator are shown in Table T-7.5-5.

T-7.5-5 Requirements for the accumulator

In a Small Break (Loss of Coolant Accident) (SB-LOCA) in the RHR mode, the Medium Head Safety Injection (MHSI) pumps shall compensate for the loss of RCP [RCS] water volume (The larger minimum flow line of the MHSI pump is in the open state). The injection flow is presented in T-7.5-6 and T-7.5-7.

T-7.5-6 Requirements for MHSI minimum injection flow in the cold leg (large miniflow line is open)

T-7.5-7 Requirements for MHSI maximum injection flow in the cold leg (large miniflow line is open)

b) RHR exchanger design

Following an accident, the RIS [SIS] can be connected to the RCP [RCS] in RHR mode once the RCP [RCS] pressure and average temperature decrease to { } and { } respectively. One train of the RHR system is sufficient to remove the residual heat from the core and maintain the primary temperature below { }.

c) Strainer design

The strainer is designed to retain the smallest debris that could lead to the clogging of internal parts of the fuel assemblies.

The surface of the strainer is large enough to ensure the normal operation of the RIS [SIS] and EHR [CHRS] pump after accidents.

7.5.3.2.3 Confinement Assumptions

a) RHR safety valves

Safety valves are equipped to each hot leg suction line to protect the RIS [SIS] from overpressures. The set pressure of the safety valves is { }, and the minimum discharge flow rate is { }.

b) IRWST volume

The water volume of the IRWST shall meet the following requirements:

1) The water volume of the IRWST needs to meet the refuelling requirements;

2) The water volume of the IRWST needs to ensure that the RIS [SIS] and EHR [CHRS] pump can operate normally after accidents;

According to the above analysis, during normal operation the minimum water inventory of the IRWST should be greater than { }.

c) MHSI maximum injection pressure

In case of the a SGTR accident, MHSI injection pressure is lower than the pressure setting of the VVP [MSS] safety valve, the maximum MHSI injection pressure shall not exceed{ }.

7.5.3.2.4 Extra Safety Function Assumptions

a) Mixing and cooling of the IRWST borated water in plant normal operation and the temperature of the IRWST shall no more than { } in plant normal operation;

b) The RIS [SIS] shall adjust the pH value of the RWST water source to alkaline after accidents (such as LOCAs , accidents when containment spray is required, etc.).

c) Pressure and water level instruments need to be installed on the accumulator.

d) The pressure monitoring of the containment after the accident needs to meet SFC criterion, therefore at least two pressure monitoring instruments are required.

7.5.4 System Description and Operation

7.5.4.1 System Description

7.5.4.1.1 General System Description

The RIS [SIS] consists of three independent trains (one train corresponds to one RCP [RCS] loop), and each train is located in a separate safeguard building. Moreover, the RBS injects the borated water into the RCP [RCS] via the RIS [SIS] cold leg injection line. The material contacting with borated water in the RIS [SIS] is stainless steel .The simplified flow diagram of the RIS [SIS] is shown in Figure F-7.5-1, Reference [30].

The basic configurations of the 3 trains are the same except for the differences outlined below:

a) Only trains A and B are connected to the RCV [CVCS] for purification;

b) Only trains A and B are connected to the EHR [CHRS] for strainer backflushing.

The pumps of all three trains are cooled by the Component Cooling Water System (RRI [CCWS]). The pump motors in train A and train B can also be cooled by the Safety Chilled Water System (DEL [SCWS]) (for diversification). Each train of the RIS [SIS] is composed of the Low Head Safety Injection (LHSI), Medium Head Safety Injection (MHSI) and Accumulator (ACC) sub-systems. The IRWST is shared by all 3 RIS [SIS] trains [28].

a) MHSI Sub-system

The MHSI sub-system consists of the following equipment:

1) The MHSI pump;

2) The suction line from the IRWST and associated valves;

3) The discharge line and associated valves.

The MHSI pumps take water from the IRWST and inject it into the connected RCP [RCS] cold leg.

b) ACC

The ACC sub-system is a passive system, located inside the Reactor Building (BRX). The accumulator is connected to the safety injection line. The accumulator is filled with borated water and is pressurised by nitrogen. If the pressure of the RCP [RCS] falls below the ACC pressure under accident conditions, it will automatically inject borated water into the RCP [RCS]. The ACC will be isolated when the RCP [RCS] pressure reaches 70bar abs during normal shutdown. The ACC will also be isolated, due to low pressure, to avoid nitrogen injection under accident conditions.

During power operation of the plant, the motor-operated isolation valve downstream of the accumulator is open and the accumulator will pressurise the line between the two RCPB isolation valves to prevent occurrence of dead leg phenomena.

c) LHSI Sub-system

The LHSI sub-system consists of:

1) The LHSI pump;

2) The heat exchanger;

3) The bypass line of the heat exchanger with an associated control valve;

4) The suction line from the IRWST;

5) The discharge line to the Cold Leg;

6) The discharge line to the Hot Leg;

7) The suction line from the RCP [RCS] Hot Leg.

The LHSI pump draws borated water from the IRWST to perform LHSI function. The borated water is injected into the cold leg of the corresponding loop of the RCP [RCS] after passing through the RHR heat exchanger downstream of the pump. The LHSI can be switched to simultaneous injection into both the cold leg and hot leg of the same RCP [RCS] loop.

When performing the RHR function, the LHSI pump draws borated water from the RCP [RCS] hot leg. After passing through the residual heat removal heat exchanger downstream of the pump, the cooled borated water is injected into the cold leg of the corresponding loop of the RCP [RCS].

RIS [SIS] trains A and B are connected to the RCV [CVCS] low pressure letdown line for purification of the primary coolant when primary coolant pressure is low.

d) IRWST

The IRWST is an open structure and constructed with concrete and a stainless steel liner, located in the bottom of the reactor building. The water inventory is sufficient to provide refueling or for RIS [SIS] and EHR [CHRS] operation following an accident.

The IRWST is equipped with a liner leakage monitoring device: embedded pipes collect leaks into a collecting sump and leakages are then sent to Nuclear Island Vent and Drain System (RPE [VDS]) sump via a mobile RPE pump.

In order to ensure the reliable operation of the RIS [SIS] and EHR [CHRS] pumps after an accident, the IRWST is equipped with a filtering system which intercepts and filters any debris washed into the IRWST. The filtering system contains：

1) The weirs: Sills placed around openings in the heavy equipment installation floor. They encourage sedimentation upstream of the openings in the event of a break;

2) The trash racks: Wide mesh grids placed above the openings in the heavy equipment installation floor. The robust cage-shaped grids are used to retain the large debris;

3) The retaining baskets：They collect debris entering the IRWST to reduce the quantity of debris entering into filters;

4) The filters: The filters are placed above the RIS [SIS] and EHR [CHRS] sumps. The filter mesh size shall be smaller than the smallest restrictions of

the fuel assembly canals to guarantee core cooling. The filtering area of the sump filters is large enough to ensure that the pressure loss across filters meets the requirements of the Net Positive Suction Head (NPSH) and the requirements of the RIS [SIS] pump and EHR [CHRS] pump under a LOCA.

e) pH level control

The passive pH adjustment basket adjusts the pH value of the water inside the containment after accidents, such as LOCAs, accidents where containment spray is required, etc.

The adjustment basket containing granulated Tri-Sodium Phosphate (TSP) is made of stainless steel with a meshed front which permits TSP contact with water. The basket is placed in the reactor building and in the water flow path to the IRWST after the occurrence of a LOCA, accidents where containment spray is required, etc.

In the case of a LOCA, the borated water flowing from the break dissolves the TSP granules in the basket and enters into the IRWST. The TSP is designed to maintain the pH value of the water inside the IRWST above 7.0. This chemical characteristic of the water can keep the radionuclides (particularly the iodine) in the sump water of the containment, so that the radioactive iodine cannot escape from the solution long after the accident occurred. As a result, the radioactivity released to the environment can be reduced. In addition, this chemical characteristic reduces the possibility of stress corrosion arising from chloride being released from the concrete of the containment.

7.5.4.1.2 Description of Main Equipment

a) LHSI pump

The LHSI pump is a horizontal multi-stage centrifugal pump made of stainless steel, installed in the safeguard building horizontally. The RRI [CCWS] provides cooling water for the motor and the mechanical seal of the LHSI pump, Reference [30].

The main design characteristics of the LHSI pump are listed in Table T-7.5-8.

T-7.5-8 Main design characteristics of the LHSI pump

Parameters	**Value**	**Unit**
Type	Multi-Stage Centrifugal Pump	
Design Lifespan	60	yr.

Parameters	Value	Unit
Nominal Flowrate	See Sub-chapter 7.5.5.1	m^3/h
Nominal Discharge Head	See Sub-chapter 7.5.5.1	m
Material	Stainless Steel	

b) MHSI pump

Under a LOCA, the MHSI pump is used for emergency water replenishment to the RCP [RCS], and to supplement the water loss of the RCP [RCS]. According to the operation state of the RCP [RCS], the MHSI pump has two operating modes, Reference [30]:

1) When a LOCA occurs during normal power operation, the MHSI pumps inject borated water to the RCP [RCS], the MHSI pump large miniflow line is closed and the low miniflow line is opened.

2) When a LOCA occurs during the RHR mode, the MHSI pumps will supplement for the water loss of the RCP [RCS] and both the MHSI pump large miniflow line and low miniflow line are opened.

The MHSI pump can also be used for filling the accumulator with water.

The MHSI pump is mainly composed of a pump, motor, coupling, coupling guard, pump base, motor base and monitoring system.

The pump is designed as a multistage, horizontal centrifugal pump, with a horizontal suction nozzle and a vertical discharging nozzle. It mainly consists of casings, a cartridge, bearings, mechanical seals and flushing parts.

The flexible coupling is used, between the pump and the motor, to transmit power. The coupling shall be safely and reliably locked on the shaft. The coupling is designed with an intermediate shaft coupling with adequate dimensions in order to remove the bearing and mechanical seal without removing the motor.

The pump uses single end, self-balanced, and cartridge type mechanical seals. To prevent leakage between the mechanical seal and the shaft (sleeve), the static seal shall be set between the mechanical seal and the shaft (sleeve). The mechanical seal can easily be repaired or replaced.

The driving motor of the pump is a 10kV/500kW/3000rpm AC asynchronous motor, lubricated by grease. The motor is cooled by RRI [CCWS] water.

The pump set shall be easily maintained, tested, assembled and disassembled.

The MHSI pump is installed in the safeguard building horizontally.

The main design characteristics of the MHSI pump are listed in Table T-7.5-9.

T-7.5-9 Main design characteristics of the MHSI pump

Parameters	**Value**	**Unit**
Type	Multi-Stage Centrifugal Pump	
Design Lifespan	60	yr.
Nominal Flowrate	See Sub-chapter 7.5.5.1	m^3/h
Nominal Discharge Head	See Sub-chapter 7.5.5.1	m
Material	Stainless Steel	

c) Residual heat removal heat exchanger

Under normal shutdown states, the RIS [SIS] operates in the RHR mode and performs the function of RHR, and the RIS [SIS] cools the primary coolant loop to the cold shutdown state by the operating the RHR heat exchanger, Reference [30].

Under the accident conditions, the RHR heat exchanger is used to remove decay heat from the core continuously and steadily and make the plant enter the safe state or final state.

The RHR heat exchanger is a U-tube heat exchanger, installed in the safeguard building horizontally. The tube side flow of the heat exchanger is the coolant from the primary coolant or the borated water from the IRWST, and the shell side flow is the component cooling water provided by the RRI [CCWS].

The main components of the heat exchanger are the following:

1) The hemispherical head which receives the primary water, the primary partition plate and the manhole;

2) The tube sheet and U- tubes;

3) The shell;

4) The fixed support;

5) The sliding support.

The main design parameters of the RHR heat exchanger are shown in Table T-7.5-10.

The main material of the RHR heat exchanger is stainless steel (hot side) and

carbon steel (cold side).

The machining, heat treatment and protection of all surfaces of the RHR heat exchanger shall comply with the provisions of the RCC-M code. The final size of the parts shall conform to the requirements of the design drawings.

Non-destructive inspection tests of the RHR heat exchanger components during fabrication shall comply with the requirements of RCC-M.

The pre-service and in-service inspection of RHR heat exchanger are subject to the requirements of the RSE-M code.

T-7.5-10 Main design characteristics of the RHR heat exchanger

Parameters	**Value**		**Unit**
Type	Tubular		
	Hot Side	Cold Side	
Design Thermal Load	8.96		MW
Medium	Reactor coolant	Demineralised water (RRI [CCWS])	
Design Pressure	8	1.35	MPa (g)
Design Temperature	180	90	°C
Design Flowrate	522	850	t/h
Material	Stainless Steel	Carbon steel	

d) ACC

The accumulator is a vertical cylindrical storage tank with hemispherical upper and lower heads, Reference [30].

T-7.5-11 Main design characteristics of the ACC

Parameters	**Value**	**Unit**
Type	Cylindrical Tank with Hemispherical Head	
Medium	H_3BO_3 N_2	1300~1400 mg/kg, 35 % concentration in ^{10}B

Parameters	Value	Unit
Design Pressure	5.5	MPa (g)
Design Temperature	120	°C
Usable Volume	35-38	m^3
Max. Volume	50	m^3
Material	Carbon steel with a austenite stainless steel liner in contact with boric acid	

e) IRWST

The IRWST is located in the bottom of the reactor building, between the reactor pit and inner containment, which adopts a double ring structure design. The inner and outer ring are "C" type structures and the inner and outer ring pool are connected through three channels.

The inner ring pool is connected to the air through three openings of the heavy equipment installation floor. The outer ring pool is located at the bottom of the annular space floor, and surface of its liquid is in contact with the floor.

The IRWST provides water for the operation of the RIS [SIS] pump and EHR [CHRS] pump during refuelling and accidents. The boron concentration of the water inside the IRWST is 1300-1400 mg/kg (^{10}B with an enrichment of 35%). The water inventory of the IRWST meets the requirement for refuelling. The water level of the IWRST ensures that all pumps drawing water from the IRWST have sufficient Net Positive Suction Head Available (NPSHa) even in accident conditions.

f) Strainer

Three RIS [SIS] strainers and two EHR [CHRS] strainers are arranged in the IRWST. The strainer is designed as a circular hole with a diameter of 2.5mm (both the RIS [SIS] and EHR [CHRS] strainers) to prevent debris from blocking the cooling channel of the fuel assembly.

The strainer debris source analysis content mainly includes the following aspects：

1) Identification of debris source；
2) Selection of the break；
3) The analysis of debris generation；
4) The analysis of debris transport.

The surface of the strainer is large enough to ensure that the normal operation of the RIS [SIS] and EHR [CHRS] pumps after accidents.

The RIS [SIS] and EHR [CHRS] strainers will conduct relevant experimental verification, such as strainer qualification tests, etc., to ensure the performance of the strainer.

The safety case related to the strainer will be developed.

7.5.4.1.3 Description of Main Layout

All main equipment of the RIS [SIS] (including the LHSI pumps, MHSI pumps and residual heat exchanger) are arranged in the safeguard buildings, while the three trains of the RIS [SIS] are located in three separate safeguard buildings, Reference [31].

Except for the equipment mentioned above, the ACC and IRWST are arranged in the containment. The IRWST is at the bottom of containment. The reactor coolant leaks from the breaks enters into the IRWST through the return passage of the reactor building in LOCAs , so the safety injection pump and EHR [CHRS] pump can still take water from the IRWST after the accident without switching to the sumps.

The suction lines of the LHSI and MHSI pump are kept in one direction to prevent gas accumulation in the lines. The IRWST provides borated water to ensure that the suction lines of the pumps are always filled with water, thus the pump can operate safely. The corresponding vent and drain lines are arranged at the high point and low point of the pipelines in the RIS [SIS]. The initial water filling and gas venting can ensure that no air exists in the lines of the system.

The 3 trains of the RIS [SIS] are located in separated safeguard buildings. The RIS [SIS] inside the containment is physically segregated by the physical arrangement. Therefore, single internal or external damage will affect only one train of the RIS [SIS]. There will be no common mode failure, and the safety function performed by the RIS [SIS] will not be affected.

The equipment and lines of the RIS [SIS] are installed in a building of Seismic Category 1 (SSE1), meeting the requirement of SSE1. The RIS [SIS] will continue to perform the safety functions under external disasters such as earthquakes and extreme weather.

7.5.4.1.4 Description of System Interface

The systems supporting the fulfilment of RIS [SIS] functions are as follows, Reference [30]:

a) RRI [CCWS]

The RRI [CCWS] cools the heat exchanger, pump motor and mechanical seal of the LHSI pump.

b) SGN [NDS]

Provides nitrogen covering for the ACC.

c) PTR [FPCTS]

Purifies the IRWST.

7.5.4.1.5 Instrumentation and Control

The RIS [SIS] will start up automatically at the signal of "SI":

a) Operation mode A

Operation mode A includes power operation and hot shutdown. The signal of pressuriser pressure low 3 will trigger safety injection in this mode.

b) Operation mode B and C (RCP [RCS] pump running)

1) Operation mode B refers to the shutdown condition where the average temperature of the coolant is higher than 140 °C.

2) The operation mode C refers to the shutdown condition when the RIS [SIS] operates in the RHR mode (at least one RCP [RCS] pump is running).

A △Psat low 1 signal from the hot leg will trigger safety injection in these two modes.

c) Operation mode C and D (RCP [RCS] pump is not running)

1) Operation mode C refers to the shutdown condition during which the RIS [SIS] operates in the RHR mode (with no RCP [RCS] pump running).

2) Operation mode D refers to the cold shutdown state when the RCP [RCS] is open.

The signal of the RCP [RCS] hot leg water level low 1 will trigger safety injection in these two modes.

d) RIS [SIS] operation in RHR mode can be achieved manually.

e) The RIS [SIS] can be started and stopped manually by the operator in the main control room when necessary.

The following parameters are monitored when the RIS [SIS] is on standby or in operation:

a) Water level and pressure inside the ACC;

b) Water level and temperature inside the IRWST;

c) Flow rates of the LHSI pump and MHSI pump;

d) Water level in safeguard building sump;

e) Pressure in safeguard building.

7.5.4.2 System Operation

7.5.4.2.1 Plant Normal Operation

a) Power operation

When the reactor is in power operation, hot shutdown and hot standby, the safety injection lines are filled with borated water. The safety injection pumps (LHSI pump and MHSI pump) are in standby state. They can start to perform the safety injection functions (automatically or manually) at any time after receiving the safety injection signal.

To prevent inadvertent dilution, the RRI [CCWS] is separated from the residual heat removal heat exchanger (shell side) of the RIS [SIS] and the mechanical seal cooling of the LHSI pump while the cooling circuit of the pump motor is in operation.

The accumulator is applying pressure to the dead leg between two RCPB isolation valves. All RCPB isolation valves on the lines connected with the RCP [RCS] are closed. The temperature and pressure monitoring instruments in the lines between two RCPB isolation valves can detect possible leakage of the RCPB isolation valves, Reference [32].

b) Reactor start-up

In start-up condition of the power plant, the RIS [SIS] connects with the RCP [RCS] to run in RHR mode when the RCP [RCS] is in water solid state. At least 2 RHR trains are in operation to prevent cold overpressure. The operation of RHR is to mix the RCP [RCS] coolant to homogenise the boron concentration and control the heating rate of the RCP [RCS]. In this case, the pressure of the RCP [RCS] is controlled by the RCV [CVCS].

c) Operation mode of RIS/RHR cooling normal shutdown

In the process of normal shutdown, train A and train B RHR systems operate to cool the primary system when the primary temperature and pressure decrease to be lower than 140℃ and 3.2MPa respectively, When the reactor coolant is cooled to 100℃, the train C RHR system will start up to accelerate the cooling rate. The RHR system is designed to ensure that the reactor coolant can be cooled to the cold shutdown condition within the required time.

Before switching to RHR mode, it is necessary to perform temperature regulation and chemical regulation for the water in the pipe to prevent thermal shock to pumps caused by high-temperature coolant and the inadvertent dilution of reactor

coolant.

When the RIS [SIS] is operating in RHR mode, the coolant flow passing through the residual heat removal exchanger is regulated by the temperature control valve to control the cooling rate of reactor coolant.

d) Mode of maintenance cold shutdown

In the mode of maintenance cold shutdown, the RIS [SIS] connecting with the RCP [RCS] still runs in RHR mode to keep the RCP [RCS] temperature at the cold shutdown condition. Before opening the Reactor Pressure Vessel (RPV) cover, at least two trains of RIS [SIS] run in RHR mode to protect the RCP [RCS] (to prevent damage under cold overpressure). The left train can be in operation, on standby or fill the reactor pool with water.

The number of RIS [SIS] trains running in RHR mode depends on the thermal load in the maintenance cold shutdown condition after the RPV cover opens.

7.5.4.2.2 Plant Accident Conditions

a) LOCA

1) During a SB-LOCA (including SGTR), the RIS [SIS] injects borated water into the RCP [RCS] to compensate for the RCP [RCS] water inventory loss via the break. Both the MHSI pump and LHSI pump take water from the IRWST. The MHSI pump will start to compensate water for the RCP [RCS] as soon as the primary pressure falls below the injection pressure of the MHSI pump. The LHSI pump injects water to the primary loop when the primary pressure is below the injection pressure of the LHSI pump.

In the controlled state, the RIS [SIS] injects water to ensure the primary water inventory and core cooling. The residual heat is removed by the break flow and steam generator. The Main Feedwater Flow Control System (ARE [MFFCS]) or ASG [EFWS] (if ARE [MFFCS] is unavailable) can ensure the feedwater supply of the steam generator.

The safe state is defined as a state in which the break flow rate is compensated by the MHSI flow rate and at least one RIS [SIS] train is connected to the RCP [RCS] in RHR mode. In this state, the RCP [RCS] makeup is performed by the MHSI pumps; the small miniflow lines of which are continuously open to reduce the MHSI pumps discharge pressure.

When the RCP [RCS] pressure is less than 3.2MPa and the temperature is below 180℃, the LHSI train can be switched to the RHR mode to remove the residual heat (under accident condition, the temperature for connecting the RIS [SIS] in RHR mode is 180℃, and one RHR train is sufficient to remove the residual core heat).

2) During Intermediate Break(Loss of Coolant Accident) (IB-LOCA) and LB-LOCA

The action of the RIS [SIS] is the same as that of the SB-LOCA accident. The safety injection line of the LHSI can be switched to the simultaneous injection mode to the cold leg and hot leg (operated by the operator manually) if necessary. In this way, evaporation can be limited through the breaks, the steam entering into the containment be reduced, and containment overheating and over pressure can be prevented. In addition, this safety injection mode can also reduce the boron concentration in the core to avoid the crystallisation of boron on the fuel (boron crystallisation will reduce the heat transfer efficiency of the fuel).

b) Main Steam Line Break

In a MSLB accident, the MHSI pump injects borated water into the RCP [RCS] to control the reactivity of the reactor.

The safety injection signal starts the VDA [ASDS] to cool the primary coolant loop. When the pressure of the RCP [RCS] drops to the injection pressure of the MHSI pump, the MHSI pump injects the borated water into the RCP [RCS] cold leg to compensate for the contraction of the reactor coolant. After the manual intervention from the operator, the RBS [EBS] is initiated (or the RCV [CVCS] if it is available) to inject boron into the primary coolant loop. The RIS [SIS] and RBS [EBS] provide the necessary boron to the core to compensate for the reactivity insertion, so the core can be maintained at or returned to the subcritical state. When the primary coolant loop reaches the RHR connecting conditions, the RIS [SIS] will operate in the RHR mode to enable the plant to enter the safety state.

c) Other accidents

Following other accidents, when the primary pressure and temperature decrease to be lower than 3.2MPa and 180℃ respectively, the residual heat removal system can connect to the RCP [RCS]. If the single failure and initiating event lead to the loss of two trains, the remaining train of the residual heat removal system connected can take away the residual heat from the core and keep the RCP [RCS] temperature below 180℃.

7.5.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. Detailed design of the system is presented in Reference [29], [30] [31], [32] and [33]. Furthermore, design substantiation of RIS [SIS] is estimated in the fault study in Chapter 12 and 13.

7.5.5.1 Compliance with Safety Requirements

a) Control of reactivity

The RIS [SIS] injects borated water (1300~1400 mg/kg, 35 % concentration ^{10}B) into the RCP [RCS] under the conditions of DBC-2/3/4 and DEC-A to control the reactivity of the reactor.

The fault study in Sub-chapter 12.9 and 13.5 justifies that each safety function required of the RIS [SIS] in Sub-chapter 7.5.1.1 is met based on the design assumptions provided in Sub-chapter 7.5.3.2.1, including the LHSI and MHSI injection flowrate.

According to the requirements in Sub-chapter 7.5.3.2, the parameters required of MHSI and LHSI pumps are presented in Table T-7.5-12 to T-7.5-15. More detailed parameter information is shown in Reference [30]. These parameter requirements are presented into the equipment technical specifications. The equipment supplier shall meet the requirements according to the specifications.

T-7.5-12 LHSI pump performance requirements (minimum head requirement)

T-7.5-13 LHSI pump performance requirements (maximum head requirement)

T-7.5-14 MHSI pump performance requirements (minimum head requirement)

T-7.5-15 MHSI pump performance requirements (maximum head requirement)

b) Removal of heat

In DBC-2/3/4 or DEC-A conditions, RIS [SIS] operates in RHR or safety injection mode to continuously remove the reactor core residual heat. The RIS [SIS] can perform the safety function of the residual heat removal during all required conditions. Each RIS [SIS] train is designed with sufficient capacity to perform the required safety function. The instrumentation and control of the RIS [SIS] also ensure effective operation of the system.

The fault study in Sub-chapter 12.9 and 13.5 justifies that each safety function required of the RIS [SIS] in Sub-chapter 7.5.1.2 is met based on the design assumptions provided in Sub-chapter 7.5.2.2.2, including the LHSI, MHSI and ACC injection flowrate.

The parameters required of the MHSI and LHSI pumps are shown in Reference [30]. These parameter requirements are presented into the equipment technical specifications and the equipment supplier shall meet the requirements according to the specifications. The design parameters of the accumulator are as follows:

T-7.5-16 Design parameters of the accumulator

When the RCP [RCS] temperature is 180℃, one train of the RHR heat exchanger can remove at least 43MW thermal, which is higher than the residual heat from the core and can therefore maintain the primary temperature below 180℃.

The RIS [SIS] strainer is designed as circular hole with a diameter of{ }. The diameter of the strainer is smaller than the minimum clearance between fuel rods in the fuel assembly.

The filtration surface of each strainer is about 89m^2. The pressure loss of the

strainer is { }and the LHSI and MHSI pumps have enough NPSHa after accident to ensure the normal operation of the pump.

c) Confinement

To ensure the integrity of the RCPB, two valves are provided for the isolation of the RCPB (the hot leg RCPB isolation valves are electric isolation valves, the cold leg RCPB isolation valves are check-valves).

To ensure the integrity of the containment, each containment penetration is equipped with two containment isolation valves in the RIS [SIS] (the hot leg and external containment isolation valves are electric isolation valves; the cold leg internal containment isolation valves are check-valves).

The RHR safety valve design requirements (setting pressure, minimum discharge flow etc.) will be presented in the technical specifications and the equipment supplier will meet the requirements according to the specifications.

The normal water volume of the IRWST is approximately 1944 m^3, which meets the water volume requirements of refuelling and normal operation of the pump after accidents.

The suction line drawing water from the IRWST (between the part inside the containment and the isolation valves) is of a double-sleeve type. The double wall is an extension of the third barrier (containment). It is specified against the same conditions as the shell of the containment. The space between the internal pipe and the sleeve is filled with compressed air. A pressure monitor is adopted to detect the presence of leaks of internal pipes.

The injection pressure of the MHSI pump is lower than the set pressure of the MSSV to prevent these valves from being opened in SGTR accidents, and thus to prevent the radioactive substances from being released into the atmosphere in large quantities.

d) Compliance with Extra Safety Function Requirements

1) In plant normal operation, the RIS [SIS] can cool and mix the IRWST through the LHSI pump and miniflow line to ensure correct temperature and boron concentration in the IRWST. Detailed information is presented in Reference [33].

2) The TSP is designed to maintain the pH value of the water inside the IRWST greater than 7. The total weight of TSP is about 5.6×10^3kg.

3) Three pressure and water level instruments are installed on the ACC to monitor the pressure and water level of the ACC in normal standby state.

4) Four redundant pressure instruments are installed in the containment to

monitor the pressure of the containment after design basis conditions.

7.5.5.2 Compliance with Design Requirements

7.5.5.2.1 Compliance with Safety Classification

The RIS [SIS] design is compliant with the requirements described in Sub-chapter 4. The safety classification of RIS [SIS] functions is listed in Table T-7.5-17 and the safety classification of main components is listed in Table T-7.5-18.

The RIS [SIS] is designed to withstand a SSE. The main components are classified as SSE1 in Table T-7.5-18.

The documents relevant to the equipment classification will be delivered.

T-7.5-17 System Function Classification

System Function	**Function Category**
LHSI cold leg safety injection	FC1
MHSI cold leg safety injection	FC1
LHSI hot leg safety injection	FC2
RHR mode following an accident	FC2
Containment isolation	FC2
RCPB isolation	FC1

T-7.5-18 Classification for Components

Component	**Function Class**	**Design Provision Category**	**Design Provision Class**	**Seismic Category**
Containment Isolation Valves	F-SC2	DPA	B-SC2	SSE1
RCPB Isolation Valve	F-SC1	DPA	B-SC1	SSE1
MHSI Pump	F-SC1	DPA	B-SC2	SSE1
LHSI Pump	F-SC1	DPA	B-SC2	SSE1

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
RIS [SIS] heat exchanger	F-SC2	DPA	B-SC2	SSE1
Accumulators	F-SC1	NC	NC	SSE1
pH adjustment basket	F-SC3	---	---	SSE1

7.5.5.2.2 Compliance with Reliability

a) Redundancy and SFC

The principle of the SFC is presented in Sub-chapter 7.2.4.

The RIS [SIS] is designed of 3 redundant trains (no connection between any two of the trains), each with 100% capacity under accident conditions. Even under the most conservative assumption, that if one train cannot work as a result of a single failure and another cannot work as a result of an initiating event, the remaining train can perform the function of the RIS [SIS].

The IRWST isolation function considers passive single failure, and therefore the intake pipes between the IRWST and the isolation valves are fitted with a double wall. In the event of passive failure of the pipes upstream of the IRWST isolation valves, the water of the IRWST is retained by the double wall.

In the case of a LOCA, the passive SFC of the RIS [SIS] accumulator check valves failing to open is not considered when implementing the safety injection function.

The prevention of the passive SFC 24 hours after the postulated initiating event is the same as for the active SFC, i.e. one train can still preform the safety function if a passive SFC occurs on one train of the RIS [SIS].

The detailed design results of the RIS [SIS] is presented in Reference [29] [30] and [32].

b) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The RIS [SIS] consists of three independent trains (one train corresponds to one RCP [RCS] loop), and each train is located in a separate safeguard building. There is no cross connecting between each train.

c) Diversity

The principle of diversity is presented in Sub-chapter 7.2.4.

The diversity design in the RIS [SIS] contains:

1) All three train pumps are cooled by the Component Cooling Water System (RRI [CCWS]). The pump motors in train A and train B can also be cooled by the Safety Chilled Water System (DEL [SCWS]);

2) The LHSI Pump and MHSI Pump can inject water to cold or hot leg;

3) Each RIS [SIS] train is supplied by an electrical division and backed-up by the Emergency Diesel Generators (EDG). Furthermore the power of trains A and B of the RIS are supplied by the SBO diesel generators in the event of loss of the EDGs.

The detailed design results of the RIS [SIS] are presented in Reference [29] and [30].

d) Fail-safe Design

Not applicable.

e) Ageing and Degradation

The system is designed for the 60 year long plant operation. The design life of the main equipment of the RIS [SIS] is 60 years, which mainly includes the:

1) LHSI pump;

2) MHSI pump;

3) Accumulator;

4) RHR heat exchanger;

5) Strainer.

However, some components of the pumps need to be replaced regularly according to manufacturer feedback (such as gaskets, mechanical seals, O-ring and bearings).

The performance of equipment is guaranteed through life examination, inspection maintenance and testing and by monitoring during normal operation. Thus it can be ensured that ageing effects will not compromise safety performance. The detailed design arrangement around EMIT and equipment monitoring is presented in Reference [33].

The system layout design can ensure the accessibility and requirement for safety equipment in-service inspection and periodic tests including the necessary NDT

are met. This also includes the requirements of emergency and scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [31].

7.5.5.2.3 Compliance with Human Factors

The design requirements relevant to human factors are stated in Chapter 4. The principles and methodology are stated in Chapter 15.

The RIS [SIS] takes the following measures to prevent human error:

a) The signals from Reactor Protection System (RPR [RPS]) can automatically start and stop the LHSI and MHSI pumps.

b) The RIS [SIS] is equipped with relevant instruments to monitor the operation of the system, such as the temperature and vibration instruments on the pumps, the flowrate instruments on the pipe, etc. These instruments provide the operators with necessary information, so that the operators can clearly understand the operational status of the system.

c) The RIS [SIS] has relevant alarms, such as the accumulator water temperature and pressure alarm and the IRWST temperature and water level alarm. These alarms can be used to remind operators to take necessary measures.

d) The normal operation environment of equipment can be ensured by Heating, Ventilation and Air Conditioning Systems (HVAC).

The system design as well as the control function design of the RIS [SIS] does not require short term operator intervention. Based on the RIS [SIS] design result, no operator action is required within 30 minutes after initial event. The design information is presented in Reference [30] and [32].

It should be noted that there are operator actions during plant normal operation or accident conditions (including plant startup, shutdown, and maintenance or testing etc.). Relevant human actions which are important to plant safety will be further identified and evaluated in the human factors safety case (which is started from Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of the human factors discipline. Relevant evaluated reports will be provided as references of Chapter 15.

7.5.5.2.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in Reference [1]. The RIS [SIS] satisfies the requirement through the following design:

1) The MHSI pump and LHSI pump are started automatically following the

injection signal under the accident condition. No human operation from the Main Control Room (MCR) is required within 30 minutes from the first significant signal;

2) All valves performing safety functions are electric valves which can be operated at the MCR. No human operation outside the MCR is required within 1 hour from the first significant signal.

The design of the RIS [SIS] fulfils these principles via the control function design which is presented in Reference [32]. The design result has been estimated in the safety analysis.

b) Autonomy in Respect to the Heat Sink

Not applicable.

c) Autonomy in Respect to Power Supply Systems

All of the electrical equipment supporting the safety functions can be powered by appropriately qualified emergency power provisions. Each RIS [SIS] trains power is supplied by a separate electrical division and backed-up by the Emergency Diesel Generators (EDGs). Furthermore, the power of trains A and B of the RIS [SIS] are supplied by the Station Black Out (SBO) diesel generators in the event of loss of the EDGs. The valves that perform safety functions are also equipped with 2h or 12h batteries.

7.5.5.2.5 Compliance with Other design requirements

c) Prevention of Harmful Interactions of Systems Important to Safety

According to Reference [1], the protection of interfacing systems shall be considered in RIS [SIS] design. The RIS [SIS] takes the following measures to prevent the harmful interactions of systems:

1) Provide adequate isolation (e.g. using double isolating valves) between RIS [SIS] and interfacing systems;

2) The design pressure of the isolation valve between the RIS [SIS] and the interface system adopts the larger pressure;

3) The RIS [SIS] is equipped with safety valves to prevent the system from being damaged under overpressure.

Detailed information is presented in Reference [32] [33].

d) Considerations Related to the Electrical Power Grid

According to Reference [1], the functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid.

The fluctuation of the electrical power grid mainly affects the functional capability of the MHSI pumps and LHSI pumps. The pump flowrate will vary due to the fluctuation of the power grid. In the HPR1000 (FCG3) project，the design of MHSI pumps and LHSI pumps considers the influence of grid fluctuation [30]. Re-estimates will be carried out during the GDA progress, on the basis of the UK site, relevant to the electrical power grid.

7.5.5.2.6 Compliance with Equipment Qualification

According to Chapter 4, all components performing the safety functions shall operate under accidental condition as well as normal conditions, thus the components shall withstand the adverse ambient environments.

The equipment that performs an FC1 or FC2 function in the RIS [SIS] will be qualified in accordance with the requirements described in Chapter 4.

The equipment that performs an FC3 function under DEC conditions in the RIS [SIS] will also be qualified in accordance with the requirements described in Chapter 4.

The documents relevant to the equipment qualification will be developed during Step 4 of GDA.

7.5.5.2.7 Compliance with Hazard Protection

The RIS [SIS] withstands internal and external hazards in accordance with the principles of Chapter 19 and Chapter 18 and takes measures outlined below to prevent the hazards.

a) Internal Hazards

The protection against internal hazards mainly depends upon the buildings, rooms, fire compartments and anti-flooding compartments arranged for the RIS [SIS]. The specific measures are as follows:

1) Three trains of RIS [SIS] are separated physically from each other since they are arranged in different safeguard buildings. If one train is affected by a single internal hazard, the other two trains will remain operational. Thus the RIS [SIS] can still perform its functions;

2) The redundant trains are physically separated by the building design in the containment.

Specific protection design is presented in Reference [31] . The evaluation of the design is presented in Chapter 19.

b) External Hazards

1) Earthquake

As shown in Table T-7.5-18 and Reference [29], the main equipment of the

RIS [SIS] which performs safety functions is SSE1; and the equipment can still perform the desired safety functions in the Safe Shutdown Earthquake (SSE) condition.

The documents relevant to the equipment seismic categorisation will be delivered.

2) Other external hazards

The RIS [SIS] protects against external disasters mainly through the building design. The specific protection design is presented in Reference [31] and the evaluation of the design is presented in Chapter 18.

7.5.5.2.8 Compliance with Commissioning

Initial testing (e.g. factory acceptance tests) of components before delivery to site shall be undertaken to ensure that the safety functions of these components can be properly performed. The design requirements will be provided to the equipment vendor in the form of technical specifications.

Commissioning and testing are going to be carried out for the RIS [SIS] to validate its functionality. The following tests need to be carried out:

a) Accumulator discharge tests;

b) LHSI pump flowrate tests;

c) MHSI pump flowrate tests;

The detailed description is presented in Reference [32], documents such as the System Commissioning Program related to the commissioning are going to be submitted.

7.5.5.2.9 Compliance with Examination, Inspection, Maintenance and Testing

For parts of the RIS [SIS] outside the reactor building, the in-service inspection can be performed during station normal operation. For parts inside the reactor building, the in-service inspection can be performed during shutdown.

The documents relevant to the equipment pre-service inspection list will be delivered.

The RIS [SIS] layout design can ensure the accessibility and requirements for maintenance, in-service inspection and periodic tests. The system layout design considers the following factors:

a) The needs for maintenance, including removing the worn parts and installing the replacement;

b) The accessibility and requirements for safety equipment in-service inspection and periodic tests;

c) The requirements of emergency and scheduled maintenance on the SSCs over the

life span of the plant.

The introduction of RIS [SIS] layout refers to Reference [31].

According to the functions performed by the RIS [SIS], the RIS [SIS] shall conduct the following periodic tests:

a) Pumps:

   1) MHSI cold leg injection with the miniflow line opened;

   2) LHSI cold leg injection with the miniflow line opened;

   3) LHSI hot leg injection;

b) Accumulator

   1) Accumulator cold leg injection;

c) Valve

   1) Sealing test of the containment isolation valve;

d) Exchanger

   1) Performance of the residual heat removal heat exchanger;

The documents relevant to the System Periodic Test Completeness Note (PTCN) will be delivered.

The detailed description around EMIT is presented in Reference [32].

7.5.5.2.10 Special Thermal-Hydraulic Phenomena

As stated in Sub-chapter 7.2.4, the thermal-hydraulic phenomena listed below are considered in RIS [SIS] design.

a) Phenomenon regarding the dead leg

   During standby of the RIS [SIS] two RCPB isolation valves are closed. The pipe between the two isolation valves can form the dead leg phenomenon and therefore the RIS [SIS] takes the following measures to prevent this:

   1) The distance between the first RCPB isolation valve and the RCP [RCS] is extended and therefore the heat conduction between the RCP [RCS] and RCPB isolation valves is reduced The method of extending the pipe can effectively avoid the dead leg phenomenon.

   2) Moreover, during normal operation, the pipe between two RCPB isolation valves can be pressurised by the accumulator, which can effectively prevent the occurrence of the dead leg phenomenon.

b) Phenomenon regarding the hot water and cold water mixing;

During operation of the RIS [SIS] in the RHR mode, the areas downstream of the RHR heat exchanger and the bypass pipe connection are cold and hot water mixing areas. In order to avoid weld fatigue caused by cold and hot water mixing, this connection adopts a long tee to keep the weld away from the cold and hot water mixing area, which can effectively reduce the risk of weld fatigue.

c) Phenomenon regarding the water hammers

During the refuelling of the reactor, most of the water in the IRWST is in the reactor pool, and only a small amount of water remaines in IRWST. Therefore, the elevation of the MHSI pump miniflow lines in the IRWST is higher than the water level. As the lines are not isolated in this condition and have a constant slope for draining, air can enter the pipe, which may lead to a risk of water hammer when operating the pump, To prevent air from entering the pipe due to water draining, a water seal (U bend) will be added on a horizontal part of the lines, which can effectively reduce the water hammer risk during MHSI pump start-up. The same configuration is used for the miniflow lines of the LHSI pump.

d) Phenomenon regarding the boiler effect

The boiler effect induced by the environment temperature change may result in the loss of opening ability of gate valves. This failure may result in a potential risk under the condition in which the valves are required to be opened to perform the safety functions.

In order to eliminate the boiler effect, small by-passes are provided for the gate valves of the RIS [SIS]. In this way, the gate valve can be opened normally and the risk to the safety induced by the boiler effect is eliminated.

7.5.5.2.11 Compliance with material selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component is presented in Sub-chapter 7.5.4.1.2.

7.5.5.2.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

The main equipment of the RIS [SIS], including MHSI pump, LHSI pump and RHR heat exchanger, are equipped with insulation made of glass fiber. The operating temperature of the accumulator is around 15°C -45°C and therefore no insulation is required.

The main pipes and valves of the RIS [SIS] in the safeguard building are provided with insulation. The insulation material is glass fiber.

The pipes and valves for the RHR function in the reactor building are provided with

insulation and the insulation material is glass fiber.

7.5.5.2.13 Decommissioning

The design of the RIS [SIS] takes into account the impact on decommissioning, including the following measures:

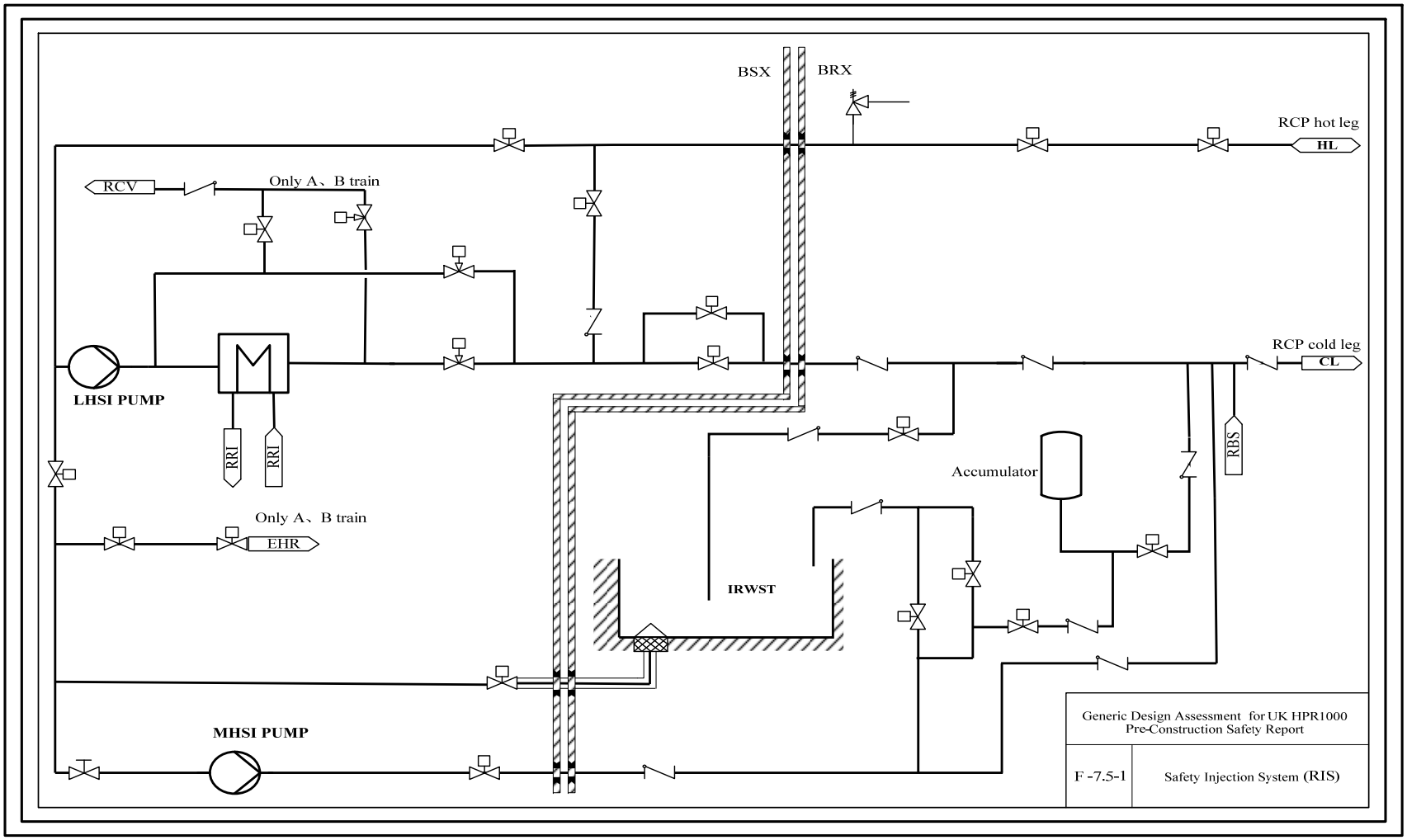
c) The main equipment is equipped a drainage pipe, which can be used to empty the equipment;

d) The IRWST are equipped with a steel liner to ensure convenience of decontamination;

e) The layout of the RIS [SIS] considers decommissioning such as the accessibility of personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.5.6 Functional Diagrams

The simplified functional diagram of the RIS [SIS] is shown in Figure F-7.5-1. The detailed system functional diagrams are presented in [33].



F-7.5-1 Simplified Functional Diagram of RIS [SIS]

7.6 Emergency Boration System (RBS [EBS])

7.6.1 Safety Requirements

The requirements of safety functions on the RBS [EBS] design for the UK HPR1000 are identified below, Reference [34] and [35]:

7.6.1.1 Control of Reactivity Requirements

The Emergency Boration System (RBS [EBS]) performs the reactivity control function via injecting borated water to the Reactor Coolant System (RCP [RCS]):

a) In DBC-2/3/4 condition, the RBS [EBS] performs the manual borated water injection function to ensure that the plant can reach a safe state;

b) In Design Extension Condition A (DEC-A) events, the RBS [EBS] performs the manual borated water injection function if necessary to ensure that the plant can reach the final state;

c) In Anticipated Transient Without Scram (ATWS) events, which are induced by control rod failure, the RBS [EBS] performs the automatic boration function for the RCP [RCS].

7.6.1.2 Removal of Heat Requirements

The RBS [EBS] is not required to perform this safety function.

7.6.1.3 Confinement Requirements

The RBS [EBS] contributes to the integrity of the Reactor Coolant Pressure Boundary (RCPB):

1) The RBS [EBS] isolation valve connecting to the RCP [RCS] can ensure isolation of the RCPB;

2) The maximum flowrate of the RBS [EBS] is limited to avoid opening of the Pressuriser Safety Valve (PSV) due to the overpressure caused by RBS [EBS] injection in the event of Chemical and Volume Control System (RCV [CVCS]) failures.

3) The RBS [EBS] also contributes to the integrity of containment so that each penetration of the RBS [EBS] can be isolated effectively when necessary.

7.6.1.4 Extra Safety Function Requirements

The RBS [EBS] shall contribute to the extra supporting functional requirements as follows:

a) Monitor the water level and temperature of the emergency boric acid tank.

7.6.2 Design Requirements

The general design requirements of the safety systems which need to be considered are shown in Sub-section 7.2.4, and the following requirements are not applicable to the RBS [EBS]:

a) Fail-safe: there is no fail-safe requirement on the RBS [EBS].

b) Autonomy in Respect to the Heat Sink: the RBS [EBS] is not a heat sink system; therefore, the autonomy of heat sink is not applicable to the RBS [EBS].

c) Special Thermal-Hydraulic Phenomena: there is no special thermal-hydraulic phenomenon in the RBS [EBS].

The substantiation analysis of the RBS [EBS] to other design requirements is shown in Sub-section 7.6.5.

7.6.3 Design Bases

The Emergency Boration System (RBS [EBS]) belongs to the engineered safety systems. The RBS [EBS] shall inject borated water into the reactor core to compensate for the insertion of positive reactivity due to core cooldown and xenon poison decrease in accidents. During the RCPB hydrotest, the emergency boration pump in train B will operate to supply the fluid medium with a small flow and high hydraulic head.

This Sub-chapter aims to provide main design assumptions considered in the system design, Reference [35].

7.6.3.1 General Assumptions

a) Safety Classification

The emergency borated water injection function is used to reach a safe state under DBC-2/3/4 condition (if the function are not performed, the consequences are high) and therefore the part of the RBS [EBS] that performs emergency borated water injection under DBC-2/3/4 conditions is FC2.

The part of the RBS [EBS] that performs emergency borated water injection under ATWS is FC3.

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which are important to safety shall be taken into account.

The design life of the main equipment of the RBS [EBS] is 60 years. In addition, some parts of the main equipment need to be replaced regularly during the life.

c) Autonomy

There is no quantitative requirement for the RBS [EBS].

d) Equipment Qualification

Active components of the RBS [EBS] performing an FC1 or FC2 safety function shall be qualified.

Active components of the RBS [EBS] performing an FC3 safety function required under DEC conditions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

The fluctuation of the electrical power grid may affect the ability of safety functions, especially the performance of active equipment, such as the emergency boration pumps.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in RBS [EBS] equipment design, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.6.3.2 Design Assumptions

7.6.3.2.1 Control of Reactivity Assumptions

The Emergency Boration System (RBS [EBS]) performs the reactivity control function via injecting borated water to the Reactor Coolant System (RCP [RCS]). The requirements for the RBS [EBS] are as follows:

a) When providing emergency boration for the RCP [RCS], the RBS [EBS] is capable of maintaining the core in a sub-critical condition, from the controlled state to a safe state (RHR connected), even with the minimum injection flowrate. The minimum injection flowrate is { }.

b) Each train shall provide a minimum volume of { }of borated water.

c) The minimum boron concentration is { } and the maximum boron concentration is { }.

d) In the Anticipated Transient without Scram (ATWS) condition, which is results from control rod failure (DEC-A condition), the RBS [EBS] shall ensure automatic boration for the RCP [RCS]. The injected flow is between { }and

{ }and the time delay from the signal to start-up of the RBS [EBS] pump until its operation at full flow rate is { }

7.6.3.2.2 Removal of Heat Assumptions

The RBS [EBS] is not required to perform this safety function.

7.6.3.2.3 Confinement Assumptions

a) When providing emergency boration, by RBS [EBS] injection at the maximum flow rate, no overpressure of the pressuriser may be caused by RBS [EBS] injection in the event of RCV [CVCS] failure. The maximum injection flowrate is { }

7.6.3.2.4 Extra Safety Function Assumptions

The water level instruments are used for stopping the emergency boration pump after accidents. This function is FC2, therefore at least two instruments need to functional.

For reliability considerations, at least two temperature instruments are required to fulfil the temperature monitoring functions.

7.6.4 System Description and Operation

7.6.4.1 System Description

7.6.4.1.1 General System Description

The RBS [EBS] is composed of three identical independent trains (train A, B and C). Each train has a 100% capacity for emergency boration. The trains A & B are located in the fuel building while train C is located in safeguard building C, Reference [36].

Each train of the RBS [EBS] consists of:

a) One emergency boric acid tank;

b) One piston pump;

c) Tracing heaters;

d) The associated pipes and valves.

The piston pump takes suction from the boron acid tank and injects the boric water into the cold leg of the corresponding loop of the RCP [RCS] via a connection line provided in the Safety Injection System (RIS [SIS]).

One train of the RBS [EBS] pump is used for the RCPB hydraulic test, therefore the pump is also referred to as the test pump. During the hydraulic test of the RCPB, the RBS [EBS] test pump draws water from the RCV [CVCS] Volume Control Tank (VCT) and injects it into the RCP [RCS] through the No.1 shaft seal of the primary

pump (after passing through the shaft seal injection line of the RCV[CVCS]).

A periodic test line is provided for the periodic tests of each RBS [EBS] pump. The periodic test line is designed as a full flow line connected from the pump outlet to the corresponding boric acid tank. The pump can also perform periodic mixing of the boric acid tank through the test line.

The safety valves are arranged at the outlet of the pump to protect the system from possible overpressure.

As the concentration of the boric acid solution is 7000 mg/kg (^{10}B with an enrichment of 35%), the minimum temperature allowed for the system medium is 20℃ to prevent boron precipitation. The temperature is guaranteed by the Heating, Ventilation and Air Conditioning System (HVAC) and the tracing heaters of the Boron Heating System (RRB [BHS]).

The simplified flow diagram of the RBS [EBS] is shown in Figure F-7.6-1.

7.6.4.1.2 Description of Main Equipment

a) Emergency Boration Pump

The emergency boration pump performs following two main functions, Reference [36]:

1) In the case of accident conditions, the RBS [EBS] pump will inject 7000 to 7700 ppm borated water into the RCP [RCS] to compensate for the insertion of positive reactivity due to cooling down of the RCP [RCS] and the decrease of xenon poison.

2) During the plant shutdown condition, the Train B RBS [EBS] pump which is located in fuel building will be used to perform the RCPB hydrostatic test.

The emergency boration pump is a piston-type pump with a high head and low flow. The main design characteristics of the emergency boration pump are listed in Table T-7.6-1.

The full flow test line and overpressure protection line are arranged at the outlet of each pump, discharging to the corresponding boric acid tank.

The pump is a piston-type pump driven by a motor which is horizontal with 3 plunger pistons. The suction nozzle of the pump is horizontal and the discharging nozzle is also horizontal. There is no reducer between the pump and the motor.

The pressure-retaining parts shall be made of austenitic stainless steel and meet the requirements for inter granular corrosion resistance as stipulated in the RCC-M D 2300.

The pump and the gear box can be replaced and maintained without removing the

motor.

The pump is cooled by air.

T-7.6-1 Main Design Characteristics of the RBS [EBS] Pump

Parameters	**Value**	**Unit**
Type	Piston Pump	
Design Lifespan	60	yr.
Nominal Flowrate	10.5	m^3/h
Design Pressure for Discharge Side	25.9	MPa (g)
Material	Stainless Steel	

b) Emergency Boric Acid Tank

The emergency boric acid tanks of the three trains are vertical storage tanks at atmospheric pressure, which are made of stainless steel. The boron concentration in the tanks are 7000~7700 mg/kg with 35% enrichment of ^{10}B. The usable volume of the tank is sufficient to provide the negative reactivity insertion required for the reactor to reach the safety shutdown state during accidents (the contribution from the control rods is not credited for the conservative consideration), Reference [36].

The boric acid solution of the RBS [EBS] emergency boric acid tank is prepared and supplemented by the boric acid makeup tank of the REA [RBWMS].

The emergency boric acid tank is kept under atmospheric pressure through the vent nozzle on the top.

The boric acid solution in the RBS [EBS] emergency boric acid tank can be mixed by the emergency boration pump of the corresponding train to ensure the homogeneity and concentration meeting the requirements. The homogeneity and concentration are monitored through periodic sampling.

Water level and temperature sensors are also designed for monitoring the tanks.

T-7.6-2 Main Design Characteristics of the RBS [EBS] Tank

Parameters	**Value**	**Unit**

Parameters	**Value**	**Unit**
Type	Cylindrical Tank	
Medium	Boric Acid	7000-7700mg/kg, ^{10}B, Enrichment Degree 35%
Design Pressure	0.1	MPa abs
Design Temperature	60	°C
Usable Volume	40	m^3
Max. Volume	50	m^3
Material	Stainless Steel	

7.6.4.1.3 Description of Main Layout

Three trains of the RBS [EBS] are independently arranged in the nuclear island buildings. Train C is arranged in safeguard building C and the other two trains, A and B, are arranged in the fuel building, Reference [37]. However, part of the injection lines and some valves are located in the BRX, as show in the functional flow diagram Figure F-7.6-1.

As the three trains of the RBS [EBS] are physically separated, they will not be affected at the same time (common mode failure) in case of any internal hazards in one building.

The fuel building, safeguard building C and the reactor building are able to withstand the crash of aircrafts, which enable the RBS [EBS] to perform its safety functions without being affected by such an external hazard.

7.6.4.1.4 Description of System Interface

The systems supporting the fulfillment of RBS [EBS] functions are as follows, Reference [36]:

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

   The RCV [CVCS] provides water to the RBS pump during the RCPB hydrostatic test.

b) Reactor Boron and Water Makeup System (REA [RBWMS])

   The REA [RBWMS] provides borated water with a boron concentration of

7000~7700 mg/kg (^{10}B with an enrichment of 35%) for the RBS [EBS] tank.

c) Safety Injection System (RIS [SIS])

The RIS [SIS] provides connection lines for RBS [EBS] injection of borated water into the RCP [RCS].

7.6.4.1.5 Description of Instrumentation and Control

The functions of automatic control of the RBS [EBS] are as follows:

a) The RBS [EBS] is automatically actuated when receiving the ATWS signal;

b) The emergency boration pumps are designed with temperature sensors to monitor pump operation. The pump can be automatically stopped once the temperature exceeds the threshold;

c) The signal of low water level of the storage tank can automatically trip the pump to prevent it from being damaged.

The following parameters are monitored when the RBS [EBS] is either in the standby state or in operation:

a) Water level and temperature inside the water storage tank;

b) The discharge pressure of the pump;

c) The flowrate of the pump;

d) The start-up and shutdown state of the RBS pump as well as the open/close states of the valves.

7.6.4.2 System Operation

7.6.4.2.1 Plant Normal Condition

The RBS [EBS] is in steady state during reactor power operation. The suction line of train B connected to the emergency boric acid tank is isolated during the hydraulic test of the RCPB. RBS [EBS] test pump draws water from the RCV [CVCS] volume control tank. The test pump injects the water into the RCP [RCS] pump through the pump shaft seal, Reference [38].

7.6.4.2.2 Plant Accident Conditions

The boration by the RBS [EBS] is manually completed by the operator in the main control room under DBC-2/3/4 condition. The RBS [EBS] will be started automatically under DEC-A conditions (ATWS).

The boric acid solution injected into the cold leg of the loop will not reach the reactor core if one loop of the RCP [RCS] loses circulation (e.g. break in the loop or the affected steam generator is isolated) in an accident. Therefore, the operator shall make

the judgment and choose another RBS [EBS] train before manually starting the RBS [EBS]. If the train is started, the operator can manually shutdown the train and start another train.

Once the boron injection is started, the RBS [EBS] will operate continuously until the boron concentration of the RCP [RCS] reaches the target value of the safety shutdown state.

7.6.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. Detailed design of the system is presented in Reference [35] [36] [37] [38] and [39]. Furthermore, design substantiation of the RBS [EBS] is estimated in the fault study in Chapter 12 and 13.

7.6.5.1 Compliance with Safety Requirements

7.6.5.1.1 Compliance with Control of Reactivity

The RBS [EBS] is provided with three 100% independent trains, which are designed according to the appropriate codes and standards and located in separated buildings. Thus the fulfilment of the safety function of reactivity control can be ensured under all required conditions.

Each of the RBS [EBS] trains is designed with sufficient capacity to perform the required safety function. The instrumentation and control of the RBS [EBS] ensure effective operation of the system.

The design capability of the RBS [EBS] provides sufficient boron for the RCP [RCS] under DBC-2/3/4 condition. The RBS [EBS] can provide sufficient boron for the RCP [RCS] under ATWS.

The fault study in Sub-chapter 12.9 and 13.5 justifies that each safety function required on the RBS [EBS] in Sub-chapter 7.6.1.1 is met based on the design assumptions provided in Sub-chapter 7.6.3.2.1. This includes the injection flowrate, borated water concentration, borated water volume etc.

When providing emergency boration for the RCP [RCS], the RBS [EBS] is capable of maintaining the core in a sub-critical condition from the controlled state to a safe state (RHR connected). The injection flowrate is 10.5 m^3/h (each train).

The usable volume of each emergency boric acid tank is 40 m^3 and the borated water concentration in the tank is 7000 to7700 ppm.

7.6.5.1.2 Compliance with Removal of Heat

The RBS [EBS] does not contribute to this safety function.

7.6.5.1.3 Compliance with Confinement

To ensure the integrity of the RCPB, two check valves (one of them in the RIS [SIS]) are provided for the isolation of the RCPB.

To ensure the integrity of the containment, each containment penetration is equipped with two containment isolations valves in the RBS [EBS]. One motor-operated valve outside the containment and one check valve inside the containment.

The injection flowrate of each RBS [EBS] train is 10.5m^3/h and the injection flow of the RBS [EBS] does not exceed { }as required.

7.6.5.1.4 Compliance with Extra Safety Function Requirements

a) Monitor the water level and temperature of the emergency boric acid tank.

   Two water and temperature instruments are installed on emergency boric acid tank; the detailed information is presented in [38].

7.6.5.2 Compliance with Design Requirements

7.6.5.2.1 Compliance with Safety Classification

The RBS [EBS] design is compliant with the requirements described in Chapter 4. The safety classification of RBS [EBS] functions is listed in Table T-7.6-3

The documents relevant to the equipment classification will be delivered.

T-7.6-3 System Function Classification

System Function	**Function Category**
Emergency boration under DBC-2/3/4	FC2
Emergency boration under ATWS	FC3
RCPB isolation	FC1
Containment isolation	FC1
Water makeup for acid tank	NC

The RBS [EBS] is designed to withstand a SSE. The safety classification of main components is listed in Table T-7.6-4.

T-7.6-4 Classification of Main Components

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
Containment Isolation Valves	F-SC1	DPA	B-SC2	SSE1
Isolation valve	F-SC2	NC	NC	SSE1
RCPB Isolation valve	F-SC1	DPA	B-SC1	SSE1
Emergency Boration Pump	F-SC2	NC	NC	SSE1
Boric Acid Tank	F-SC2	NC	NC	SSE1
Test line Isolation valve	F-SC2	NC	NC	SSE1

7.6.5.2.2 Compliance with Reliability

a) Redundancy and SFC

The principle of the SFC is presented in Sub-chapter 7.2.4.

The RBS [EBS] is designed with 3 redundant trains (none of them are connected to each other), each of which has a 100% capacity under accident conditions. Even under the most conservative assumption, that if one train cannot work as a result of a single failure and another cannot work as a result of an initiating event, the remaining train can still perform the function of emergency boration.

The prevention of the passive SFC 24 hours after the postulated initiating event is the same as the active SFC, i.e. another train can still preforms safety function if the passive SFC occurs on one train of the RBS [EBS].

The detailed design result of RBS [EBS] is presented in Reference [35], [36] and [38].

b) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The RBS [EBS] consists of three independent trains, each of which has a 100%

capacity for emergency boration. Train A & B are located in the fuel building while train C is in safeguard building C.

c) Diversity

The principle of diversity is presented in Sub-chapter 7.2.4.

The diversity design in the RBS [EBS] contains:

1) Each containment penetration is equipped with two containment isolation valves in the RBS [EBS]. One motor-operated valve outside the containment and one check valve inside the containment.

2) The RBS [EBS] and RCV [CVCS] can be used to perform the function of emergency boration after accidents.

The detailed design result of the RBS [EBS] is presented in Reference [35] and [36].

d) Fail-safe Design

There is no fail-safe designed equipment in the RBS [EBS].

e) Ageing and Degradation

The system is designed for the 60 year plant operation. The design life of the main equipment of the RBS [EBS] system is 60 years, which mainly include the:

1) Emergency Boration Pump;

2) Emergency Boric Acid Tank.

The performance of equipment is guaranteed through life examination, inspection maintenance and testing, as well as monitoring during normal operation. Thus it can be ensured that ageing effects do not compromise safety performance. The detailed design arrangement around EMIT and equipment monitoring is presented in Reference [38].

The system layout design can ensure the accessibility and requirements for safety equipment in-service inspection and periodic tests including the necessary NDT. This includes the requirements of emergency and scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [37] .

7.6.5.2.3 Compliance with Human Factors

The system design and control function design of the RBS [EBS] do not require short term operator intervention. No operator action is required within 30 minutes after the initial event based on the RBS [EBS] design result. The design information is presented in Reference [36] and [38].

It should be noted that there are operator actions during plant normal operation and

accident conditions (including plant startup, shutdown, and maintenance or testing etc.). Relevant human actions which are important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of the human factor discipline. Relevant evaluated reports will be provided as references of Chapter 15.

7.6.5.2.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in Reference [1]. The RBS [EBS] satisfies the requirement through the following design:

1) Under the condition of ATWS, the emergency boration pumps are started automatically by the injection signal. No human operation is required from the Main Control Room (MCR) less than 30 minutes from the first significant signal;

2) In other accident conditions (except ATWS), the RBS [EBS] performs the manual borated water injection function, These operations can be performed at the MCR, and no human operation is required outside the MCR less than 1 hour from the first significant signal;

The design of the RBS [EBS] fulfils these principles via the control function design [38]. The design result has been estimated in the safety analysis.

b) Autonomy in Respect to the Heat Sink

The design principles relevant to the autonomy in respect to the heat sink are listed in Reference [1]. These principles are not applicable for RBS [EBS] design.

c) Autonomy in Respect to Power Supply Systems

The three trains of RBS [EBS] are powered by different electrical divisions. Each RBS [EBS] pump and relevant active equipment is powered by a corresponding Emergency Diesel Generator (EDG), so that their safety functions can be met even in the case of Loss of Offsite Power (LOOP). Moreover, the RBS [EBS] pump (train A and B) is powered by the SBO diesel generator in Station Black Out (SBO) accident conditions.

In SBO accident conditions or severe accident conditions, the motor-operated isolation valves outside the containment can be powered by 12h batteries.

7.6.5.2.5 Compliance with Other Design Requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

According to Reference [1], the protection of interfacing systems shall be considered in RBS [EBS] design. The RBS [EBS] takes the following measures to prevent the harmful interactions of systems:

1) Provides adequate isolation (e.g. using double isolating valves) between the RBS [EBS] and interfacing systems;

2) The design pressure of the isolation valve between the RBS [EBS] and the interface system adopts the larger pressure;

Detailed information is in Reference [38] [39].

b) Considerations Related to the Electrical Power Grid

According to Reference [1], the functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid.

The fluctuation of the electrical power grid mainly affects the functional capability of the emergency boration pumps. The pump flow will change with the fluctuation of the power grid. In the HPR1000 (FCG3) project，the design of emergency boration pumps considers the influence of grid fluctuation [36]. Re-estimates will be carried out during the GDA progress, on the basis of the UK context, relevant to the electrical power grid.

7.6.5.2.6 Compliance with Equipment Qualification

According to Chapter 4, all components required to perform the safety functions shall be capable of operating under both normal and accidental conditions, which requires the components to withstand the adverse ambient environment.

The equipment performing safety functions in the RBS [EBS] will be qualified in accordance with the requirements described in Chapter 4.

The documents relevant to the equipment qualification will be developed during Step 4 of GDA.

7.6.5.2.7 Compliance with Hazard Protection

The RBS [EBS] protection against internal and external hazards is in accordance with the principles of Chapter 19 and Chapter 18. The RBS [EBS] takes the measures outlined below to prevent hazards.

a) Internal Hazards

The protection against internal hazards mainly depends upon the buildings, rooms, fire compartments and anti-flooding compartments arranged for the RBS [EBS]. The specific protection design is presented in Reference [37]. The evaluation of the design is presented in Chapter 19.

b) External Hazards

1) Earthquake

As shown in Table T-7.6-4 and reference [35], the main equipment of the RBS [EBS] performing safety functions is SSE1; the equipment can still perform the desired safety functions in the Safe Shutdown Earthquake (SSE) condition.

The documents relevant to the equipment seismic categorisation will be delivered.

2) Other external hazards

The RBS [EBS] protects against external disasters mainly through the building design. The specific protection design is presented in Reference [37], while the evaluation of the design is presented in Chapter 18.

7.6.5.2.8 Compliance with Commissioning

Initial testing (e.g. factory acceptance tests) of components before delivery to site shall be undertaken to ensure that the safety functions of these components can be properly performed. The design requirements will be provided to the equipment vendor in the form of technical specifications.

Commissioning is going to be carried out for the RBS [EBS] to validate its functionality. The following tests need checking or validating:

a) Test RBS [EBS] pumps operation on their test line.

b) Test of motor and manually operated valves

c) Test of the RBS [EBS] tanks;

d) System flushing;

e) Instrumentation and control channel tests.

The detailed description is presented in Reference [38]. Documents related to the commissioning, such as the System Commissioning Program, are going to be submitted.

7.6.5.2.9 Compliance with Examination, Inspection, Maintenance and Testing

According to Chapter 31, in-service inspection implemented during operation is defined on the basis of RSE-M 2010 edition including the 2012 addendum. The components and lines belonging to the primary loop are required to perform in-service inspection, i.e., the RCPB isolation valve of the RBS [EBS] and its downstream pipes require in-service inspection.

The documents relevant to the equipment pre-service inspection list will be delivered.

The system is designed for the 60 year plant operation. The design life of the main equipment of the RBS [EBS] is 60 years. These components mainly include the:

a) Emergency Boration Pump

b) Emergency Boric Acid Tank

However, some pump components require replacing regularly according to manufacturer feedback（such as gaskets, mechanical seals, O-ring and bearings）.

The RBS [EBS] layout design can ensure the accessibility and requirement for maintenance, in-service inspection and periodic tests. The system layout design considers the following factors:

a) The needs for maintenance, including removing the worn parts and installing the replacement;

b) The accessibility and requirement for safety equipment in-service inspection and periodic tests;

c) The requirements of emergency and scheduled maintenance on the SSCs over the life span of the plant.

The introduction of RBS [EBS] layout refers to reference [37].

The borated water in the RBS [EBS] tank is periodically mixed, and functional tests of pumps and valves are also conducted periodically.

The detailed description about EMIT is presented in Reference [38].

7.6.5.2.10 Special Thermal-Hydraulic Phenomena

No special thermal-hydraulic phenomenon needs to be considered in the RBS [EBS].

7.6.5.2.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component is presented in Sub-chapter 7.6.4.1.2.

7.6.5.2.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

In order to prevent the occurrence of boron crystallization, the temperature of RBS [EBS] equipment and pipe cannot be lower than the 20°C.

In the fuel building and safeguard building C where the RBS [EBS] equipment and pipes are located, the ambient temperature will be kept above 20°C by the HVAC system; therefore there is no need for insulation.

However, in order to prevent the borated water temperature in the pipe falling below

20°C, insulation and heat tracing measures will be taken for the RBS [EBS] injection pipe in the Reactor Building (BRX).

7.6.5.2.13 Decommissioning

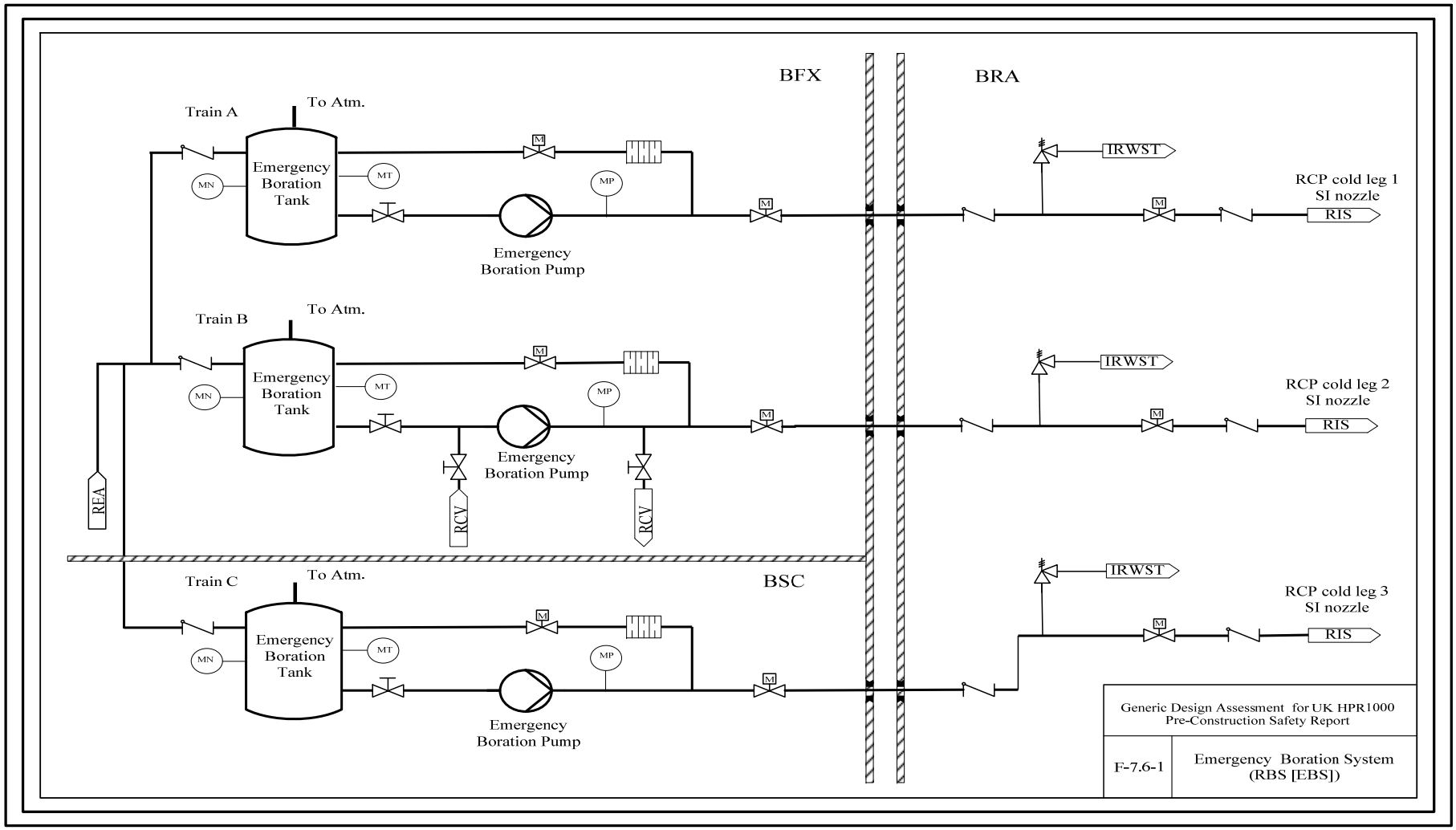
The design of the RBS [EBS] takes into account the impact on decommissioning, including the following measures:

a) The main equipment is equipped with a drainage pipe, which can be used to empty the equipment;

b) The layout of the RBS [EBS] considers decommissioning, such as the accessibility for personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.6.6 Functional Diagrams

The simplified functional diagram of the RBS [EBS] is presented in Figure F-7.6-1. The detailed system functional diagrams are presented in Reference [39].



F-7.6-1 Simplified Functional Diagram of the RBS [EBS]

7.7 Atmospheric Steam Dump System (VDA [ASDS])

7.7.1 Safety Requirements

The requirements of safety functions on the VDA [ASDS] design for the UK HPR1000 are identified in this sub-chapter, Reference [40] and [41].

7.7.1.1 Control of Reactivity Requirements

The VDA [ASDS] does not participate in reactivity control directly. However, the excessive steam flowrate shall cause excessive cooling of the RCP [RCS] and increase the reactivity of the core. In this kind of accident, the isolation of the VDA [ASDS] serves against overcooling of the RCP [RCS].

7.7.1.2 Removal of Heat Requirements

In DBC-2/3/4 and DEC-A events with the GCT [TBS] unavailable, the VDA [ASDS] removes residual heat through discharging steam into atmosphere to:

a) Bring the reactor to the controlled state, and then cool the RCP [RCS] to the condition in which Safety Injection System (RIS [SIS]) can be operated in the Residual Heat Removal (RHR) mode, so as to bring the reactor to the safety shutdown state (for DBC-2/3/4); or bring the reactor to the final state (for DEC-A events).

   In DBC-2/3/4 and DEC-A events with the primary inventory decreasing (intermediate & small break LOCA or SGTR), Medium Pressure Rapid Cooldown (MCD) shall be carried out through the VDA [ASDS] if the GCT [TBS] is unavailable when the primary pressure is higher than the injection pressure of Medium Head Safety Injection (MHSI). Thus the pressure and temperature of the RCP [RCS] can be reduced to MHSI operating conditions.

   In addition, during intermediate & small break LOCA with complete loss of MHSI (DEC-A), Low Pressure Full Cooldown (LCD) shall be carried out through the opening of the VDA [ASDS], thus RCP [RCS] pressure and temperature can be reduced to the injection conditions of the safety injection tank and the LHSI.

b) Ensure the integrity of the SG and the removal of heat through limiting the increase of pressure at the secondary side of the SG (with the Main Steam Safety Valve (MSSV)).

7.7.1.3 Confinement Requirements

During DBC-2/3/4 and DEC-A events, the opening of the VDA [ASDS] participates in the protection of the SG against overpressure.

7.7.1.4 Extra Safety Function Requirements

The VDA [ASDS] protects the Steam Generator (SG) against overpressure.

7.7.2 Design Requirements

The general design requirements of the safety systems which need to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to the VDA [ASDS]:

a) Fail-safe: There is no fail-safe requirement on the VDA [ASDS].

b) Autonomy in Respect to the Heat Sink: The VDA [ASDS] is not a heat sink system; therefore the autonomy of the heat sink is not applicable to the VDA [ASDS].

c) Considerations Related to the Electrical Power Grid: VDAs [ASDS] do not include pumps and other equipment which would be affected by the power grid.

The substantiation analysis of the VDA [ASDS] to other design requirements is shown in Sub-chapter 7.7.5.

7.7.3 Design Bases

The VDA [ASDS] belongs to the engineered safety systems. It is designed to discharge steam to the atmosphere in DBC-2/3/4 or DEC-A when the Turbine Bypass System (GCT [TBS]) is unavailable.

This sub-chapter aims to provide main design assumptions considered in the system design, Reference [41].

7.7.3.1 General Assumptions

a) Safety Classification

   The VDA [ASDS] are used to reach a controlled state under DBC-2/3/4 (if the functions are not performed, the consequences are high), therefore the VDA [ASDS] is classified as Function Category 1 (FC1).

b) Ageing and Degradation

   During system and equipment design, the ageing and degradation of the equipment which is important to safety shall be taken into account.

   The design life of the main equipment of the VDA [ASDS] is 60 years. In addition, some parts of the main equipment may need to be replaced regularly during the design life.

c) Autonomy

   There is no requirement for VDA [ASDS].

d) Equipment Qualification

The components of the VDA [ASDS] performing safety functions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

There is no requirement for the VDA [ASDS].

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in the VDA [ASDS] equipment design, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.7.3.2 Design Assumptions

7.7.3.2.1 Control of Reactivity

The VDA [ASDS] does not participate in reactivity control directly. However, the isolation of the VDA [ASDS] serves against overcooling of the RCP [RCS] after accidents.

In an SGTR condition, the set pressure of the VDA [ASDS] will be adapted to higher than MHSI injection head after the MCD with the SG high water level (NR) 2 signals.

7.7.3.2.2 Removal of Heat

The requirements for the Main Steam Relief Isolation Valve (MSRIV) are as follows:

a) Under a pressure of{ }, the discharge capacity of each MSRIV is at least { }of the nominal steam flowrate;

b) The opening setpoint is { };

c) The valve opening time is { }.

The requirements for the Main Steam Relief Control Valve (MSRCV) are as follows:

a) Under a pressure of { }, the discharge capacity of each MSRCV is at least { }of the nominal steam flowrate;

b) The full open time is less than { }.

7.7.3.2.3 Confinement

The discharge capacity and the opening time delay of the VDA [ASDS] meets the requirements of the overpressure protection criterion. In an SGTR condition, the VDA [ASDS] can be isolated to avoid radioactive release after accidents.

Under a pressure of { }, the MSRIV and MSRCV discharge capacity is at least { } of the nominal steam flowrate, and the opening time delays of the VDA [ASDS] are presented in Sub-chapter 7.7.3.2.2.

7.7.3.2.4 Extra Safety Function Assumptions

The requirement for the opening set pressure of the MSRIV is less than{ }.

7.7.4 System Description and Operation

7.7.4.1 System Description

7.7.4.1.1 General System Description

The VDA [ASDS] is composed of three identical independent trains (train A, B and C) corresponding to the three SGs. Each train is connected to the main steam line upstream of the two MSSVs nozzles and the Main Steam Isolation Valve (MSIV).

Each train mainly consists of a MSRIV, a MSRCV and a silencer. The simplified flow diagram of the VDA [ASDS] is in Figure F-7.7-1.

7.7.4.1.2 Description of Main Equipment

a) MSRIV

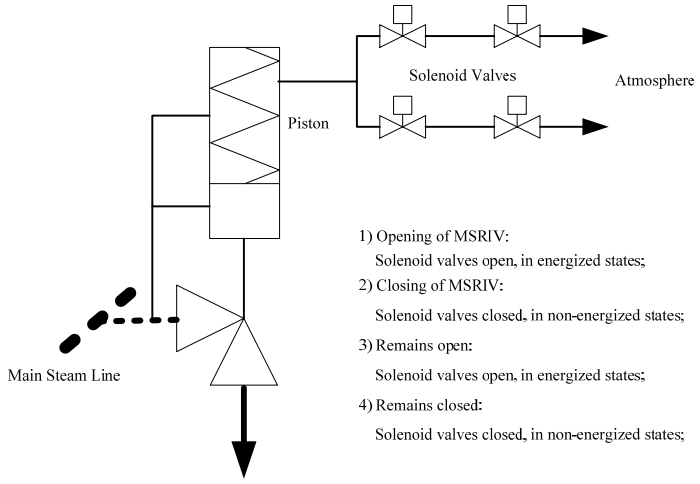
The MSRIV provides isolation for the system, and it is welded directly on the main steam line between the containment penetration and the MSIV, upstream of the MSSV nozzles. The general parameters of the MSRIV are shown in Table T-7.7-1, Reference [42].

T-7.7-1 General Parameters of the MSRIV

Parameters	Value	Unit
Actuator Type	System Medium Self-Actuated Solenoid-Valve-Actuated	/
Design Pressure	8.9	MPa (g)
Design Temperature	303	°C

Parameters	Value	Unit
Discharged Mass Flowrate	At Least 50% of the Full Load Steam Flow at the Design Pressure	/
Stroke Time	Opening:≤1.8; Closing:<20 (<26 without flow)	s
Material	Carbon Steel	/

The MSRIV is an angle valve actuated by both secondary-side steam and solenoid valves, as shown in Figure F-7.7-2



F-7.7-2 Actuation of the MSRIV

The main body of the MSRIV includes a piston and a piston chamber. Both the upper and the lower parts of the piston chamber are connected to the main steam line to be filled with steam. The two trains of redundant discharge lines (called manifolds) are composed of two serial solenoids each and can discharge steam from the piston chamber into the atmosphere.

The actuation principles of the MSRIV are as follows:

1) Open

Once the solenoid valves are energised and therefore opened, steam in the upper piston chamber will be discharged into the atmosphere. The piston will move upward and the MSRIV will be opened since the steam pressure in the lower chamber is greater than the downward thrust of the spring.

2) Close

Once the solenoid valves are de-energised and therefore closed, the upper piston chamber will be isolated from the atmosphere and filled with the steam. The piston will move downward and the MSRIV be closed under the steam pressure of the upper piston chamber and the downward thrust of the spring.

The design of the solenoid valves manifolds:

1) Facilitates the rapid opening and closing of the MSRIV; and

2) Prevents any failure of a single solenoid valve from causing inadvertent opening (because there are two solenoid valves in each train) or an opening failure (two trains of redundant control lines) of the MSRIV.

b) MSRCV

The MSRCV is connected to the discharge pipeline downstream of the MSRIV.

An angle control valve is used to the regulate steam discharge flow rate when the MSRIV is open.

The general parameters of the MSRCV are shown in T-7.7-2, Reference [42].

T-7.7-2 General Parameters of the MSRCV

Parameters	Value	Unit
Actuator Type	Electric	/
Design Pressure	8.9	MPa (g)
Design Temperature	303	°C
Discharged Mass Flowrate	At Least 50% of the Full Load Steam Flow at the Design Pressure	/
Stroke Time	≤40	s
Material	Carbon Steel	/

c) Silencer

The silencer located at the end of the discharge piping receives the steam discharged from the MSRCV.

The silencer reduces the noise produced during the discharging of steam to protect personnel and the environment. The design of silencers ensures that the noise of a steam discharge through the VDA [ASDS] remains within the UK statutory limits.

7.7.4.1.3 Description of Main Layout

The VDA [ASDS] is located in the steam valves compartments. The silencers are installed on the roof of Safeguard Building A (BSA) and Safeguard Building B (BSB), Reference [43].

Physical isolation and space separation are provided for the three trains of the VDA [ASDS] to minimise the possibility of common cause failures.

The components shall be easily accessible, while the compartment is sufficient dimensionally and in facilitating in-service inspection, periodic testing, maintenance and replacement.

7.7.4.1.4 Description of System Interface

The systems supporting the fulfilment of VDA [ASDS] functions are:

a) Main Steam System (VVP [MSS])

During VDA [ASDS] atmosphere steam dumping, steam from SG flows into the VDA [ASDS] via VVP [MSS] pipelines.

7.7.4.1.5 Description of Instrumentation and Control

The Instrumentation and Control (I&C) functions related to the VDA [ASDS] are classified as follows:

a) Automatic control

During DBC-2/3/4 and DEC-A events, the automatic control of the VDA [ASDS] will be implemented to bring the reactor into the controlled state (DBC-2/3/4) or final state (DEC-A).

During plant normal operation, the opening of the MSRCVs is controlled automatically according to the reactor power level.

b) Controls available to the operator

1) Opening and closing of the MSRIVs;

2) Adjusting the opening of the MSRCVs;

3) Manual triggering of RCP [RCS] cooling with the VDA [ASDS];

4) Adjusting the set pressure of the system (After the MCD with the SG high water level (NR) 2 signal, the set pressure of VDA will be adapted to higher than MHSI injection head.).

7.7.4.2 System Operation

7.7.4.2.1 Plant Normal Condition

During plant normal operation, the secondary side steam will be dumped into the atmosphere through the VDA [ASDS] only if the GCT [TBS] is unavailable; otherwise, the VDA [ASDS] will be in the standby state, Reference [44].

7.7.4.2.2 Plant Accident Conditions

During DBC-2/3/4 and DEC-A events with GCT [TBS] unavailable, the pressure at the secondary side of the SG is controlled by the VDA [ASDS] until the controlled state (DBC-2/3/4) or the final state (DEC-A) is reached.

During DBC-2/3/4 and DEC-A events with GCT [TBS] unavailable, RCP [RCS] cooling with the VDA [ASDS] via steam dumping into the atmosphere will be performed to the conditions in which RIS [SIS] can be operated in RHR mode.

During DBC-3/4 and DEC-A events with GCT [TBS] unavailable, when the pressure of the RCP [RCS] is required to be reduced to meet the safety injection conditions, the depressurisation is performed through medium head fast cooling or low head fast cooling with the VDA [ASDS]. If the water level inside the SG is still high with the medium head fast cooling finished (e.g. SGTR), the opening setpoint of the VDA [ASDS] will be increased to limit discharge of radioactive water into the environment.

During DBC-3/4 events of uncontrolled heat removal at the secondary side, the VDA [ASDS] will be isolated to reach the controlled state.

7.7.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. Detailed design of the system is presented in Reference [40], [41], [42], [43], [44] and [45], and design substantiation of the VDA [ASDS] is estimated in the fault study of Chapter 12 and 13.

7.7.5.1 Compliance with Safety Requirements

7.7.5.1.1 Compliance with Control of Reactivity Requirements

The VDA [ASDS] does not participate in reactivity control directly. However, the excessive steam flowrate will cause the excessive cooling of the RCP [RCS] and increase the reactivity of the core. In this kind of accident, isolation of the VDA [ASDS] serves against overcooling of the RCP [RCS].

7.7.5.1.2 Compliance with Removal of Heat Requirements

The discharge capacity of the three redundant VDA [ASDS] trains is at least { } of the full steam flow load (at the design pressure).

The fault study in Sub-chapter 12.9 and 13.5 justifies that each safety function required on the VDA [ASDS] in Sub-chapter 7.7.1.2 is met based on the design assumptions provided in Sub-chapter 7.7.3.2.2, including the opening setpoint of the MSRIV, the valve opening time, etc.

The design requirements (discharge capacity, opening setpoint valve, opening time etc.) of the MSRCV and MSRIV shall be presented in the technical specifications and the equipment supplier shall meet the requirements according to the specifications.

7.7.5.1.3 Compliance with Confinement Requirements

The fault study in Sub-chapter 12.9 and 13.5 justifies that each safety function required on the VDA [ASDS] in Sub-chapter 7.7.1.3 is met based on the design assumptions provided in Sub-chapter 7.7.3.2.3, including the opening setpoint of MSRIV, the valve opening time, etc.

The design requirements for confinement of the MSRCV and MSRIV will be presented in the technical specifications and the supplier shall meet the requirements according to the specifications.

7.7.5.1.4 Compliance with Extra Safety Function Requirements

The system is designed to realise the extra supporting functions described in Sub-chapter 7.7.1.4:

The MSRIV is closed during normal operation of the plant and the opening setpoint of MSRIV is { }.

The MSRCV is varied automatically (opening/closing) depending on the power level of the core to give a rapid response when the SG pressure increases and to protect the RCP [RCS] against overcooling when the MSRIV opens spuriously.

7.7.5.2 Compliance with Design Requirements

7.7.5.2.1 Compliance with Safety Classification

The VDA [ASDS] is designed in accordance with the requirement described in Sub-chapter 4.4. The function category of VDA [ASDS] functions is listed in Table T-7.7-3 and the classification of main components of the system in Table T-7.7-4.

The documents relevant to the equipment classification will be delivered later.

T-7.7-3 Function Category of the VDA [ASDS]

System Function	Function Category
Isolating steam discharge line	FC1
Dumping steam to atmosphere	FC1
Controlling the steam discharge flowrate	FC1
Reducing noise	NC

T-7.7-4 Classification of Main Components of VDA [ASDS]

Component	Design Provision Category	Function Class	Design Provision Class	Seismic Category
MSRIV	DPM	F-SC1	B-SC2	SSE1
MSRCV	DPA	F-SC1	B-SC2	SSE1
Silencer	NC	F-SC1	NC	SSE1

7.7.5.2.2 Compliance with Reliability

a) Redundancy and SFC

The principle of the SFC is presented in Sub-chapter 7.2.4.

The VDA [ASDS] consists of three independent, redundant trains. Under accident conditions, even conservatively assuming one of the three trains is unavailable as a result of a single failure and another train is unavailable as a consequence of the initiating event, the remaining train can still satisfy the RCP [RCS] cooling requirement.

The prevention of the passive SFC after the postulated initiating event is the same as the active SFC, i.e. at least one train can perform the safety function if the passive SFC occurs on one train of the VDA [ASDS].

The detailed design result of the VDA [ASDS] is presented in Reference [41] [42] and [44].

b) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

Physical isolation and space separation are provided for the three trains of the VDA [ASDS].

c) Diversity

The principle of diversity is presented in Sub-chapter 7.2.4.

The diversity design in the VDA [ASDS] contains:

1) Heat removal via the SG is achieved with the diversity among the VDA [ASDS], GCT [TBS] and MSSVs.

2) SG overpressure protection is guaranteed with the diversity between the VDA [ASDS] and MSSVs.

3) SG isolation is provided with the diversity between the MSRIV and MSRCV.

The detailed design result of the VDA [ASDS] is presented in Reference [41] and [42].

d) Fail-safe Design

There is no fail-safe designed equipment in the VDA [ASDS].

e) Ageing and Degradation

The system is designed for the 60 year plant operation. The design life of the main equipment of the VDA [ASDS] is 60 years, which mainly include the:

1) MSRIV

2) MSRCV

However, some components of the valves may need to be replaced regularly according to manufacturer feedback.

The performance of equipment is guaranteed through life examination, inspection maintenance and testing, as well as monitoring during normal operation. Thus it can be ensured that ageing effects will not compromise safety performance. The detailed design arrangement around EMIT and equipment monitoring is presented [44].

The VDA [ASDS] is divided into three trains. Train A of the VDA [ASDS] is arranged in and on the roof of Safeguard Building A (BSA), while train B and train C are arranged in and on the roof of Safeguard Building B (BSB). The system layout design can ensure the accessibility and requirement for safety equipment in-service inspection and periodic tests including the necessary NDT. This includes the requirements of emergency and scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [43].

7.7.5.2.3 Compliance with Human Factors

The system design and the control function design of the VDA [ASDS] do not require short term operator intervention. No operator action within 30 minutes after initial event is required based on the VDA [ASDS] design result. The design information is presented in Reference [42] and [44].

It should be noted that there are operator actions during plant normal operation or accident conditions (including plant startup, shutdown, and maintenance or testing etc.). Relevant human actions important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of the human factor discipline. Relevant evaluated reports will be provided as references of Chapter 15.

7.7.5.2.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in Reference [1]. The VDA [ASDS] satisfies the requirement through the following design:

1) The VDAs [ASDS] are started automatically; no human operation is required from the Main Control Room (MCR) less than 30 minutes from the first significant signal;

2) The pilot valves of the MSRIVs and MSRCVs are solenoid and electric valves respectively which can be operated at MCR. No human operation is required outside the MCR less than 1 hour from the first significant signal.

The design of the VDA [ASDS] fulfils these principles via the control function design [44]. The design result has been estimated in the safety analysis.

b) Autonomy in Respect to the Heat Sink

The design principles relevant to the autonomy in respect to the heat sink are listed in Reference [1]. These principles are not applicable for the VDA [ASDS] design.

c) Autonomy in Respect to Power Supply Systems

All of the electrical equipment which supports the safety functions can be powered by appropriately qualified emergency power provisions. The MSRIV and MSRCV will be supplied with 2h batteries (safety class), EDGs and SBO diesel generators.

7.7.5.2.5 Compliance with Other design requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

This principle is not applicable for VDA [ASDS] design.

b) Considerations Related to the Electrical Power Grid

The principle is not applicable for VDA [ASDS] design.

7.7.5.2.6 Compliance with Equipment Qualification

According to Chapter 4, all components required to perform the safety functions shall be capable of operating under normal conditions and accidental conditions, which requires the components to withstand the adverse ambient environments.

The MSRIV and MSRCV will be qualified in accordance with the requirements described in Chapter 4.

The documents relevant to the equipment qualification will be developed during Step 4 of GDA.

7.7.5.2.7 Compliance with Hazard Protection

The VDA [ASDS] protection against internal and external hazards is in accordance with the principle of Chapter 19 and Chapter 18. The VDA [ASDS] takes the following measures to prevent the hazards:

a) Internal Hazards

The three trains of the VDA [ASDS] are distributed in and on the roof of the steam valve compartments of Safeguard Building A (BSA) and Safeguard Building B (BSB). The specific protection design is presented in Reference [43]. Evaluation of the design is presented in Chapter 19.

b) External Hazards

1) Earthquake

As shown in Table T-7.7-4, the seismic categorisation of the MSRIV, MSRCV and silencer is SSE1; the equipment can still perform the desired safety functions in the Safe Shutdown Earthquake (SSE) condition.

2) Other external hazards

The VDA [ASDS] protects against external disasters mainly through the building design. Specific protection design is presented in Reference [43], while the evaluation of the design is presented in Chapter 18.

7.7.5.2.8 Compliance with Commissioning

Initial testing (e.g. factory acceptance tests) of components before delivery to site

shall be undertaken to ensure that the safety functions of these components can be properly performed. The design requirements will be provided to the equipment vendor in form of technical specifications.

Commissioning is going to be carried out for the VDA [ASDS] to validate its functionality. During commission, the following tests will be implemented to validate the operability of individual components and system functions:

a) Valve Test: Examination and test of valves;

b) MSRIV Test: Operability of the MSRIV and its solenoid pilot valve, correct action of stem limit switch, action sequence and opening/closing time of MSRIV;

c) MSRCV Test: Operability, operating time and correct valve position of MSRCV;

The detailed description is presented in Reference [44], and documents such as the System Commissioning Program related to the commissioning are going to be submitted.

7.7.5.2.9 Compliance with Examination, Inspection, Maintenance and Testing

According to Chapter 31, the in-service inspection implemented during operation is defined on the basis of RSE-M 2010 edition including the 2012 addendum. The equipment and lines belonging to the main secondary loop require in-service inspection, i.e., VDA [ASDS] components located from the Main Steam Line (MSL) nozzle to the MSRCV.

The documents relevant to the equipment pre-service inspection list will be delivered.

The main equipment of the VDA [ASDS] is arranged in the steam valve compartments, located in the uncontrolled zone outside the containment, hence accessible in any plant normal operation state. The introduction of the VDA [ASDS] layout refers to Reference [43].

Equipment availability and characteristic values must be measured through periodic tests. The following tests will be carried out for the VDA [ASDS] valves:

a) Operability of the MSRIV pilot valve;

b) Operability of the MSRIV and MSRCV;

c) Local operability of the MSRIV and MSRCV.

The documents relevant to the System Periodic Test Completeness Note will be delivered.

The detailed description around EMIT is presented in Reference [44].

7.7.5.2.10 Special Thermal-Hydraulic Phenomena

In order to prevent water hammer while the VDA [ASDS] dumps steam into

atmosphere, the drain line downstream of the MSRCV is used to drain condensate. The arrangement of the drain line can ensure that there is no water in the discharge line during normal operation, so that the risk of water hammer can be reduced.

7.7.5.2.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component is presented in Sub-chapter 7.7.4.1.2.

7.7.5.2.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

Insulation of the VDA [ASDS] is considered for staff safety protection. Accessible equipment or pipe with high surface temperature will be insulated to prevent burns.

The main equipment of the VDA [ASDS], including the MSRCV and MSRIV are equipped with insulation and the insulation material is glass fiber.

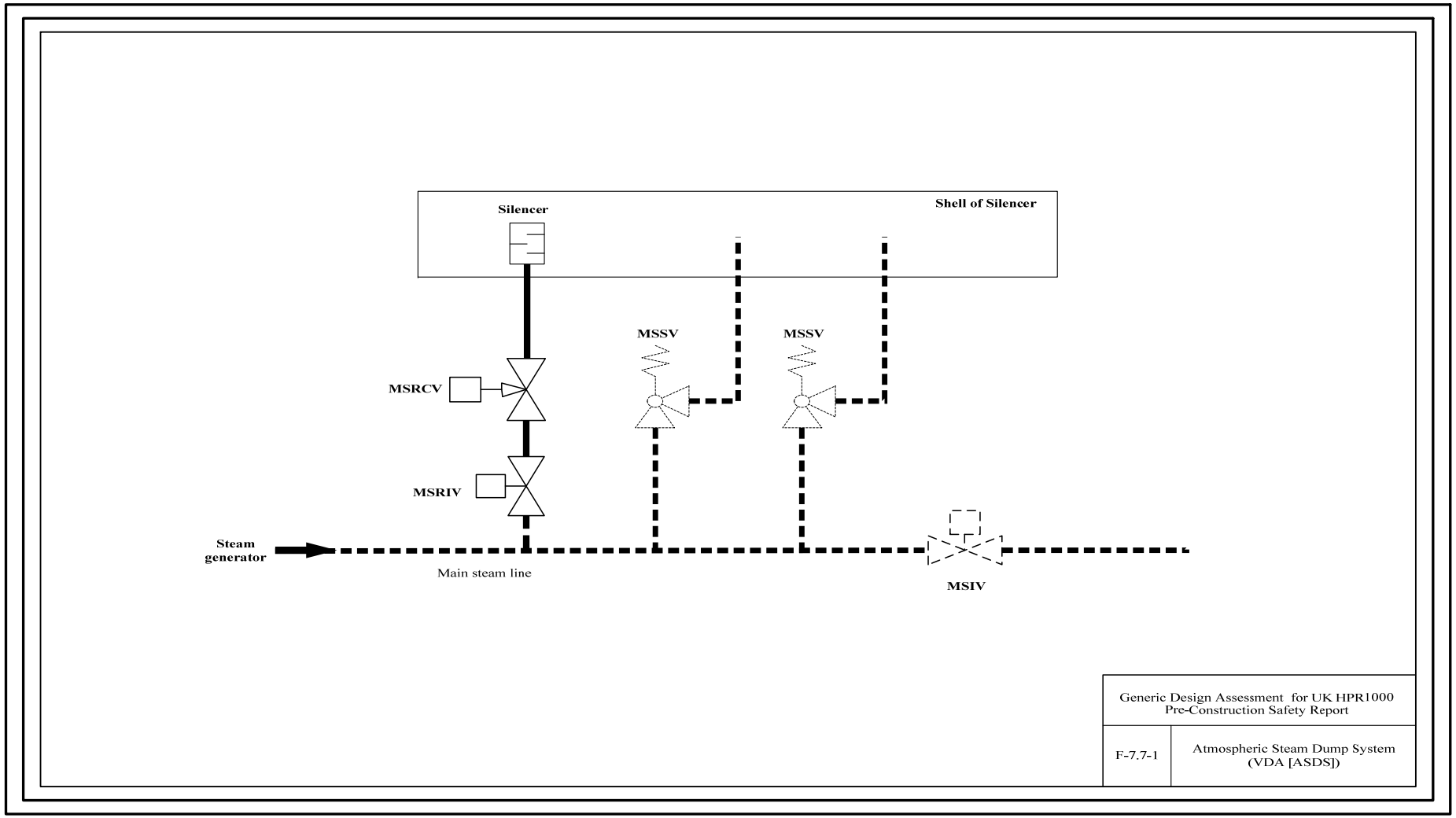
The main steam dumping line with the instrument line and drain line connected to it, and the silencer drain line are equipped with insulation. The insulation material is glass fiber.

7.7.5.2.13 Decommissioning

The layout of the VDA [ASDS] considers decommissioning, such as the accessibility for personnel, how the arrangement of access to components will facilitate maintenance and dismantling, etc.

7.7.6 Functional Diagrams

The simplified functional diagram of the VDA [ASDS] is shown in Figure F-7.7-1. The detailed system functional diagrams are presented in Reference [45].



F-7.7-1 Simplified Functional Diagram of the VDA [ASDS]

7.8 Emergency Feedwater System (ASG [EFWS])

7.8.1 Safety Requirements

The contribution of the ASG [EFWS] to the safety functions is described below, Reference [46] and [47].

7.8.1.1 Control of Reactivity Requirement

In the event of a Main Steam Line Break (MSLB), the ASG [EFWS] connecting to the affected SG is isolated to avoid overcooling of the reactor.

7.8.1.2 Removal of Heat Requirement

The ASG [EFWS] supplies water to the SGs to remove the residual heat until the Safety Injection System (RIS [SIS]) is able to operate in the RHR mode when the ARE [MFFCS] and Startup and Shutdown Feedwater System (AAD [SSFS]) are unavailable.

In the case of DEC-A, such as SBO and Total Loss of Cooling Chain (TLOCC), the ASG [EFWS] supplies water to SGs to cool the RCP [RCS] and reactor.

7.8.1.3 Confinement Requirement

The ASG [EFWS] connecting to the affected SG is isolated to avoid containment bypass in the event of SGTR.

In the event of MSLB or Feedwater Line Break (FLB), the ASG [EFWS] connecting to the affected SG is isolated to limit the pressure and temperature of the containment.

7.8.1.4 Extra Safety Function Requirements

The ASG [EFWS] shall contribute to the extra supporting functional requirements as follows, Reference [47]:

a) Limiting the power of ASG [EFWS] pumps;

b) Adjusting the SG level.

7.8.2 Design Requirements

The general design requirements of the safety systems which need to be considered are shown in Sub-section 7.2.4, and the following requirements are not applicable to the ASG [EFWS]:

a) Fail-safe: There is no fail-safe requirement on the ASG [EFWS].

b) Autonomy in Respect of Heat Sink: the ASG [EFWS] is not a heat sink system. The autonomy of heat sink is not applicable to the ASG [EFWS].

The substantiation analysis of the ASG [EFWS] to other design requirements is shown

in Sub-section 7.8.5.

7.8.3 Design Bases

7.8.3.1 General Assumptions

The ASG [EFWS] belongs to the engineered safety systems and supplies water to the SG to remove residual heat in the events when the ARE [MFFCS] and AAD [SSFS] are unavailable.

This sub-chapter aims to provide the main design assumptions considered in the system design.

a) Safety Classification

The emergency feedwater pump and related valves are used to reach a controlled state under DBC-2/3/4 (if the functions are not performed, the consequences are high), therefore the equipment that perform this function is FC1 classified.

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which are important to safety shall be taken into account.

The design life of the main equipment of the ASG [EFWS] is 60 years. In addition, some parts of the main equipment may need to be replaced regularly during the design life.

c) Autonomy

The water inventory of the tanks allows the plant to be maintained in the hot shutdown state for 24h.

d) Equipment Qualification

The components of the ASG [EFWS] performing safety functions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

The fluctuation of the electrical power grid may affect the ability of safety functions, especially the performance of the active equipment, such as the emergency feedwater pumps.

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in ASG [EFWS] equipment design, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions shall be performed under earthquake events. Therefore, equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.8.3.2 Design Assumptions

7.8.3.2.1 Control of Reactivity Assumptions

There is no quantitative requirement for the ASG [EFWS].

7.8.3.2.2 Removal of Heat Assumptions

The ASG [EFWS] supplies water to the SGs to remove the residual heat until the RIS [SIS] is able to operate in the RHR mode when the ARE [MFFCS] and AAD [SSFS] are unavailable. The requirements for the ASG [EFWS] are as follows, Reference [47]:

a) Flowrate Requirements Assumptions

The minimum flowrate requirements of one ASG [EFWS] train are as follows:

1) { }

2) { }

The maximum required ASG [EFWS] flowrate shall be limited to avoid containment overpressure in a MSLB accident. The maximum flowrate requirement of one ASG [EFWS] train is { } at { } in the SG.

b) Water Inventory

The ASG [EFWS] is designed to provide three separate tanks; each tank can be connected to the others manually to ensure that the water in all three tanks is available under the accident conditions.

The water inventory of the tanks allows the plant to be maintained in hot shutdown state for 24h. The minimum water inventory of each tank is { }.

The tanks can be resupplied by the ASP [SPHRS] if all of them are empty (The quantity of the storage tank in the ASG can satisfy the 24h operation requirement. After 24h, the ASG water tank can be filled by the ASP. The ASG can continuously operate for another 48h by the ASP refilling the water in the storage tank.

c) Temperature Requirements

The temperature requirement for the water in the storage tanks is between { } in the short term following accidents and { } in the long term (over 24 hours).

d) System start-up time

The time delay from the signal to start-up of the emergency feedwater pumps until its operation at full flow rate is no more than { }.

7.8.3.2.3 Confinement

In the event of SGTR, ASG [EFWS] isolation is required on the affected SG. This function can be actuated automatically following the SG high level signal in the event of SGTR. The isolation time shall not exceed{ }.

Both the SG level control valves and containment isolation valves can be used to isolation the ASG [EFWS].

In severe accidents, isolation can be achieved by closing the external containment isolation valves of the ASG [EFWS].

7.8.3.2.4 Extra Safety Function Assumptions

Relevant control valves need to be set to control the flow rate at the pump discharge and the water level within the SG.

7.8.4 System Description and Operation

7.8.4.1 System Description

7.8.4.1.1 General System Description

The ASG [EFWS] consists of three identical trains corresponding to each SG. Each ASG [EFWS] train consists of the following equipment:

a) One storage tank;

b) One emergency feedwater pump;

c) One flow limitation control valve;

d) One SG level control valve;

e) Containment isolation valves.

The suction and discharge sides of the three pumps are connected via common headers which are normally isolated, Reference [48].

The volume of the three water tanks meets the water demand for24h after the accident. After 24h the ASG [EFWS] water tank can be filled by the ASP [SPHRS]. If the water replenishment function of the ASG [EFWS] is still required after 72 hours, mobile

equipment can provide water to the ASG [EFWS] water tank through the temporary interface of the ASG [EFWS] water tank.

The simplified flow diagram of the ASG [EFWS] is shown in Figure F-7.8-1.

7.8.4.1.2 Description of Main Equipment

a) Emergency Feedwater Pump

The emergency feedwater pumps are identical, centrifugal multistage and horizontal motor-driven pumps. Each pump can perform the emergency feedwater function for the SGs with 100% capacity. These pumps are self-lubricating and self-cooling, and consequently do not require support from additional cooling water systems, Reference [48].

A three-way valve is installed at the outlet of each pump to meet the requirements of minimum flow and the periodic pump test. If the pump flowrate is lower than the set point, the valve will open the miniflow line to the ASG [EFWS] tank automatically.

In the event of injection to a depressurised SG, the injection flowrate is limited by a flow limitation control valve.

T-7.8-1 Main design characteristics of the Emergency Feedwater Pump

Parameters	**Value**	**Unit**
Type	Multi-Stage Centrifugal Pump	
Design Life	60	yr.
Nominal Flowrate	90/110	m^3/h
Discharge Head at Nominal Flowrate	1077/1013	mWc
Material	Stainless Steel	

b) Storage Tank

The ASG [EFWS] storage tanks are of a concrete construction with a stainless steel liner.

T-7.8-2 Main design characteristics of the ASG [EFWS] tank

Parameters	**Value**	**Unit**

Parameters	Value	Unit
Type	Concrete Tank with Steel Liner	
Medium	Demineralised water	
Design Pressure	0.1	MPa (g)
Design Temperature	60	°C
Usable Volume	561.9	m^3
Max. Volume	692.8	m^3
Material	Stainless Steel	

c) Flow Limitation Control Valve

They are electric control valves installed downstream of each emergency feedwater pump. They can limit the maximum feedwater flowrate of the pump and consequently protect the pump motor from damage, Reference [48].

Each valve has a mechanical stop to prevent the valve from fully closing. When the valve is at the mechanical stop position, the flowrate will not exceed the maximum allowed value of the pump even in worst case scenario, Reference [48].

d) SG Level Control Valve

The motor-driven valves control the SG level and prevent the affected SGs from overfilling. The valve will be closed automatically if the affected SG level is too high, Reference [48].

e) Containment Isolation Valves

There are two containment isolation valves in each ASG [EFWS] train. One is a check valve located inside the containment, while the other is an electrical valve outside the containment. The electrical valve at the affected train will be closed automatically if the SG level is too high, Reference [48].

7.8.4.1.3 Description of Main Layout

The ASG [EFWS] is a safety system with three trains and each train is located in the three safeguard buildings respectively. This layout can prevent the three trains from being affected by internal hazards (common cause failure) simultaneously, Reference [49].

The ASG [EFWS] lines are connected to the SGs directly instead of the ARE [MFFCS] to avoid a water hammer phenomenon.

7.8.4.1.4 Description of System Interface

The following systems are set to support the ASG [EFWS] operation, Reference [48].

a) CI Dematerialised Water Distribution System (SER [DWDS (CI)])

SER [DWDS (CI)] supplies demineralised water to the ASG [EFWS] tanks.

b) Secondary Passive Heat Removal System (ASP [SPHRS])

In the event of DBC-2/3/4 long-term stage and DEC-A, ASP [SPHRS] can supply water to the ASG [EFWS] tanks if the SER [DWDS (CI)] is unavailable.

c) NI Chemical Reagents Distribution System (SIH [CDS])

The SIH [CDS] adds chemical reagents at the discharge of the emergency feedwater pumps.

d) Station Sewage System (SEO [SSS])

The ASG [EFWS] tanks can be drained to the SEO [SSS] during plant outage.

7.8.4.1.5 Instrumentation and Control

a) Automatic control

The ASG [EFWS] has the following automatic control functions, Reference [50]:

1) Start-up of the corresponding train if any SG is at water level low 2;

2) Start-up all trains if Safety Injection (SI) plus LOOP occur;

3) Isolate the corresponding train if any SG is at high water level;

4) Control SG level;

5) Protect the emergency feedwater pump against overflow.

These automatic controls are actuated by the Reactor Protection System (RPR [RPS]). The corresponding train can also be started through Diversity Actuation System (KDS [DAS]) even if the RPR [RPS] is unavailable when one SG is at water low level 2.

The ASG [EFWS] can be started and isolated manually by the operator in the MCR when necessary

b) Information to the Operator

The information available to the operator in the MCR for each ASG [EFWS] train is as follows:

1) Water level and temperature inside the storage tanks;

2) Position of the valves on the injection lines and common headers;

3) The injection flow rates.

7.8.4.2 System Operation

7.8.4.2.1 System Operation in Plant Normal Operation

During normal shutdown, the ASG [EFWS] can be used to supply water with the appropriate chemical reagent for wet lay-up of the SGs.

Before the ARE [MFFCS] or AAD [SSFS] is put into operation, the ASG [EFWS] can be used to compensate for the water evaporation of the SGs during plant start-up to maintain the normal water level of the SGs.

During other normal states of the plant, the ASG [EFWS] is in the standby state while:

a) The emergency feedwater pumps are shut down and available;

b) The flow limitation control valves are closed at the mechanical stop;

c) The SG level control valves are fully open;

d) The electrical containment isolation valves are open;

e) The manual valves on the connection lines are closed;

f) The ASG [EFWS] tanks are full of water.

The SER [DWDS (CI)] can supply water to the ASG [EFWS] tanks if necessary.

7.8.4.2.2 System Operation under Accident Conditions

The ASG [EFWS] shall provide emergency feedwater to the unaffected SGs in DBC-2/3/4 to remove the core decay heat from the RCP [RCS] via the SGs, until the RIS [SIS] connects and operates in RHR mode.

The ASG [EFWS] shall provide emergency feedwater to the SGs and remove the core decay heat from the RCP [RCS] via the SGs. Thus the reactor can achieve the safety state in DEC-A condition (such as SBO and TLOCC).

a) System Start

The emergency feedwater pumps can be started automatically by the RPR [RPS] or manually by the operator. Water can be injected into the SGs directly as the valves are in open position originally or in the mechanical stop position (flow limitation control valve).

In the event of SBO, train A or train B can be started manually because of SBO diesel generators power supply.

b) System Isolation

In the event of MSLB or FLB, the train connected to the affected SG shall be isolated to limit the pressure and temperature of the containment.

In the event of SGTR, the train connected to the affected SG shall be isolated automatically to prevent a potential containment bypass route from radioactive release to the environment.

The ASG [EFWS] can be isolated automatically or manually by either the SG level control valve or the electrical containment isolation valve.

c) SG Level Control

The SG water level can be maintained at the set value automatically by the SG level control valve.

In the event of SBO, the SG level control valves are powered by 2-hour batteries.

d) Water Sharing of ASG [EFWS] tanks

The manual valves on the connection lines of pumps on the suction side can be opened by the operator if necessary to share the water of the three ASG [EFWS] by using any of the pumps.

e) Feedwater Sharing of SGs

The manual valves on the connection lines of pumps on the discharge side can be opened by the operator to share the feedwater of one pump to any SGs.

f) Refilling of ASG [EFWS] Tanks

The ASG [WFES] tanks can be refilled by the SER [DWDS (CI)], and can also be refilled by the ASP [SPHRS] in the event of DBC-2/3/4 or DEC-A accidents if the SER [DWDS (CI)] is unavailable.

7.8.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. The detailed design of the system is presented in Reference [47] [48] [49] [50] and [51]. Furthermore, design substantiation of the ASG [EFWS] is estimated in the fault study in Chapter 12 and 13.

7.8.5.1 Compliance with Safety Requirements

a) Compliance with Control of Reactivity Requirements

The water injected into the affected SG in the event of a MSLB can be isolated by closing the SG level control valve and electrical containment isolation valve manually to avoid overcooling of the reactor.

b) Compliance with Removal of heat Requirements

The emergency feedwater in the ASG [EFWS] tanks can be injected to the SGs by pumps, and the residual heat of the core can be removed through SGs until the RIS [SIS] is able to connect in RHR mode. The ASG [EFWS] can be started automatically or manually.

The fault study in Sub-chapter 12.9 and 13.5 justifies that each safety function required on the ASG [EFWS] in Sub-chapter 7.8.1.2 is met based on the design assumptions provided in Sub-chapter 7.8.3.2.2, including the flowrate, water tank volume etc.

The parameter requirements of the emergency feedwater pump are shown in Reference [48]. These parameter requirements are presented in the equipment technical specifications and the equipment supplier shall meet the requirements according to the specifications.

The usable water volume of each tank is about $560m^3$, which meets the water requirement specified in Sub-chapter 7.8.3.2.2.

c) Compliance with Confinement Requirements

In the event of SGTR, ASG [EFWS] isolation is required on the affected SG. This function can be actuated automatically on the SG high level signal in the event of SGTR. The closing time of the valve is 30s (the equipment supplier will meet the closing time requirement), which meets the requirement specified in Sub-chapter 7.8.3.2.3.

d) Compliance with Extra Safety Function Requirements

The flow limitation control valve controls the flow rate of the emergency feedwater pump to limit the pump power.

The SG level control valve can adjust the SG level and avoid the SGs overfilling.

7.8.5.2 Compliance with Design Requirements

7.8.5.2.1 Compliance with Safety Classification

The ASG [EFWS] design is compliant with the requirements described in Chapter 4.

The safety function category of the ASG [EFWS] is listed below, Reference [47]:

a) Emergency feedwater function: FC1;

b) SG isolation: FC1;

c) Connection of the pumps suction and discharge: FC2;

d) Mixing and drain of the storage tanks: NC

The documents relevant to the equipment classification will be delivered.

T-7.8-3 Classification for Components

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
Emergency Feedwater Pump	F-SC1	---	NC	SSE1
Flow Limitation Control Valve	F-SC1	---	NC	SSE1
SG Level Control Valve	F-SC1	---	NC	SSE1
Containment Isolation Valve	F-SC1	DPA	B-SC2	SSE1
ASG [EFWS] Tank	F-SC1	---	NC	SSE1

7.8.5.2.2 Compliance with Reliability

a) Redundancy and SFC

The principle of the SFC is presented in Sub-chapter 7.2.4.

The ASG [EFWS] consists of three independent and redundant trains. The connection headers of the suction side and discharge side of pumps between the three trains allow individual pumps to be re-aligned to any available ASG [EFWS] tank and SG. The three ASG [EFWS] trains are physically separated from each other since they are located in each of the three safeguard buildings respectively. Under accident conditions, even conservatively assuming one of the three trains is unavailable as a result of a single failure and another train is unavailable as a consequence of the initiating event, the remained train can still perform the required safety function with 100% capacity (The ASG water tank does not consider the passive SFC within 24h after the accident, the volume of three water tanks meets the water demand for 24h after the accident).

The prevention of the passive SFC after the postulated initiating event is the same as the active SFC, i.e. one train can still preform the safety function if the passive SFC occurs on one train of the ASG [EFWS].

The detailed design result of the ASG [EFWS] is presented in Reference [47] [48]

and [50].

b) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The ASG [EFWS] consists of three independent trains, each of which is located in one of the three safeguard buildings respectively. The cross connection lines between them are isolated by manual valves in the standby state.

c) Diversity

The principle of diversity is presented in Sub-chapter 7.2.4.

The diversity design in the ASG [EFWS] contains that:

1) The residual heat can be removed by either the ASG [EFWS] or ASP [SPHRS] after accident.

2) Each ASG [EFWS] train is supplied by an electrical division and backed-up by the EDGs. Furthermore, train A and train B of the ASG [EFWS] can be powered by the SBO diesel generators if the EDGs are unavailable.

3) The ASG [EFWS] can be isolated by either the SG level control valve or the electrical containment isolation valve.

The detailed design result of the ASG [EFWS] is presented in Reference [47] and [48].

d) Fail-safe Design

There is no fail-safe designed equipment in the ASG [EFWS].

e) Ageing and Degradation

The system is designed for the 60 year plant operation. The design life of the main equipment of the ASG [EFWS] is 60 years, which mainly includes the:

1) Emergency Feedwater Pump;

2) Storage Tank.

The performance of equipment is guaranteed through life examination, inspection maintenance and testing, as well as monitoring during normal operation. Thus it can be ensured that ageing effects will not compromise safety performance. The Detailed design arrangement around EMIT and equipment monitoring is presented in Reference [50].

The system layout design can ensure the accessibility and requirement for safety equipment in-service inspection and periodic tests including the necessary NDT. This includes the requirements of emergency and scheduled maintenance on the

SSCs. Detailed layout information is presented in Reference [49].

7.8.5.2.3 Compliance with Human Factors

The system design and the control function design of the ASG [EFWS] does not require short term operator intervention. No operator action is required within 30 minutes after the initial event based on the ASG [EFWS] design result. The design information is presented in Reference [48] and [50].

It should be noted that there are operator actions during plant normal operation or accident conditions (including plant startup, shutdown, and maintenance or testing etc.). Relevant human actions important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of the human factors discipline. Relevant evaluated reports will be provided as references of Chapter 15.

7.8.5.2.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in Reference [1]. The ASG [EFWS] satisfies the requirement through the following design:

1) The emergency feedwater pumps are started automatically under the accident condition; no human operation is required from the MCR less than 30 minutes from the first significant signal;

2) All electric valves performing safety functions can be operated at the MCR; no human operation is required outside the MCR less than 1 hour from the first significant signal.

3) The manual valve of the ASG [EFWS] can be operated one hour after the accident; no human operation is required outside the MCR less than 1 hour from the first significant signal.

The design of the ASG [EFWS] fulfils these principles via the control function design [50]. The design result has been estimated in the safety analysis.

b) Autonomy in Respect to the Heat Sink

The total usable water capacity of the ASG [EFWS] tank is about 1700m^3; the water volume of the tanks can maintain the plant in hot shutdown mode for 24h without requiring any refilling.

c) Autonomy in Respect to Power Supply Systems

All of the electrical equipment which supports the safety functions can be

powered by appropriately qualified emergency power provisions. Each ASG [EFWS] train is supplied by an electrical division and backed-up by the Emergency Diesel Generators (EDGs). Furthermore, ASG [EFWS] trains A and B are powered by the Station Black Out (SBO) diesel generators in the event of loss of the EDGs.

7.8.5.2.5 Compliance with Other design requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

According to Reference [1], the protection of interfacing systems shall be considered in ASG [EFWS] design. The ASG [EFWS] takes the following measures to prevent the harmful interactions of systems:

1) Provide adequate isolation between the ASG [EFWS] and interfacing systems;

2) The design pressure of the isolation valve between ASG [EFWS] and the interface system adopts the larger pressure;

Detailed information is in [50] and [51].

b) Considerations Related to the Electrical Power Grid

According to Reference [1], the functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid.

The fluctuation of the electrical power grid mainly affects the functional capability of emergency feedwater pumps. The pump flow will change with the fluctuation of the power grid. In the HPR1000 (FCG3) project，the design of emergency feedwater pumps considers the influence of grid fluctuation [48]. Re-estimates will be carried out during GDA progress, on the basis of the UK context, relevant to the electrical power grid.

7.8.5.2.6 Compliance with Equipment Qualification

According to Chapter 4, all components required to perform the safety functions shall be capable of operating under both normal and accidental conditions, which requires the components to withstand the adverse ambient environments.

The equipment performing an FC1 or FC2 function in the ASG [EFWS] will be qualified in accordance with the requirements described in Chapter 4.

The documents relevant to equipment qualification will be developed during Step 4 of GDA.

7.8.5.2.7 Compliance with Hazard Protection

The ASG [EFWS] protection against internal and external hazards is in accordance

with the principles of Chapter 19 and Chapter 18. The ASG [EFWS] takes the following measures to prevent the hazards:

a) Internal Hazards

The protection against internal hazards mainly depends upon the buildings, rooms, fire compartments and anti-flooding compartments arranged for the ASG [EFWS]. The specific measures are as follows:

1) Three trains of the ASG [EFWS] are arranged in different safeguard buildings, therefore if one train is affected by a single internal hazard, the other two trains will remain since they are separated from each other physically. Thus the ASG [EFWS] can still perform its functions;

2) The redundant trains are physically separated by the building in the containment.

The specific protection design is presented in Reference [49]. The evaluation of the design is presented in Chapter 19.

b) External Hazards

1) Earthquake

As shown in Table T-7.8-3 and [47], the main equipment of the ASG [EFWS] performing safety functions is SSE1; the equipment can still perform the desired safety functions in the Safe Shutdown Earthquake (SSE) condition.

The documents relevant to the equipment seismic categorisation will be delivered.

2) Other external hazards

The building design of the ASG [EFWS] can protect against external hazards. The specific protection design is presented in Reference [49]. The evaluation of the design is presented in Chapter 18.

7.8.5.2.8 Compliance with Commissioning

Initial testing (e.g. factory acceptance tests) of components before delivery to site shall be undertaken to ensure that the safety functions of these components can be performed properly. The design requirements will be provided to the equipment vendor in form of technical specifications.

Commissioning is going to be carried out for the ASG [EFWS] to validate its functionality. The following tests require checking or validating:

a) Components of the ASG [EFWS], such as valves, pumps and the I&C system, can operate compliant with design specifications;

b) ASG [EFWS] is in compliance with its safety functions;

c) ASG [EFWS] is in compliance with its operating functions.

The detailed description is presented in Reference [50]. The documents such as the 'System Commissioning Program' related to the commissioning are going to be submitted.

7.8.5.2.9 Compliance with Examination, Inspection, Maintenance and Testing

According to Chapter 31, in-service inspection implemented during operation is defined on the basis of RSE-M 2010edition including the 2012 addendum. In-service inspection shall be considered for the components from the electric containment isolation valve to the SGs.

The documents relevant to the equipment pre-service inspection list will be delivered.

The ASG [EFWS] equipment is designed and installed by considering personnel accessibility. There is enough space for inspection and testing around the equipment.

The system is designed for the 60 year plant operation. The design life of the main equipment in the ASG [EFWS] is 60 years. The components mainly include the:

a) Emergency Feedwater Pump

b) Storage Tank

However, some pump components require replacing regularly according to manufacturer feedback, such as gaskets, mechanical seals, O-ring and bearings.

The ASG [EFWS] doesn't consider the scheduled maintenance when it is on standby. The scheduled maintenanc can be done in Refuelling Cold Shutdown (RCS) or Maintenance Cold Shutdown (MCS) if necessary.

The ASG [EFWS] layout design can ensure the accessibility and requirement for maintenance; in-service inspection and periodic tests are met. The system layout design considers the following factors:

a) The needs for maintenance, including removing the worn parts and installing the replacements;

b) The accessibility and requirement for safety equipment in-service inspection and periodic tests;

c) The requirements of emergency and scheduled maintenance on the SSCs over the life span of the plant.

The introduction of the ASG [EFWS] layout refers to reference [49]

The safety function of the ASG [EFWS] shall be checked in periodic tests; this also applies to the operability of the emergency feedwater pumps. The documents relevant

to the System Periodic Test Completeness Note will be delivered.

The detailed description around EMIT is presented in Reference [50].

7.8.5.2.10 Special Thermal-Hydraulic Phenomena

The ASG [EFWS] lines are connected to the SGs directly, independently of the ARE [MFFCS] to avoid the water hammer phenomena occurring.

The lines inside the containment do not have any inverted U types to avoid the water hammer phenomena occurring.

7.8.5.2.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component is presented in Sub-chapter 7.8.4.1.2.

7.8.5.2.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

The operating temperature of the main pipes and valves of the ASG [EFWS] in the safeguard building is low, therefore there is no requirement for insulation.

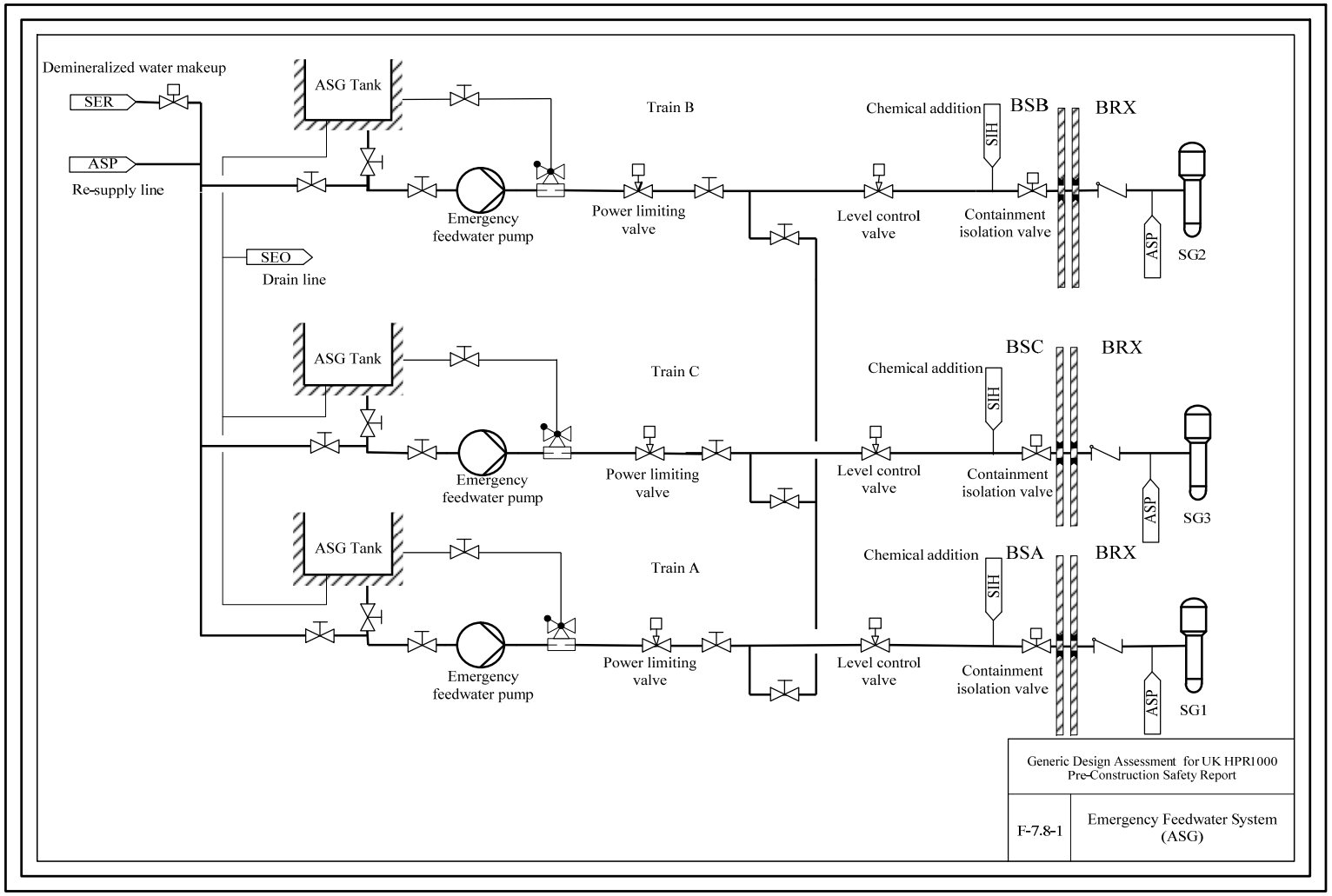
The lines between the SGs and the check valves (as the part of secondary loop) inside the containment are equipped with insulation and the insulation material is glass fiber.

7.8.5.2.13 Decommissioning

The ASG [EFWS] is not radioactive and therefore the main consideration of the ASG [EFWS] for decommissioning is in the layout, i.e. the arrangement of access to components will facilitate maintenance and dismantling.

7.8.6 Functional Diagrams

The simplified functional diagram of the ASG [EFWS] is shown in Figure F-7.8-1. The detailed system functional diagrams are presented in Reference [51].



F-7.8-1 Simplified Functional Diagram of the ASG [EFWS]

7.9 Secondary Passive Heat Removal System (ASP [SPHRS])

7.9.1 Safety Requirements

The requirements of safety functions on the ASP [SPHRS] design for the UK HPR1000 are identified below, Reference [52] and [53].

7.9.1.1 Control of Reactivity Requirements

The ASP [SPHRS] does not contribute to this safety functions.

7.9.1.2 Removal of heat

The ASP [SPHRS] is designed to provide decay heat removal during DEC-A accidents and when the Emergency Feedwater System (ASG [EFWS]) is required to put into operation and the ASG [EFWS] fails. In these conditions, the ASP [SPHRS] is able to start automatically or manually to remove the primary loop heat continuously.

7.9.1.3 Confinement Requirements

The ASP [SPHRS] contributes to the containment isolation of the secondary system.

7.9.1.4 Extra Safety Function Requirements

The ASP [SPHRS] shall contribute to the extra supporting functional requirements as follows:

a) The ASP [SPHRS] water tank shall be equipped with relevant water level monitoring instruments to monitor the water level of the water tank.

b) The ASP [SPHRS] shall provide makeup water manually for spent fuel pools when the Fuel Pool Cooling and Treatment System (PTR [FPCTS]) cooling loop mechanical system fails.

7.9.2 Design Requirements

The general design requirements of the safety systems which need to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to the ASP [SPHRS]:

a) Redundancy and the SFC: The ASP [SPHRS] performs an FC3 function and does not need to meet the SFC criteria. However, the equipment that performs FC1 and FC2 functions within the system need to meet the SFC criteria.

b) Fail-safe: There is no fail-safe requirement on the ASP [SPHRS].

c) Considerations Related to the Electrical Power Grid: The ASP [SPHRS] does not include pumps that perform safety functions or other equipment which would be affected by the power grid.

The substantiation analysis of the ASP [SPHRS] to other design requirements is shown in Sub-chapter 7.9.5.

7.9.3 Design Bases

7.9.3.1 General Assumptions

The ASP [SPHRS] belongs to the safety systems, which is designed to remove primary loop heat during DEC-A and provide water to the Emergency Feedwater System (ASG [EFWS]) and Fuel Pool Cooling and Treatment System (PTR [FPCTS]) when necessary. The ASP [SPHRS] consists of three trains, each of which corresponds to one SG.

This Sub-chapter aims to provide the main design assumptions considered in the system design, Reference [53].

a) Safety Classification

The ASP [SPHRS] is used in DEC-A accident conditions, therefore the classification of the system is FC3. However, the ASP [SPHRS] needs to perform the containment isolation function under design basis conditions, and these valves that perform the containment isolation are classified as FC1.

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which is important to safety shall be taken into account.

The design life of the main equipment of the ASP [SPHRS] is 60 years. In addition, some parts of the main equipment may need to be replaced regularly during the design life.

c) Autonomy

The function of the water tank is to receive the heat from the condenser and discharge the heat into the atmosphere through evaporation or boiling of the water stored in the tank. The water inventory of the tanks needs to meet the heat removal requirement 72h after the accident.

d) Equipment Qualification

The components of the ASP [SPHRS] performing safety functions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

There is no quantitative requirement for the ASP [SPHRS].

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in ASP [SPHRS] equipment design, such as internal flooding, high energy pipe failure, and earthquakes.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions shall be performed under earthquake events. Therefore, equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.9.3.2 Design Assumption

a) Control of reactivity

The ASP [SPHRS] does not contribute to this safety function.

b) Removal of heat

The ASP [SPHRS] shall perform the residual heat removal function during DEC-A accident conditions as follows:

1) SBO with Emergency Feedwater System (ASG [EFWS]) failure;

2) Total Loss of Feedwater (TLOFW);

3) Other accidents requiring the ASG [EFWS] with ASG [EFWS] failure.

In addition, the ASP [SPHRS] can also supply water to the ASG [EFWS] in the long term following DEC-A events when the ASG [EFWS] and VDA [ASDS] are used for heat removal. The ASP [SPHRS] ensures cooling of the spent fuel pool by providing make-up water when all trains of the Fuel Pool Cooling and Treatment System (PTR [FPCTS]) cooling loop fail.

The water tank of the ASP [SPHRS] has an available volume of { }of water.

Each ASP [SPHRS] is required to remove at least { }of heat.

b) Confinement

The ASP [SPHRS] contributes to the containment isolation of the secondary system.

c) Extra Safety Function Design Assumptions

1) The function of monitoring the water level of the water tank is FC3, no SFC is considered. Therefore, at least one water level sensor shall be set.

2) The ASP [SPHRS] shall provide makeup water manually for the spent fuel pools when the PTR [FPCTS] cooling loop mechanical system fails, there is no quantitative requirement.

7.9.4 System Description and Operation

7.9.4.1 System Description

7.9.4.1.1 General System Description

The system is composed of three trains corresponding to the three SGs. Each train mainly consists of:

a) Steam Inlet Pipe

The steam inlet pipe is connected to the main steam line between the containment boundary and the MSIV, and contains two isolation valves.

b) Condenser

The condenser is located at a higher elevation than the SG and is submerged in the ASP [SPHRS] tank.

c) Feed Pipes

The feed pipes connect the outlet of the condenser to the ASG [EFWS] feedwater lines that deliver the condensate water to the SGs.

More detailed information is presented in Reference [55].

The system operation is designed as passive operation using natural circulation. The cold heat sink, i.e the water tank (where the condensers are submerged), is arranged at a higher position than the hot source (SG). The density difference can be formed between the steam pipe and the condensate pipe. Consequently, the height and density difference can provide a sufficient driving force for the natural circulation. The primary heat transferred to the SG secondary side can be removed by the water tank of the ASP [SPHRS] and finally discharged to the atmosphere by evaporating water in the tank.

During normal operation of the plant, the ASP [SPHRS] is in the standby state, and the valves located on the steam inlet pipe and feed pipes are in the closed state. When the ASP [SPHRS] is in the operational state, these valves in the ASP [SPHRS] are in the open state.

The main material of the ASP [SPHRS] is stainless steel.

The simplified flow diagram of the ASP [SPHRS] is shown in Figure F-7.9-1.

7.9.4.1.2 Description of Main Equipment

a) Condenser

The ASP [SPHRS] condenser receives the steam from the secondary side of the SG, condenses the steam into water and transfers the heat to the ASP [SPHRS] water tank. The ASP [SPHRS] condenser is submerged during the normal

operation of the power plant. The tube side is filled with demineralised water. The condenser operates for at least 72 hours after an accident, Reference [54].

The condenser is a vertical “C” shaped tube heat exchanger, and is located at the bottom of the water tank. The condenser serves as the key component supporting natural circulation.

The condenser is composed of an upper/lower head, manhole, c-shaped vertical heat transfer tube bundle, upper/lower tube plate, connection flanges and supporting frames, etc.

The condenser is fixed on the water tank wall and floor by a stainless steel support frame. The heat transfer pipe bundle is supported in the water tank as a whole, and the top of the heat transfer pipe is lower than the water surface of the water tank.

The “C” type vertical heat transfer tube bundle consists of 69 austenitic stainless steel heat transfer tubes, the top/bottom heads are semi-spherical with a similar structure, and the condenser also has manholes for inspection and maintenance.

The equipment is made of stainless steel.

T-7.9-1 General Parameters of the ASP [SPHRS] Condenser

Parameters	**Value**		**Unit**
Type	“C” shaped and Tubular		
	Tube Side	Shell Side[1]	
Design Thermal Load	20		MW
Medium	Steam/Condensate Water	Dematerialised Water	
Design Pressure	8.9	0.2	MPa (g)
Design Temperature	303	130	°C
Design Flowrate	77	/	t/h
Material	Stainless Steel		

Note 1: The condenser doesn’t have a real shell. The tubes are submerged in the water tank directly.

b) Water Tank

The water tank is located on the outer wall of the reactor building. The function of the water tank is to receive the heat from the condenser and discharge the heat into atmosphere through evaporation or boiling of the water stored in the tank. The tanks available water capacity is more than 3035t, Reference [54].

T-7.9-2 Main Design Characteristics of the ASP [SPHRS] Water Tank

Parameters	**Value**	**Unit**
Type	Concrete Tank with Steel Liner	
Medium	Dematerialised Water	Additives:H_2O_2 (50±20ppm)
Design Pressure	0.2	MPa (g)
Design Temperature	130	°C
Usable Volume	≥3035	m^3
Max. Volume	~4010	m^3
Material	Concrete Tank with Steel Liner	

7.9.4.1.3 Description of Main Layout

The three trains are located in BSA and BSB (except the water tank which is located outside of the BRX). Equipment on each train is arranged as follows, Reference [55]:

a) The steam inlet valve is arranged in the main steam valve station of the Safeguard Buildings (BSX);

b) The water tank is arranged around the outer wall of the BRX, and the bottom of the tank is higher than the ASG [EFWS] header nozzle on the SG. The condenser is submerged in the cell at the bottom of the tank;

c) The condensate reflux isolation valve is arranged near the containment penetration of the ASG [EFWS] line, and the condensate reflux check valve close to the ASG [EFWS] nozzle of the SG.

The elevation difference between the ASP [SPHRS] condenser and the SG is sufficient to provide the driving head supporting the required natural circulation flow.

As the backup of the ASG [EFWS], the ASP [SPHRS] is physically segregated from the ASG [EFWS]. It is located apart away from the connection to the ASG [EFWS]

feedwater delivery line.

7.9.4.1.4 Description of System Interface

The systems supporting the fulfillment of ASP [SPHRS] functions are as follows, Reference [54]:

a) Main Steam System (VVP [MSS])

The VVP [MSS] transfers steam from the SG to the ASP [SPRHR].

b) ASG [EFWS]

The ASG [EFWS] transfer condensate water from condenser of the ASP [SPRHR] back to the SG.

c) NI Demineralised Water Distribution System (SED [DWDS(NI)])

The SED [DWDS (NI)] fills the water tank and feed pipes in plant normal operation.

d) Station Sewage System (SEO [SSS])

The SEO [SSS] drains the water tank

e) Nitrogen Distribution System (SGN [NDS]

The SGN [NDS] provides nitrogen for ASP [SPHRS] pipes to avoid corrosion when the system is on standby in plant normal operation.

7.9.4.1.5 Description of Instrumentation and Control

a) System Start-up

The system can be started as follows, Reference [56]:

1) Automatically when the water level of three SGs is lower than the set point;

2) Manually for post-accident or test purposes.

b) Controls Available to the Operator

1) Control of the motor valves in the MCR;

2) Control of the Water tank recirculation pump locally;

3) Start-up of the system in the MCR.

7.9.4.2 System Operation

7.9.4.2.1 Plant Normal Operation

During the normal operation of the power plant, the ASP [SPHRS] is in the standby state or in the periodic test condition, Reference [56]:

7.9.4.2.2 Plant Accident Conditions

a) Heat Removal Operation

The ASP [SPHRS] is designed to provide decay heat removal during DEC-A accidents and other accident conditions in which the ASG [EFWS] has failed. The ASP [SPHRS] performs the safety function utilising natural circulation. During DEC-A conditions the ASP [SPHRS] will be started automatically.

The highest operating temperature of the ASP [SPHRS] is { }. The primary temperature during ASP [SPHRS] operation is about{ }. The ASP [SPHRS] can be put out of operation when the ASG [EFWS] or RHR operation mode of the RIS [SIS] is restored.

b) Makeup for the ASG [EFWS] and PTR [FPCTS]

The ASP [SPHRS] can supply water to the ASG [EFWS] in the long term following DEC-A conditions where the ASG [EFWS] and VDA [ASDS] are used for heat removal, Reference [56].

The ASP [SPHRS] ensures cooling of the spent fuel pool by providing make-up water when all trains of the PTR [FPCTS] cooling loop fail. The flowrate of makeup water is more than 50m^3/h (the ASP [SPHRS] make-up water flow to the spent fuel pool is not a continuous, the make-up water flow works operates in either an on or off mode).

7.9.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. Detailed design of the system is presented in Reference [53], [54] [55], [56] and [57]. Furthermore, design substantiation of the ASP [SPHRS] is estimated in the fault study in Chapter 13.

7.9.5.1 Compliance with Safety Requirements

a) Control of reactivity

The ASP [SPHRS] does not contribute to this safety functions.

b) Removal of heat

The fault study in Sub-chapter 13.5 justifies that each safety function required on the ASP [SPHRS] in Sub-chapter 7.9.1.2 is met based on the design assumptions provided in Sub-chapter 7.9.3.2, including the capacity of each train and the volume of the tank.

The total volume of the ASP [SPHRS] water tank is between 3035 to 4010t, which meets the water requirement identified in Section 7.9.3.2.

Each train of condensers can remove at least 20MW of heat, which meets the heat removal requirement identified in Section 7.9.3.2.

c) Confinement of the Radioactive Substance

To ensure the integrity of the secondary system boundary, two valves are provided for the isolation of the Main Steam System (VVP [MSS]).

One isolation valve and one check valve are provided for the isolation of the ASG [EFWS] and Main Feedwater Flow Control System (ARE [MFFCS]).

These valves also contribute to the integrity of the containment.

d) Compliance with Extra Safety Function Requirements

Three water level instruments are used to monitor the water level of the tank.

The ASP [SPHRS] provides make-up water when all trains of the PTR [FPCTS] cooling loop fail. The flowrate of makeup water is more than $50m^3/h$ (the ASP [SPHRS] make-up water flow to the spent fuel pool is not a continuous, the make-up water flow works operates in either an on or off mode).

7.9.5.2 Compliance with Design Requirements

7.9.5.2.1 Compliance with Safety Classification

The ASP [SPHRS] design is compliant with the requirements described in Sub-chapter 4. The safety classification of the ASP [SPHRS] functions are listed in Table T-7.9-3 and the safety classification of main components in Table T-7.9-4.

The documents relevant to the equipment classification will be delivered.

T-7.9-3 System Function Classification

Safety Function	**Function Category**
Residual heat removal under DEC-A accidents	FC3
Water makeup for ASG [EFWS] tank or spent fuel pools in the long term following DEC-A accidents	FC3
Participation in isolating secondary system boundary	FC1
Containment isolation	FC1

T-7.9-4 Classification for Components

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
Steam inlet and feed pipes isolation valves (These valves also contribute to the integrity of the secondary system boundary and containment)	F-SC1	DPM	B-SC2	SSE1
Condensers	F-SC3	NC	NC	SSE1
Water tank	F-SC3	NC	NC	SSE1
Steam inlet and feed pipes	F-SC3	NC	NC	SSE1

7.9.5.2.2 Compliance with Reliability

a) Redundancy and SFC

The ASP [SPHRS] will not perform any function in DBC-2/3/4. According to the general safety principles, single failure considerations are not required to be taken into account in the design of the ASP [SPHRS].

b) Independence

The containment isolation valves, which are classified as FC1, are located in separated rooms and independence is ensured through the layout.

c) Diversity

The ASP [SPHRS] is a diverse backup for the ASG [EFWS] and the residual heat can be removed by either the ASG [EFWS] or ASP [SPHRS] after some accident conditions.

The detailed design result of the ASP [SPHRS] is presented in Reference [53], [54] and [57].

d) Fail-safe Design

There’s no fail-safe designed equipment in the ASP [SPHRS].

e) Ageing and Degradation

The system is designed for the 60 year plant operation. The design life of the condenser in the ASP [SPHRS] is 60 years.

The performance of equipment is guaranteed through life EMIT, as well as the monitoring during normal operation, thus it can be ensured that ageing effects will not compromise the safety performance. The detailed design arrangement around EMIT and equipment monitoring is presented in Reference [56].

The system layout design can ensure the accessibility and requirement for safety equipment in-service inspection and periodic tests including the necessary NDT. This included the requirements of emergency and scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [55].

7.9.5.2.3 Compliance with Human Factors

The system design as well as the control function design of the ASP [SPHRS] does not require short term operator intervention. No operator action within 30 minutes after the initial event is required based on the ASP [SPHRS] design result. The design information is presented in Reference [54] and [56].

It should be noted that there are operator actions during plant normal operation or accident conditions (including plant startup, shutdown, and maintenance or testing etc.). Relevant human actions important to plant safety will be further identified and evaluated in the human factors safety case (which is started from Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of the human factor discipline. Relevant evaluated reports will be provided as references of Chapter 15.

7.9.5.2.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in [1]. The ASP [SPHRS] satisfies the requirements through the following design:

3) The ASP [SPHRS] are started automatically under the accident conditions; no human operation is required from the MCR less than 30 minutes from the first significant signal;

4) All valves performing safety functions are electric valves which can be operated at the MCR; no human operation is required outside the MCR less than 1 hour from the first significant signal.

The design of the ASP [SPHRS] fulfils these principles via the control function design [56]. The design result has been estimated in the safety analysis.

b) Autonomy in Respect to the Heat Sink

The design principles relevant to the autonomy in respect to the heat sink are

listed in Reference [1] . The water tank of the ASP [SPHRS] is made of concrete with a minimum water inventory of 3035t which meets the heat removal requirements for primary circuit, 72 hours after accidents.

c) Autonomy in Respect of Power Supply Systems

The electric valves of the ASP [SPHRS] are powered by Emergency Diesel Generators (EDG) and batteries.

7.9.5.2.5 Compliance with Other design requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

According to Reference [1], the protection of interfacing systems shall be considered in ASP [SPHRS] design. The ASP [SPHRS] takes the following measures to prevent the harmful interactions of systems:

1) Providing adequate isolation (e.g. using double isolating valves) between the ASP [SPHRS] and interfacing systems;

2) The design pressure of the isolation valve between the ASP [SPHRS] and the interface system adopts the larger pressure;

Detailed information is in Reference [56] and [57].

b) Considerations Related to the Electrical Power Grid

The principle is not applicable for ASP [SPHRS] design.

7.9.5.2.6 Compliance with Equipment Qualification

According to Chapter 4, all components required to perform safety functions shall be capable of operating under both normal and accidental conditions, which requires the components to withstand the adverse ambient environments.

The equipment performing an FC1 or FC2 function in the ASP [SPHRS] will be qualified in accordance with the requirements described in Chapter 4.

The equipment performing an FC3 function under DEC-A conditions in the ASP [SPHRS] will also be qualified in accordance with the requirements described in Chapter 4.

The documents relevant to the equipment qualification will be developed during Step 4 of GDA.

7.9.5.2.7 Compliance with Hazard Protection

The ASP [SPHRS] protection against internal and external hazards is in accordance with the principles of Chapter 19 and Chapter 18. The ASP [SPHRS] takes the following measures to prevent the hazards:

a) Internal Hazards

For ASP [SPHRS] equipment performing FC1 functions internal hazards such as fire, internal missiles, line break, internal flooding, internal explosion and the drop of heavy objects shall be taken into account. These parts of the system satisfy the requirements above through the physical separation, physical protections, etc.

The valves of each ASP [SPHRS] in the containment are located in different rooms, The ASP [SPHRS] is primarily protected against internal hazards by the physical separation.

The specific protection design is presented in Reference [55] and the evaluation of the design is presented in Chapter 19.

b) External Hazards

1) Earthquake

As shown in Table T-7.5-18 and [53], the main equipment of the ASP [SPHRS] performing safety functions is SSE1, therefore the equipment can still perform the desired safety functions in the Safe Shutdown Earthquake (SSE) condition.

The documents relevant to the equipment seismic categorisation will be delivered.

2) Other external hazards

The FC1 safety classified parts of the ASP [SPHRS] protect against external disasters mainly through the building design. Specific protection design is presented in Reference [55] and the evaluation of the design is presented in Chapter 18.

7.9.5.2.8 Compliance with Commissioning

The prototype and engineering test of ASP [SPHRS] will be carried out on a dedicated experimental facility before site commissioning. The technical specification of the ASP [SPHRS] heat exchanger will be delivered to present the detailed requirements of the component.

Commissioning is going to be carried out for the ASP [SPHRS] to validate its functionality. The following tests need to be validated:

a) Instrumentation and control channel tests;

b) Valve tests;

c) The pumps and motor tests;

d) The test of water tank.

The detailed description is presented in Reference [56], documents such as System Commissioning Program related to the commissioning are going to be submitted.

7.9.5.2.9 Compliance with Examination, Inspection, Maintenance and Testing

According to Chapter 31, in-service inspection implemented during operation is defined on the basis of RSE-M 2010edition including the 2012 addendum. The valves on the lines connected to the secondary loop of the ASP [SPHRS] are required to be checked during in-service inspection.

The preliminary maintenance plan will be developed after receiving the data/feedback from the equipment suppliers of the ASP [SPHRS].

The ASP [SPHRS] shall have the following periodic tests conducted on it according to its functions:

1) The water tank level instruments require a cross comparison;

2) The start logic of the ASP [SPHRS] need validating, including the correct start sequence and valve opening time;

3) The manual valves filling the ASG [EFWS] and PTR [FPCTS] shall be validated to ensure the open and close function;

The documents relevant to the System Periodic Test Completeness Note will be delivered.

The detailed description around EMIT is presented in Reference [56].

7.9.5.2.10 Special Thermal-Hydraulic Phenomena

The drain line is located between the two steam inlet isolation valves, which are arranged at a certain inclined angle to avoid water seal.

The ASP [SPHRS] reflux line is connected to the pipes from below to reduce convection heat transfer during the standby state, thus the mixing of hot water and cold water can be prevented.

7.9.5.2.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component is presented in Sub-chapter 7.9.4.1.2.

7.9.5.2.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

Insulation of the ASP [SPHRS] is considered for the safety of operators. Accessible

equipment or pipes with high surface temperatures will be insulated to prevent burns.

When the ASP [SPHRS] is operating, the main pipes and valves of the ASP [SPHRS] may be of a temperature higher than 60°C, therefore these pipes and valves are equipped with insulation. The insulation material is glass fiber.

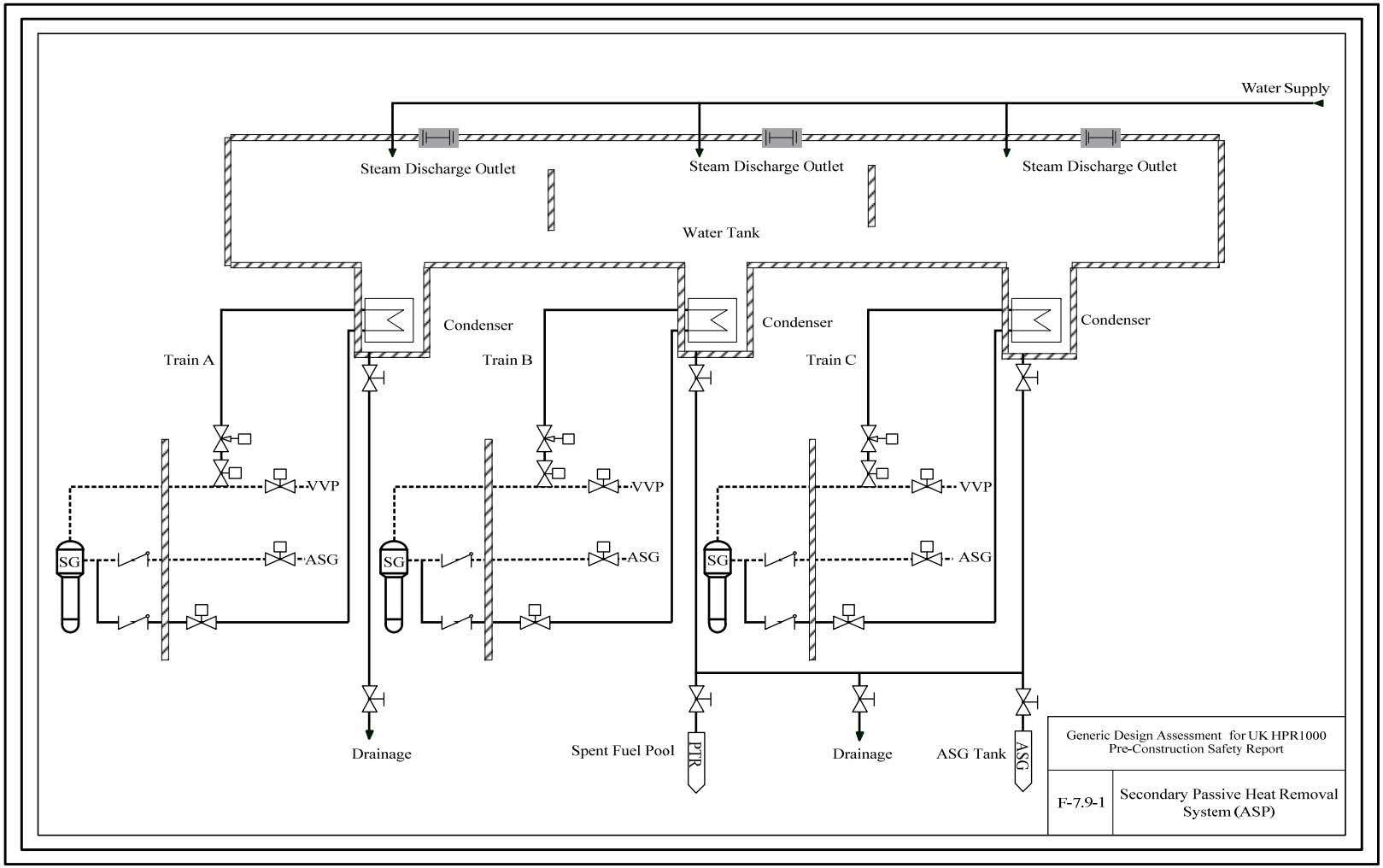
The condenser is located at the bottom of the water tank; there is no need insulation for the condenser.

7.9.5.2.13 Decommissioning

The ASP [SPHRS] is not radioactive, the main consideration of the ASP [SPHRS] for decommissioning is in the layout, i.e. the arrangement of access to components will facilitate maintenance and dismantling.

7.9.6 Functional Diagrams

The simplified functional diagram of the ASP [SPHRS] is in Figure F-7.9-1. The detailed system functional diagrams are presented in Reference [57].



F-7.9-1 Simplified Functional Diagram of the ASP [SPHRS]

7.10 Extra Cooling System (ECS [ECS])

7.10.1 Safety Requirements

The requirements of safety functions on the ECS [ECS] design for the UK HPR1000 are identified below, Reference [58] and [59].

7.10.1.1 Control of Reactivity Requirements

The ECS [ECS] is not required to perform the safety function of reactivity control.

7.10.1.2 Removal of Heat Requirements

The ECS [ECS] removes the core residual heat and the decay heat from the spent fuel pool in DEC-A (such as TLOCC and SBO) and DEC-B.

7.10.1.3 Confinement Requirements

The intermediate circuit of the ECS [ECS] forms a barrier between the users (the users are the EHR [CHRS] and PTR [FPCTS] heat exchangers) and the environment to ensure that radioactive material is not released.

7.10.1.4 Extra Safety Function Requirement

During the Reactor Complete Discharge (RCD) condition, one train of the ECS [ECS] is the backup of the RRI [CCWS] for cooling the PTR [FPCTS].

7.10.2 Design Requirements

The general design requirements of the safety systems which need to be considered are shown in Sub-chapter 7.2.4, and the following requirements are not applicable to the ECS [ECS]:

a) Redundancy and SFC: The ECS [ECS] performs an FC3 function and does not need to meet the SFC.

b) Fail-safe: There is no fail-safe requirement on the ECS [ECS].

c) Special Thermal-Hydraulic Phenomena: There is no special thermal-hydraulic phenomenon in the ECS [ECS]

The substantiation analysis of the ECS [ECS] to other design requirements is shown in Sub-chapter 7.10.5.

7.10.3 Design Bases

This sub-chapter aims to provide the main design assumptions considered in the system design, Reference [59].

7.10.3.1 General Assumption

a) Safety Classification

The ECS [ECS] is used in DEC accident conditions, therefore the classification of the system is FC3.

b) Ageing and Degradation

During system and equipment design, the ageing and degradation of the equipment which is important to safety shall be taken into account.

The design life of the main equipment of the ECS [ECS] is 60 years. In addition, some parts of the main equipment may need to be replaced regularly during the design life.

c) Autonomy

The water inventory of the makeup pool allows the ECS [ECS] to maintain operating for a duration of 24h.

d) Equipment Qualification

The components of the ECS [ECS] performing safety functions shall be qualified.

Equipment qualification includes environmental and seismic qualification.

e) Considerations Related to the Electrical Power Grid

The fluctuation of electrical power grid may affect the ability of safety functions, especially the performance of the active equipment, such as the pumps in the ECS [ECS].

f) Protection against Internal and External Hazards

The effect of internal and external hazards shall be considered in ECS [ECS] equipment design.

These hazards may induce an environmental condition change in the compartment where the equipment is located. Moreover, safety functions shall be performed under earthquake events. Therefore, the equipment design shall take the effects of hazards into account to ensure the ability of the safety function.

7.10.3.2 Design Assumptions

a) Control of reactivity

The ECS [ECS] does not perform the safety function of reactivity control.

b) Removal of heat

The ECS [ECS] removes the core residual heat and decay heat from the spent fuel pool in DEC-A (such as TLOCC, SBO) and DEC-B. One ECS [ECS] train can cool the Containment Heat Removal System (EHR [CHRS]) and Fuel Pool Cooling and Treatment System (PTR [FPCTS]) at the same time. The ECS [ECS]

related requirements are as follows:

1) Minimum flow

The ECS [ECS] design must meet the flow requirements outlined below:

- Flow rate of terminal circulation is{ };
- Flow rate to the EHR [CHRS] is { };
- Flow rate to the PTR [FPCTS] is { }.

2) Maximum temperature

The maximum water temperature at the ECS [ECS] intermediate circulation cooling water inlet for users is { }.

3) Head load requirements

In the case of loss of RRI [CCWS], the ECS [ECS] removes the heat of the core and the spent fuel pool through the EHR [CHRS] and PTR [FPCTS] heat exchanger. The total heat load need required to be removed is about { }.

4) Makeup pool capacity

The capacity of the makeup pool will supply the water required by one train of the ECS [ECS] continually for 24h. After 24h, it extracts the water from other sources to replenish the collecting tank via auxiliary equipment (such as the temporary mobile pumps).

c) Confinement

The intermediate circuit of the ECS [ECS] forms a barrier between the users and the environment, to ensure that radioactive material is not released. The operating pressure of the ECS [ECS] is higher than the users.

The ECS [ECS] is isolated in standby instead of being put into operation in normal operation of the power plant. It is assessed in periodic tests to confirm that it is capable of executing its safety function.

To ensure the availability of the intermediate circuit, the ECS [ECS] intermediate surge tank is automatically refilled by controlling its water level. Compressed air can also be refilled in the ECS [ECS] intermediate surge tank manually (the air refilling is performed by a mobile compressed air bottle).

The intermediate fluid is conditioned with the chemical additive TSP supplied by the NI Chemical Reagents Distribution System (SIH [CDS]) to minimise corrosion.

d) Extra Safety Function Assumptions

During RCD condition, one train of the ECS [ECS] is the backup of the RRI [CCWS] for cooling thePTR [FPCTS]. The heat load that the ECS [ECS] needs remove is about { }.

7.10.4 System Description and Operation

7.10.4.1 System Description

7.10.4.1.1 General System Description

The ECS [ECS] consists of two identical trains, and each of them includes:

a) ECS [ECS] terminal cooling circuit: consisting of a terminal circulation pump, a terminal filter, an intermediate heat exchanger (cold side), a suite of mechanical draught cooling towers, a makeup pool, relevant pipes, valves and pipe fittings, Reference [60].

b) ECS [ECS] intermediate cooling circuit: consisting of an intermediate circulation pump, an intermediate surge tank, an intermediate heat exchanger (hot side), relevant pipes, valves and pipe fittings, Reference [60].

The simplified flow diagram of the ECS [ECS] is shown in Figure F-7.10-1.

The main material of the pipes in the ECS [ECS] terminal cooling circuit is seawater corrosion resisting stainless steel, and carbon steel for those in the intermediate cooling circuit.

7.10.4.1.2 Main Components and Characteristics

The main components of the ECS [ECS] include the intermediate circulation pumps, intermediate heat exchangers, intermediate surge tanks, terminal circulation pumps, terminal filters, and mechanical draught cooling towers, Reference [60].

a) Intermediate Circulation Pumps

T-7.10-1 Main Design Characteristics of the Intermediate Circulation Pumps

Parameters	**Value**	**Unit**
Type	Single-Stage Centrifugal Pump	
Design Life	60	yr.
Nominal Flowrate	820	m^3/h
Discharge Head at Nominal Flowrate	32	mWc

Parameters	**Value**	**Unit**
Material	Carbon Steel	

b) Intermediate Circuit Heat Exchangers

T-7.10-2 Main Design Characteristics of the Intermediate Heat Exchangers

Parameters	**Value**		**Unit**
Type	Plate		
	Hot Side	Cold Side	
Design Thermal Load	15.1		MW
Medium	Dematerialised Water +Na3PO4	Fresh Water/Seawater	
Design Pressure	2.9	0.7	MPa (g)
Design Temperature	85	65	°C
Design Flow rate	780	900	m3/h
Material	Titanium Plate	Titanium Plate	

c) Intermediate Surge Tanks

T-7.10-3 Main Design Characteristics of the Intermediate Surge Tanks

Parameters	**Value**	**Unit**
Type	Cylindrical Tank	
Medium	Liquid Phase: Dematerialised Water +Na_3PO_4 Gaseous Phase: Air	
Design Pressure	3.0	MPa (g)
Design Temperature	65	°C

Parameters	**Value**	**Unit**
Usable Volume	11.1	m^3
Max. Volume	11.4	m^3
Material	Carbon Steel	

d) Terminal Circulation Pumps

T-7.10-4 Main Design Characteristics of the Terminal Circulation Pumps

Parameters	**Value**	**Unit**
Type	Single-Stage Centrifugal Pump	
Design Life	60	yr.
Nominal Flowrate	950	m^3/h
Discharge Head at Nominal Flowrate	34	mWc
Material	Stainless Steel	

e) Terminal Filters

T-7.10-5 Main Design Characteristics of the Terminal Circuit Filters

Parameters	**Value**	**Unit**
Design Pressure	0.7	MPa (g)
Design Temperature	65	°C
Design Maximum Flow	950	m^3/h
Filtration Efficiency	100	%
Filtration Fineness	2000	μm
Material	Neoprene Lining of Carbon Steel	

f) Mechanical Draft Cooling Tower

The heat load of the cooling towers is designed to remove as much heat as possible for the users. The water in the makeup pool meets the requirements for 24 hours of usage. It will extract the water from other sources (including seawater) to replenish the collecting tank via temporary makeup equipment after 24 hours.

During plant normal operation, the ECS [ECS] is on standby. The terminal circuit is filled with potable water from the Potable Water System (SEP [PWS (NI)]). In order to prevent the growth of microorganisms of the makeup pool and collecting tank, operators should monitor water quality each month (water quality standard: total number of bacteria≤1000/ml , turbidity≤5 NTU), operators drain water and replenishes water by the SEP [PWS (NI)] when the water quality does not meet the required standard.

7.10.4.1.3 Description of Main Layout

The pumps, heat exchangers, surge tanks and filters in trains A and B of the ECS [ECS] are located in two separated rooms of Extra Cooling System and Fire-fighting System Building (BEJ), Reference [61]. The makeup pool of the mechanical draught cooling towers is also in the BEJ; the space is big enough for inspection and maintenance of the equipment.

The intermediate circuit pipelines pass through the Fuel Building (BFX) and convey the cooling water to the EHR [CHRS] user heat exchanger in Safeguard Buildings A (BSA) and Safeguard Buildings B (BSB) and the PTR [FPCTS] user heat exchangers in BFX.

7.10.4.1.4 Description of System Interface

The systems supporting the fulfilment of ECS [ECS] functions are as follows, Reference [60]:

a) NI Dematerialised Water Distribution System (SED [DWDS (NI)])

   When the system is put on standby or refilled after exhaustion, the SED [DWDS (NI)] will fill the intermediate circuit of the ECS [ECS] to protect the system and make sure that the system can be started at any time.

b) Extra Cooling Water and NI Firefighting Building Ventilation System (DXE [ECW&FFB VS])

   The temperature of the BEJ of ECS [ECS] is controlled by the DXE [ECW&FFB VS], and it accepts the air discharged from safety valves.

c) SEP [PWS (NI)])

   The SEP [PWS (NI)] provides makeup water for the makeup pool of the ECS [ECS] mechanical draught cooling towers.

d) SIH [CDS]

The ECS [ECS] maintains the chemical properties of the fluid through the SIH [CDS].

7.10.4.1.5 Description of Instrumentation and Control

In DEC-A (such as TLOCC, SBO) and DEC-B, the ECS [ECS] will be started manually by operators. During system standby or operation, the following parameters shall be measured.

a) Flowrate measurement

The flowrate of the terminal cooling circuit and intermediate cooling circuit requires monitoring and alarming to ensure that it meets the requirement.

b) Temperature measurement

The inlet and outlet temperature of the intermediate heat exchanger at the cold and hot side needs monitoring and alarming.

c) Pressure measurement

The pressure of intermediate surge tank requires monitoring and alarming to maintain a normal pressure fluctuation range.

Once the inlet or outlet pressure of the terminal circulation pump is low, the pump will stop automatically.

d) Water level measurement

The water level of intermediate surge tank and makeup pool require monitoring and alarming to maintain a normal water level fluctuation range.

7.10.4.2 System Operation

7.10.4.2.1 Plant Normal Operation

The ECS [ECS] is on standby in normal operation of the power plant. The whole circuit is filled with water from the SEP [PWS (NI)] and SED [DWDS (NI)]. The liquid level in the makeup pool of the mechanical draught cooling towers shall be kept above the safe level, and the water shall be maintained clean, Reference [62].

7.10.4.2.2 Plant Accident Conditions

The ECS [ECS] is on standby in DBC-2/3/4 and DEC-A when the normal cold chains of the Component Cooling Water System (RRI [CCWS]) and Essential Service Water System (SEC [ESWS]) do not fail.

In DEC-A (such as TLOCC, SBO) and DEC-B, the ECS [ECS] can be put into operation manually by operators through starting up the terminal cooling circuit and the intermediate cooling circuit in turn.

7.10.5 Preliminary Design Substantiation

The system design is based on the design of the HPR1000 (FCG3). A review of the consistency of the system design against the design principles is currently being undertaken. Detailed design of the system is presented in Reference [59] [60] [61] [62] and [63]. Furthermore, design substantiation of the ECS [ECS] is estimated in the fault study in Chapter 13.

7.10.5.1 Compliance with Safety Requirements

a) Control of reactivity

The ECS [ECS] does not contribute to the safety function of reactivity control.

b) Removal of heat

The ECS [ECS] consists of two trains. The two trains are put into operation manually and each of them can cool the EHR [CHRS] and PTR [FPCTS] at the same time.

The fault study in Sub-chapter 13.5 justifies that each safety function required on the ECS [ECS] in Sub-chapter 7.10.1.2 is met based on the design assumptions provided in Sub-chapter 7.10.3.2.

The parameter requirements of the ECS [ECS] main equipment (including terminal circulation pump, intermediate circulation pump, heat exchanger and cooling tower) are shown in Reference [60]. These parameter requirements are presented in the equipment technical specifications and the equipment supplier shall meet the requirements according to the specifications.

The ECS [ECS] removes the heat of the core and spent fuel pool through the EHR [CHRS] and PTR [FPCTS] heat exchanger. Each ECS [ECS] train can remove 15.1MW, which meets the requirements of Sub-chapter 7.10.3.2.

c) Confinement

The intermediate circuit of the ECS [ECS] forms a barrier between the heat exchangers and the environment to ensure that radioactive substances are not released, which means the pressure of the ECS [ECS] intermediate cooling circuit is required to be higher than the EHR [CHRS] and PTR [FPCTS]. The operating pressure of the ECS [ECS] and users are listed as follows:

1) PTR [FPCTS] maximum operating pressure is about 0.6MPa abs, EHR [CHRS] heat exchanger maximum operating pressure is 2.1MPa abs, and EHR [CHRS] heat exchanger cold side (ECS [ECS]) minimum operating pressure is 2.2 MPa abs.

According to the above analysis, the operating pressure of the ECS [ECS] is higher than the users.

d) Compliance with Extra Safety Function Requirements

During RCD condition, one train of the ECS [ECS] is the backup of the RRI [CCWS] for cooling the PTR [FPCTS]. The design heat load of the ECS [ECS] is 15.1MW, which is higher than the requirement of { }.

7.10.5.2 Compliance with Design Requirements

7.10.5.2.1 Compliance with Safety Classification

The ECS [ECS] design is compliant with the requirements described in Chapter 4. The safety classification of ECS [ECS] functions is listed in Table T-7.10-6, and the safety classification of main components in Table T-7.10-7.

The ECS [ECS] is designed to withstand the SSE. The main components are classified as SSE1 as shown in Table T-7.10-7.

The documents relevant to the equipment classification will be delivered.

T-7.10-6 System Function Classification

System Function	**Function Category**
Cool the PTR [FPCTS]	FC3
Cool the EHR [CHRS]	FC3
Make up of intermediate surge tank	NC
Refilling of compressed air into the ECS [ECS] intermediate surge tank	NC

T-7.10-7 Classification for Components

Component	**Function Class**	**Design Provision Category**	**Design Provision Class**	**Seismic Category**
Intermediate Circulation Pumps	F-SC3	NC	NC	SSE1
Intermediate Heat Exchangers	F-SC3	NC	NC	SSE1
Intermediate Surge Tanks	F-SC3	NC	NC	SSE1
Terminal Circulation	F-SC3	NC	NC	SSE1

Component	Function Class	Design Provision Category	Design Provision Class	Seismic Category
Pumps				
Terminal Filters	F-SC3	NC	NC	SSE1
Mechanical Draught Cooling Towers	F-SC3	NC	NC	SSE1
Makeup pools	F-SC3	NC	NC	SSE1

7.10.5.2.2 Compliance with Reliability

a) Redundancy and SFC

There is no redundancy and SFC requirement for the ECS [ECS] according to the principles in Chapter 4. But the ECS [ECS] is designed to have two trains to improve its reliability, considering the possible failure of active sensitive equipment in long term operation.

The detailed design result of the ECS [ECS] is presented in Reference [59], [60], [61] and [62].

b) Independence

The principle of independence is presented in Sub-chapter 7.2.4.

The ECS [ECS] consists of two independent trains, and trains A and B are located in separate rooms of the BEJ respectively.

c) Diversity

The principle of diversity is presented in Sub-chapter 7.2.4.

The diversity design in the ECS [ECS] contains:

1) The SEP [PWS (NI)] provides makeup water for the makeup pool of the ECS [ECS] mechanical draught cooling towers. The ECS [ECS] terminal circuit may be filled with other temporary water sources when the SEP [PWS (NI)] fails;

2) Each ECS [ECS] train is supplied with an electrical division and backed-up by the EDGs. Furthermore, the ECS [ECS] trains A and B can be powered by the SBO diesel generators or by mobile power supplies;

3) The EHR [CHRS] and PTR [FPCTS] are normally supported by the RRI [CCWS]. The ECS [ECS] provides a diverse heat sink to remove the core

residual heat and the decay heat from the spent fuel pool to the atmosphere.

The detailed design result of the ECS [ECS] is presented in Reference [59] and [60].

d) Fail-safe Design

There's no fail-safe designed equipment in the ECS [ECS].

e) Ageing and Degradation

The system is designed for the 60 year plant operation. The design life of the main equipment of the ECS [ECS] is 60 years, which mainly includes the:

1) Intermediate Circulation Pumps;

2) Intermediate Circuit Heat Exchangers;

3) Terminal Circulation Pumps.

4) Terminal Filters

The performance of equipment is guaranteed through life EMIT, as well as monitoring during normal operation, which will ensure that ageing effects do not compromise safety performance. Detailed design arrangement around EMIT and equipment monitoring is presented in Reference [62].

The system layout design can ensure the accessibility and requirements for safety equipment periodic tests including the requirements of emergency and scheduled maintenance on the SSCs. Detailed layout information is presented in Reference [61] .

7.10.5.2.3 Compliance with Human Factors

ECS [ECS] is in a standby state under normal plant operation conditions, while it provides cooling water to the heat exchangers of the EHR [CHRS] and PTR [FPCTS] under DEC conditions. The ECS [ECS] is started manually by the operator after the accident. No operator action within 30 minutes after the initial event is required based on the ECS [ECS] design result. The design information is presented in Reference [59] and [62].

Relevant human actions important to plant safety will be further identified and evaluated in the human factors safety case (which is started in Chapter 15). The systematic method is summarised in Chapter 15 and detailed in the references of the human factor discipline. Relevant evaluated reports will be provided as references of Chapter 15.

7.10.5.2.4 Compliance with Autonomy

a) Autonomy in Respect to Operators

The design principles relevant to the autonomy in respect to operators are listed in Reference [1]. The ECS [ECS] is started manually by the operator after the accident. No human operation is required from the MCR less than 30 minutes and no human operation is required outside the MCR less than 1 hour from the first significant signal. The detailed description is presented in Reference [62].

b) Autonomy in Respect to the Heat Sink

The design principles relevant to the autonomy in respect to the heat sink are listed in Reference [1]. The capacity of one makeup pool can supply the water required by one train of the ECS [ECS] continually for 24 hours. After 24 hours, it extracts water from other sources to replenish the makeup pool via auxiliary equipment (such as temporary mobile pumps).

The detailed description is presented in Reference [59].

c) Autonomy in Respect to Power Supply Systems

Trains A and B of the ECS [ECS] are powered by trains A and B of the power supply unit respectively, and by EDGs and SBO diesel generators as well to ensure that ECS [ECS] is able to perform its safety functions in SBO conditions.

The ECS [ECS] is also supplied by mobile diesel generators to ensure the safety function under extreme accidents such as Fukushima.

7.10.5.2.5 Compliance with Other design requirements

a) Prevention of Harmful Interactions of Systems Important to Safety

According to Reference [1], the protection of interfacing systems shall be considered in the ECS [ECS] design. The pressure of the intermediate circuit of the ECS [ECS] is higher than the EHR [CHRS] and PTR [FPCTS], which can ensure that radioactive substances are not released from the ECS [ECS]. Detailed information is given in [62] and [63].

b) Considerations Related to the Electrical Power Grid

According to Reference [1], the functionality of items important to safety at the nuclear power plant shall not be compromised by disturbances in the electrical power grid.

The fluctuation of the electrical power grid mainly affects the functional capability of the ECS [ECS] pumps. The pump flow will change with the fluctuation of the power grid. In the HPR1000 (FCG3) project，the design of the intermediate circulation pumps and terminal circulation pumps considers the influence of grid fluctuation. Based on the UK context, relevant to the electrical power grid, re-estimates will be carried out during GDA progress.

7.10.5.2.6 Compliance with Equipment Qualification

According to Chapter 4, all components required to perform safety functions shall be capable of operating under both normal and accidental conditions. Thus the components shall withstand the adverse ambient environments.

The equipment performing an FC3 function under DEC conditions in the ECS [ECS] will also be qualified in accordance with the requirements described in Chapter 4.

The documents relevant to the equipment qualification will be developed during Step 4 of GDA.

7.10.5.2.7 Compliance with Hazard Protection

The ECS [ECS] protection against internal and external hazards is in accordance with the principles of Chapter 19 and Chapter 18. The ECS [ECS] system takes the following measures to prevent the hazards:

a) Internal Hazards

The protection against internal hazards mainly depends upon the buildings, rooms, fire compartments and anti-flooding compartments arranged for the ECS [ECS]. The specific measures are as follows:

1) The two trains of ECS [ECS] shall be arranged in different rooms for physical separation to ensure that only one train fails following an internal hazard.

The specific protection design is presented in Reference [61]. The evaluation of the design is presented in Chapter 19.

b) External Hazards

1) Earthquake

As shown in Table T-7.10-7 and Reference [59], the main equipment of the ECS [ECS] performing safety functions is SSE1; the equipment can still perform the desired safety functions in the Safe Shutdown Earthquake (SSE) condition.

The documents relevant to the equipment seismic categorisation will be delivered.

2) Other external hazards

The ECS [ECS] protects against external hazards mainly through the building design. The specific protection design is presented in Reference [61]. The evaluation of the design is presented in Chapter 18.

7.10.5.2.8 Compliance with Commissioning

Initial testing (e.g. factory acceptance tests) of components before delivery to site shall be undertaken to ensure that the safety functions of these components can be properly performed. The design requirements will be provided to the equipment vendor in the form of technical specifications.

Commissioning is going to be carried out for the ECS [ECS] to validate its functionality. The main commissioning tests of ECS [ECS] include:

a) System tests

   1) System flushing

   2) Functional test of system operation.

   3) Terminal circuit filling tests;

b) Pump tests

   1) Intermediate circulation pump tests;

   2) Terminal circulation pump tests;

c) Other equipment tests

   1) Intermediate surge tank tests;

   2) Terminal filter tests;

   3) Cooling tower fan tests;

   4) Valve tests

The detailed description is presented in Reference [62]. Documents such as the System Commissioning Program related to the commissioning are going to be submitted.

7.10.5.2.9 Compliance with Examination, Inspection, Maintenance and Testing

There is no in-service inspection requirement for the ECS [ECS].

During normal operation, maintenance and replacement of the main equipment of the ECS [ECS] can be performed.

Equipment of the ECS [ECS] performing safety functions shall be subject to periodic test, mainly including pump and fan performance. The periodic test of the ECS [ECS] will be performed during normal operation of the unit, and the test mainly includes:

a) Start-up of the intermediate circuit;

b) Measurement of the intermediate circuit flow;

c) Start-up of the terminal circuit;

d) Measurement of the terminal circuit flow.

The documents relevant to the System Periodic Test Completeness Note will be delivered.

The detailed description around EMIT is presented in Reference [62].

7.10.5.2.10 Special Thermal-Hydraulic Phenomena

No special thermal-hydraulic phenomenon needs to be considered in the ECS [ECS].

7.10.5.2.11 Compliance with Material Selection

Based on the principles of material selection stated in Sub-chapter 7.2.4, and engineering experience, the material selected for the main component is presented in Sub-chapter 7.10.4.1.2.

7.10.5.2.12 Compliance with Insulation Design

The principles of insulation design are stated in Sub-chapter 7.2.4.

Insulation of the ECS [ECS] is considered for the safety of operators. Accessible equipment or pipes with high surface temperatures will be insulated to prevent burns.

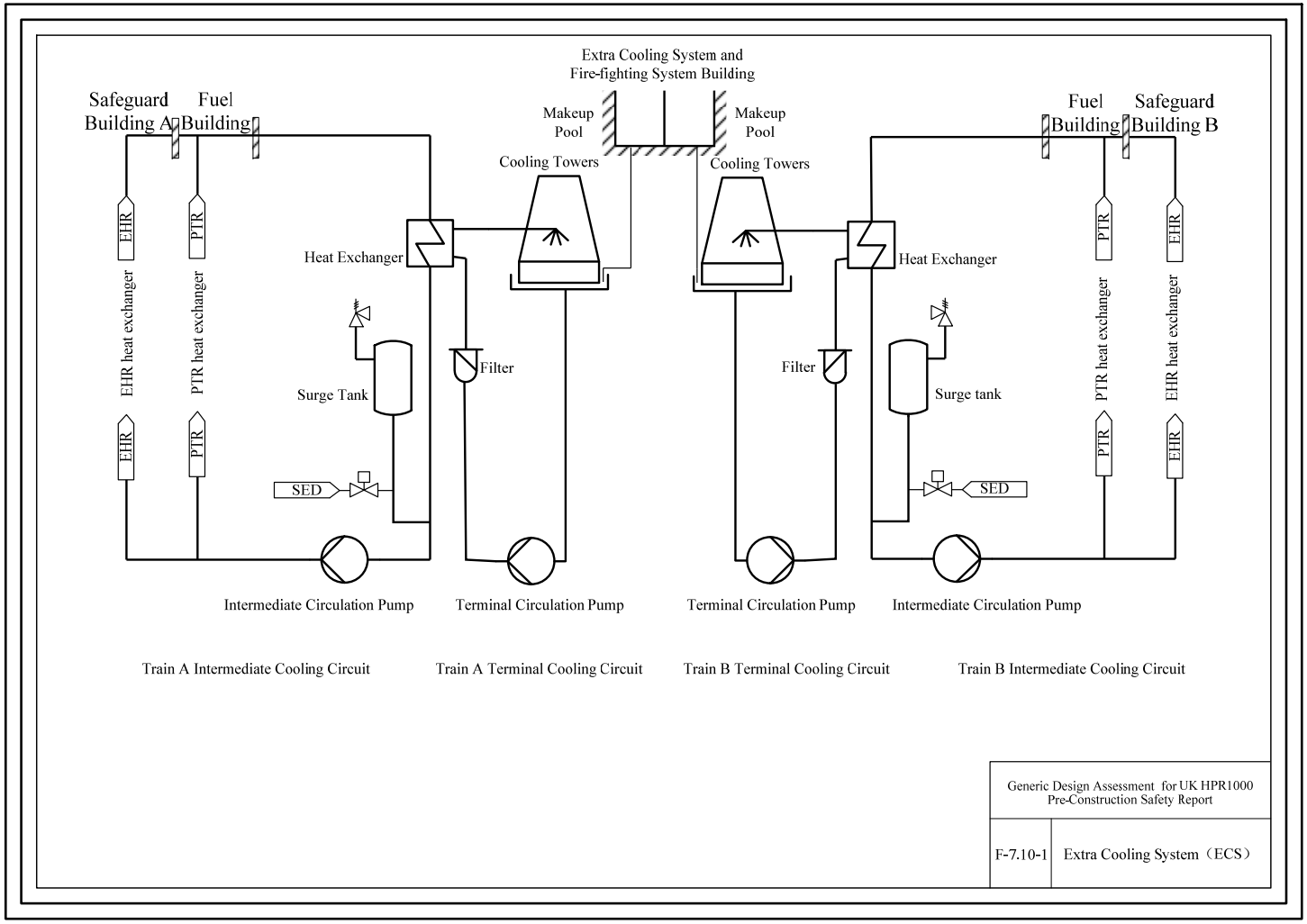
The temperature of the relevant pipes from the user heat exchangers to the ECS [ECS] intermediate heat exchangers may be higher than 60°C, therefore these pipes are equipped with insulation. The insulation material is glass fiber.

7.10.5.2.13 Decommissioning

The ECS [ECS] is not radioactive, the main consideration of the ECS [ECS] for decommissioning is in the layout, i.e. the arrangement of access to components will facilitate maintenance and dismantling.

7.10.6 Functional Diagrams

The simplified functional diagram of the ECS [ECS] is shown in Figure F-7.10-1. The detailed system functional diagrams are presented in Reference [63].



F-7.10-1 Simplified Functional Diagram of the ECS [ECS]

7.11 ALARP Assessment

The main applicable codes and standards for safety system and component design are presented in Table T-7.3-1. The detailed codes and standards list is presented in Reference [6]. The consistency analyses between the current design and the RGP is still under development. However, based on current analysis results, no significant gap has been identified at the system level. The preliminary ALARP demonstration based on the current design is presented in Reference [64]; the consistency analysis will continue to ensure that the design of the safety systems meets the requirements of the UK context.

In addition, a review of consistency of the system design against the UK HPR1000 principles is being undertaken.

Furthermore, the cross-cutting assessments, such as hazard analysis, fault schedule, probabilistic safety assessment and human factors are still under development at this stage. If these assessments highlight opportunities to enhance the design of safety systems, the potential enhancements will be taken through the optioneering process.

In summary, the review is still in progress. If any potential enhancements are identified, analysis and optioneering will be performed to determine whether enhancements to the design are practicable.

7.12 Concluding Remarks

The safety systems in the UK HPR1000 consist of containment and related safety systems, engineered safety systems, DEC-A and DEC-B mitigation systems. This chapter provides an introduction of the design and operation of safety systems provided in the UK HPR1000 nuclear power plant. The information includes system design requirements, design basis, system description and operation, design substantiation, etc. This information helps regulators understand the design of the UK HPR1000 safety systems.

Currently, no gap has been identified at the system level, but the gap analysis work is continuing. If any new gap is identified, the ALARP analysis will be performed to optimise the related design.

According to the arrangement of the mechanical engineering area, the reference documents of the safety system are still in progress, which will provide support for PCSR Chapter 7.

7.13 References

[1] CGN, General Safety Requirements, GHX00100017DOZJ03GN, Revision C, 2018.

[2] CGN, Material Selection Methodology, GHX00100006DPCH03GN, Revision

B, 2018.

[3] CGN, Methodology of Safety Categorisation and Classification, GHX00100062DOZJ03GN, Revision B, 2018.

[4] CGN, The General Requirements of Protection Design against Internal and External Hazards, GHX00100028DOZJ03GN, Revision C, 2018.

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

[6] CGN, Applicable Code and Standards in Context of Mechanical Engineering, GHX00800001DNHX02GN, Revision A, 2018.

[7] CGN, EHR-Containment Heat Removal System Design Manual Chapter 2 Brief Introduction to the System, GHX17EHR002DNHX45GN, Revision A, 2018.

[8] CGN, EHR-Containment Heat Removal System Design Manual Chapter 3 System Functions and Design Bases, GHX17EHR003DNHX45GN, Revision A, 2018.

[9] CGN, EHR-Containment Heat Removal System Design Manual Chapter 4 System and Component Design, GHX17EHR004DNHX45GN, Revision A, June 2018.

[10] CGN, EHR-Containment Heat Removal System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17EHR005DNHX45GN, Revision A, 2018.

[11] CGN, EHR-Containment Heat Removal System Design Manual Chapter 6 System Operation and Maintenance, GHX17EHR006DNHX45GN, Revision B, June 2018.

[12] CGN, EHR-Containment Heat Removal System Design Manual Chapter 9 Flow Diagrams, GHX17EHR009DNHX45GN, Revision B, June 2018.

[13] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 2 Brief Introduction to the System, GHX17EUF002DNHX45GN, Revision B, 2018.

[14] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 3 System Functions and Design Bases, GHX17EUF003DNHX45GN, Revision A, 2018.

[15] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 4 System and Component Design, GHX17EUF004DNHX45GN, Revision B, June 2018.

[16] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17EUF005DNHX45GN, Revision A, 2018.

[17] CGN, EUF-Containment Filtration and Exhaust System Design Manual Chapter 6 System Operation and Maintenance, GHX17EUF006DNHX45GN, Revision B, June 2018.

[18] CGN, EUH-Containment Combustible Gas Control System Design Manual Chapter 2 Brief Introduction to the System, GHX17EUH002DNHX45GN, Revision A, 2018.

[19] CGN, EUH-Containment Combustible Gas Control System Design Manual Chapter 3 System Functions and Design Bases, GHX17EUH003DNHX45GN, Revision A, 2018.

[20] CGN, EUH-Containment Combustible Gas Control System Design Manual Chapter 4 System and Component Design, GHX17EUH004DNHX45GN, Revision A, June 2018.

[21] CGN, EUH-Containment Combustible Gas Control System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17EUH005DNHX45GN, Revision A, 2018.

[22] CGN, EUH-Containment Combustible Gas Control System Design Manual Chapter 6 System Operation and Maintenance, GHX17EUH006DNHX45GN, Revision A, June 2018.

[23] CGN, EPP-Containment Leak Rate Testing and Monitoring System Design Manual Chapter 2 Brief Introduction to the System, GHX17EPP002DNHX45GN, Revision A, 2018.

[24] CGN, EPP-Containment Leak Rate Testing and Monitoring System Design Manual Chapter 3 System Functions and Design Bases, GHX17EPP003DNHX45GN, Revision A, 2018.

[25] CGN, EPP-Containment Leak Rate Testing and Monitoring System Design Manual Chapter 4 System and Component Design, GHX17EPP004DNHX45GN, Revision A, June 2018.

[26] CGN, EPP-Containment Leak Rate Testing and Monitoring System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17EPP005DNHX45GN, Revision A, 2018.

[27] CGN, EPP-Containment Leak Rate Testing and Monitoring System Design Manual Chapter 6 System Operation and Maintenance, GHX17EPP006DNHX45GN, Revision B, June 2018.

[28] CGN, RIS-Safety Injection System Design Manual Chapter 2 Brief Introduction to the System, GHX17RIS002DNHX45GN, Revision A, 2018.

[29] CGN, RIS-Safety Injection System Design Manual Chapter 3 System Functions and Design Bases, GHX17RIS003DNHX45GN, Revision B, 2018.

[30] CGN, RIS-Safety Injection System Design Manual Chapter 4 System and Component Design, GHX17RIS004DNHX45GN, Revision A, June 2018.

[31] CGN, RIS-Safety Injection System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17RIS005DNHX45GN, Revision A, 2018.

[32] CGN, RIS-Safety Injection System Design Manual Chapter 6 System Operation and Maintenance, GHX17RIS006DNHX45GN, Revision B, June 2018.

[33] CGN, RIS-Safety Injection System Design Manual Chapter 9 Flow Diagrams, GHX17RIS009DNHX45GN, Revision B, June 2018.

[34] CGN, RBS-Emergency Boration System Design Manual Chapter 2 Brief Introduction to the System, GHX17RBS002DNHX45GN, Revision A, 2018.

[35] CGN, RBS-Emergency Boration System Design Manual Chapter 3 System Functions and Design Bases, GHX17RBS003DNHX45GN, Revision A, 2018.

[36] CGN, RBS-Emergency Boration System Design Manual Chapter 4 System and Component Design, GHX17RBS004DNHX45GN, Revision A, June 2018.

[37] CGN, RBS-Emergency Boration System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17RBS005DNHX45GN, Revision A, 2018.

[38] CGN, RBS-Emergency Boration System Design Manual Chapter 6 System Operation and Maintenance, GHX17RBS006DNHX45GN, Revision B, June 2018.

[39] CGN, RBS-Emergency Boration System Design Manual Chapter 9 Flow Diagrams, GHX17RBS009DNHX45GN, Revision B, June 2018.

[40] CGN, VDA-Atmospheric Steam Dump System Design Manual Chapter 2 Brief Introduction to the System, GHX17VDA002DNHX45GN, Revision A, 2018.

[41] CGN, VDA-Atmospheric Steam Dump System Design Manual Chapter 3 System Functions and Design Bases, GHX17VDA003DNHX45GN, Revision A, 2018.

[42] CGN, VDA-Atmospheric Steam Dump System Design Manual Chapter 4 System and Component Design, GHX17VDA004DNHX45GN, Revision A, June 2018.

[43] CGN, VDA-Atmospheric Steam Dump System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17VDA005DNHX45GN, Revision B, 2018.

[44] CGN, VDA-Atmospheric Steam Dump System Design Manual Chapter 6 System Operation and Maintenance, GHX17VDA006DNHX45GN, Revision B, June 2018.

[45] CGN, VDA-Atmospheric Steam Dump System Design Manual Chapter 9 Flow Diagrams, GHX17VDA009DNHX45GN, Revision B, June 2018.

[46] CGN, ASG-Emergency Feedwater System Design Manual Chapter 2 Brief Introduction to the System, GHX17ASG002DNHX45GN, Revision A, 2018.

[47] CGN, ASG-Emergency Feedwater System Design Manual Chapter 3 System Functions and Design Bases, GHX17ASG003DNHX45GN, Revision A, 2018.

[48] CGN, ASG-Emergency Feedwater System Design Manual Chapter 4 System and Component Design, GHX17ASG004DNHX45GN, Revision A, June 2018.

[49] CGN, ASG-Emergency Feedwater System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17ASG005DNHX45GN, Revision B, 2018.

[50] CGN, ASG-Emergency Feedwater System Design Manual Chapter 6 System Operation and Maintenance, GHX17ASG006DNHX45GN, Revision B, June 2018.

[51] CGN, ASG-Emergency Feedwater System Design Manual Chapter 9 Flow Diagrams, GHX17ASG009DNHX45GN, Revision B, June 2018.

[52] CGN, ASP-Secondary Passive Heat Removal System Design Manual Chapter 2 Brief Introduction to the System, GHX17ASP002DNHX45GN, Revision B, 2018.

[53] CGN, ASP-Secondary Passive Heat Removal System Design Manual Chapter 3 System Functions and Design Bases, GHX17ASP003DNHX45GN, Revision A, 2018.

[54] CGN, ASP-Secondary Passive Heat Removal System Design Manual Chapter 4 System and Component Design, GHX17ASP004DNHX45GN, Revision A, June 2018.

[55] CGN, ASP-Secondary Passive Heat Removal System Design Manual Chapter 5 Layout Requirements and Environment Condition, GHX17ASP005DNHX45GN, Revision A, 2018.

[56] CGN, ASP-Secondary Passive Heat Removal System Design Manual Chapter 6 System Operation and Maintenance, GHX17ASP006DNHX45GN, Revision B,

June 2018.

[57] CGN, ASP-Secondary Passive Heat Removal System Design Manual Chapter 9 Flow Diagrams, GHX17ASP009DNHX45GN, Revision B, June 2018.

[58] CGN, ECS-Extra Cooling System Design Manual Chapter 2 Brief Introduction to the System, GHX17ECS002DNHX45GN, Revision A, 2018.

[59] CGN, ECS-Extra Cooling System Design Manual Chapter 3 System Functions and Design Bases, GHX17ECS003DNHX45GN, Revision B, 2018.

[60] CGN, ECS-Extra Cooling System Design Manual Chapter 4 System and Component Design, GHX17ECS004DNHX45GN, Revision A, June 2018.

[61] CGN, ECS-Extra Cooling System Design Manual Manual Chapter 5 Layout Requirements and Environment Condition, GHX17ECS005DNHX45GN, Revision A, 2018.

[62] CGN, ECS-Extra Cooling System Design Manual Chapter 6 System Operation and Maintenance, GHX17ECS006DNHX45GN, Revision B, June 2018.

[63] CGN, ECS-Extra Cooling System Design Manual Chapter 9 Flow Diagrams, GHX17ECS009DNHX45GN, Revision B, June 2018.

[64] CGN, ALARP Demonstration Report for Safety Systems, GHX00100050 KPGB03GN, Revision B, 2018.

Appendix 7A Route Map

Claim		Sub-claim		Argument		PCSR Links	Evidence
3.3.3	The design of the Safety Systems has been substantiated.	3.3.3A	The safety functional requirements (Design Basis) have been derived for the system.	3.3.3A-1	The specific design principles are identified for the Structures, Systems and Components (SSCs) based on relevant good practice.	Sub-chapter 7.3	Reference [5] Reference [6]
				3.3.3A-2	The design basis (requirements) of the SSCs has been derived from the safety analysis in accordance with the general design and safety principles.	Sub-chapter 7.4.X.1 Sub-chapter 7.4.X.3 Sub-chapter 7.X.1 Sub-chapter 7.X.3	SDM Chapter 2, SDM Chapter 3 SDM Chapter 5
				3.3.3A-3	The Safety Class of the SSCs has been identified from the safety analysis.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 3
		3.3.3B	The system design satisfies the safety functional requirements.	3.3.3B-1	Appropriate design methods have been identified for the SSCs including design codes and standards.	Sub-chapter 7.2.4. Sub-chapter 7.4.X.2 Sub-chapter 7.X.2	SDM Chapter 3
				3.3.3B-2	The SSCs have been analysed using the appropriate design methods and meet the design basis requirements.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 4 SDM Chapter 6 SDM Chapter 9
				3.3.3B-3	The SSCs analysis recognises interface requirements and effects from/to the interfacing SSCs.	Sub-chapter 7.4.X.4 Sub-chapter 7.X.4	SDM Chapter 4
		3.3.3C	All reasonably practicable measures have been adopted to improve the design.	3.3.3C-1	The SSCs meet the requirements of the relevant design principles (generic and system specific) and therefore of relevant good practice.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 3 SDM Chapter 4 SDM Chapter 6
				3.3.3C-2	PSA indicates the SSCs are not disproportionate contributor to risk.	Sub-chapter 7.11	/
				3.3.3C-3	Design improvements have been considered in the SSCs and any reasonably practicable changes implemented.	Sub-chapter 7.11	/
		3.3.3D	The system performance will be validated by suitable commissioning and testing.	3.3.3D-1	The SSCs have been designed to take benefit from a suite of pre-construction tests, to provide assurance of the initial quality of the manufacture.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 4 SDM Chapter 6
				3.3.3D-2	The SSCs has been designed to take benefit from a suite of commissioning tests, to provide assurance of the initial quality of the build.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 6
		3.3.3E	The effects of ageing of the system have been addressed in the design and suitable examination, inspection, maintenance and testing specified.	3.3.3E-1	An initial Examination, Maintenance, Inspection and Testing (EMIT) strategy has been developed for the SSCs that are expected to be examined, maintained, inspected and tested.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 6
				3.3.3E-2	The SSCs that cannot be replaced have been shown to have adequate life, which includes the requirements during decommissioning.	Sub-chapter 7.4.X.5 Sub-chapter 7.X.5	SDM Chapter 6

Appendix 7B Functional Diagram of Safety Systems