Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Mechanical Engineering for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-004
Revision 0
January 2022

Published 01/22

EXECUTIVE SUMMARY

This report presents the findings of my assessment of the Mechanical Engineering aspects of the UK HPR1000 reactor design. It forms part of the Office for Nuclear Regulation's Generic Design Assessment. My assessment used the Pre-Construction Safety Report and supporting documentation submitted by the Requesting Party.

The objective of my assessment was to judge whether the generic design could be built and operated safely in Great Britain (subject to site specific assessment and licensing). My judgement informs the Office for Nuclear Regulation's decision on whether to grant a Design Acceptance Confirmation.

The scope of my assessment was to review the safety aspects of the generic UK HPR1000 design. It examined the claims, arguments and supporting evidence in the safety case. My Generic Design Assessment Step 4 assessment built upon the work undertaken in Steps 2 and 3. This enabled me to make a judgement on the adequacy of the Mechanical Engineering information in the Pre-Construction Safety Report and supporting documentation.

My assessment focussed on the following aspects of the generic UK HPR1000 safety case:

- heating, ventilation and air conditioning design substantiation;
- mechanical engineering schedule including safety functional categorisation and safety classification;
- equipment qualification arrangements;
- relevant good practice;
- examination, inspection, maintenance and testing arrangements;
- design assurance arrangements;
- application of the 'as low as reasonably practicable' principle during design changes;
- reducing fibrous material risks within containment;
- demonstrating nuclear lifting risks are reduced as low as reasonably practicable; and
- risks relating to fuel handling within the Fuel Building.

The conclusions from my assessment are that the Requesting Party has, for the purposes of Generic Design Assessment, adequately:

- substantiated the heating, ventilation and air conditioning system design;
- produced a suitable safety categorisation and classification methodology allowing safety functions to be traced;
- improved its equipment qualification arrangements;
- understood relevant good practice and implemented this during design changes;
- understood examination, inspection, maintenance and testing requirements, including safe isolation of plant and equipment;
- applied the 'as low as reasonably practicable' principle when making design changes;

- replaced fibrous material insulation with reflective metallic insulation, reducing associated risks as low as reasonably practicable in containment;
- understood reactor pressure vessel head lifting risks, reducing these as low as reasonably practicable;
- improved its fuel handling equipment design; and
- improved its spent fuel pool crane design.

I also conclude that the Requesting Party has closed four Mechanical Engineering Regulatory Observations. These related to:

- Relevant good practice
- Nuclear lifting operations
- Heating, ventilation and air conditioning performance
- Equipment qualification

My conclusions are based on the following:

- a sampled technical assessment of generic safety case documentation;
- independent reviews and analyses by Technical Support Contractors;
- detailed technical interactions with the Requesting Party; and
- responses to Regulatory Queries and Regulatory Observations.

A number of matters remain. I judge these matters are appropriate for a licensee to consider and take forward in its site-specific safety submissions. They do not undermine the generic design or safety case. They are primarily concerned with evidence that will become available as the project progresses. I judge the licensee can consider them within site-specific safety submissions. These matters are captured in 16 Assessment Findings.

I judge the Requesting Party's safety case is adequate. I recommend, from a Mechanical Engineering perspective, that a Design Acceptance Confirmation be granted.

LIST OF ABBREVIATIONS
(General)

ALARP	As Low as Reasonably Practicable
ANSI	American National Standards Institute
ASME	American Society of Mechanical Engineers
BFX	Fuel Building
BNX	Nuclear Auxiliaries Building
BRX	Reactor Building
BS	British Standard
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
BWR	Boiling Water Reactor
C&I	Control and Instrumentation
CAE	Claims-Arguments-Evidence
CCF	Common Cause Failure
CDM	Construction, Design and Management Regulation 2015
CFD	Computational Fluid Dynamics
CGN	China General Nuclear Power Corporation Ltd
COMAH	Control of Major Accident Hazards
CR	Contact Record
CRDM	Control Rod Drive Mechanism
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
DBC	Design Basis Condition
DEC	Design Extension Condition
DR	Design Reference
DG	Diesel Generator
DMGL	Delivery Management Group Lead
DRR	Design Risk Register
DRP	Design Reference Point
DSEAR	The Dangerous Substances and Explosive Atmospheres Regulations 2002
ECCS	Emergency Core Cooling System
EDG	Emergency Diesel Generator
EHA	Equipment Access Hatch
EIMT	Examination, Inspection, Maintenance and Testing[*]
ENSREG	European Nuclear Safety Regulators Group
EPDM	Ethylene Propylene Diene Monomer

[*] *This abbreviation is sometimes referred to by others as EMIT. For example, see sub-section 4.5 where this term is used in conjunction with RO-UKHPR1000-0021.*

EPRI	Electrical Power Research Institute
EQ	Equipment Qualification
FA	Fuel Assembly
FOAK	First of a Kind
GDA	Generic Design Assessment
GNSL	General Nuclear System Ltd.
GSR	Generic Security Report
HF	Human Factors
HOW2	ONR's Business Management System
HEPA	High Efficiency Particulate Air (ventilation filters)
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
iDAC	Interim Design Acceptance Confirmation
ISO	International Organisation for Standardisation
LHSI	Low Head Safety Injection (pump)
LOCA	Loss of Cooling Accident
LOLER	The Lifting Operations and Lifting Equipment Regulations 1998
MCR	Main Control Room
MDSL	Master Document Submission List
ME	Mechanical Engineering (used in sub-section 4.2 only)
MHSI	Medium Head Safety Injection (pump)
MSL	Main Steam Line
MSQA	Management for Safety and Quality Assurance
MSCRV	Main Steam Relief Control Valve
MSIV	Main Steam Isolation Valve
MSSV	Main Steam Safety Valve
MW	Megawatts
NDE	Non-Destructive Examination
NDT	Non-Destructive Testing
NEA	Nuclear Energy Agency (within OECD)
NPP	Nuclear Power Plant
NPSH	Net Positive Suction Head
OECD	Organisation for Economic Cooperation and Development
ONR	Office for Nuclear Regulation
OPEX	Operational Experience[†]
PCER	Pre-Construction Environmental Report
PCSR	Pre-Construction Safety Report

[†] *This is also referred to by others as Operating Experience.*

PIE	Postulated Initiating Event
PSV	Pressuriser Safety Valve
PSA	Probabilistic Safety Analysis
PSR	Preliminary Safety Report (includes security and environment)
PWR	Pressurised Water Reactor
QA	Quality Assurance
RCCA	Rod Cluster Control Assembly
RGP	Relevant Good Practice
RHR	Residual Heat Removal
RI	Regulatory Issue
RMI	Reflective Metallic Insulation
RO	Regulatory Observation
ROA	Regulatory Observation Action
RP	Requesting Party
RPV	Reactor Pressure Vessel
RSS	Remote Shutdown Station
RQ	Regulatory Query
SAA	Severe Accident Analysis
SADV	Severe Accident Dedicated Valve
SAP(s)	Safety Assessment Principle(s)
SB-LOCA	Small Break Loss of Cooling Accident
SBO	Station Black Out
SDM	System Design Manual
SFA	Spent Fuel Assembly
SFC	Single Failure Criterion
SFCC	Spent Fuel Cask Crane
SFAIRP	So Far as is Reasonably Practicable
SFIS	Spent Fuel Interim Storage
SFP	Spent Fuel Pool
SFPC	Spent Fuel Pool Crane
SFR	Safety Functional Requirement
SG	Steam Generator
SoDA	Statement of Design Acceptability (Environment Agency)
SQEP	Suitably Qualified and Experienced Personnel
SSC	Structures, Systems and Components
SSER	Safety, Security and Environment Report
TAG	Technical Assessment Guide(s)
TLOCC	Total Loss of Cooling Chain
TSC	Technical Support Contractor

WENRA	Western European Nuclear Regulators' Association
WSE	Written Scheme of Examination [LOLER]
ZOI	Zone of Influence

LIST OF ABBREVIATIONS
(UK HPR1000 Systems)

ADG [FDTGSS]	Feedwater Deaerating Tank and Gas Stripper System
APG [SGBS]	Steam Generator Blowdown System
ARE [MFFCS]	Main Feedwater Flow Control System
ASG [EFWS]	Emergency Feedwater System
ASP [SPHRS]	Secondary Passive Heat Removal System
ATE [CPS]	Condensate Polishing System
CRF [CWS]	Circulating Water System
DCL [MCRACS]	Main Control Room Air Conditioning System
DEL [SCWS]	Safety Chilled Water System
DFL [SCS]	Smoke Control System
DMK [FBHE]	Fuel Building Handling Equipment
DMR [RBHE]	Reactor Building Handling Equipment
DVD [DBVS]	Diesel Building Ventilation System
DVL [EDSBVS]	Electrical Division of Safeguard Building Ventilation System
DWK [FBVS]	Fuel Building Ventilation System
DWL [SBCAVS]	Safeguard Building Controlled Area Ventilation System
DWN [NABVS]	Nuclear Auxiliary Building Ventilation System
DWW [ABCAVS]	Access Building Controlled Area Ventilation System ABCAVS
EBA [CSBVS]	Containment Sweeping and Blowdown Ventilation System
ECS [ECS]	Extra Cooling System
EHR [CHRS]	Containment Heat Removal System
EPP [CLRTMS]	Containment Leak Rate Testing and Monitoring System
EUF [CFES]	Containment Filtration and Exhaust System
EVR [CCVS]	Containment Cooling and Ventilation System
GCT [TBS]	Turbine Bypass System
JAC [FWPS]	Fire-fighting Water Production System
JPI [FWSNI]	Fire-fighting Water System for Nuclear Island
JPV [FSDB]	Fire Extinguishing System for Nuclear Island Diesel Generator Building
KDS [DAS]	Diverse Actuation System
LHP	NI 10 kV Emergency Power Supply System (Train A)
LHQ	NI 10 kV Emergency Power Supply System (Train B)
LHR	NI 10 kV Emergency Power Supply System (Train C)
LHU	NI 10 kV SBO Power Supply System (Train A)
LHV	NI 10 kV SBO Power Supply System (Train B)
PMC [FHSS]	Fuel Handling and Storage System
PTR [FPCTS]	Fuel Pool Cooling and Treatment System
RBS [EBS]	Emergency Boration System

RCP [RCS]	Reactor Coolant System
RCV [CVCS]	Chemical and Volume Control System
REA [RBWMS]	Reactor Boron and Water Makeup System
REN [NSS]	Nuclear Sampling System
RIS [SIS]	Safety Injection System
RPE [VDS]	Nuclear Island Vent and Drain System
RRI [CCWS]	Component Cooling Water System
SEC [ESWS]	Essential Service Water System
SEL [LWDS (CI)]	Conventional Island Liquid Waste Discharge System
SRE [SRS]	Sewage Recovery System
TEG [GWTS]	Gaseous Waste Treatment System
TEP [CSTS]	Coolant Storage and Treatment System
TER [NLWDS]	Nuclear Island Liquid Waste Discharge System
TEU [LWTS]	Liquid Waste Treatment System
VDA [ASDS]	Atmospheric Steam Dump System
VVP [MSS]	Main Steam System

TABLE OF CONTENTS

Figures

Figure 1 to Figure 15, Figure 17 to Figure 21 and Figure 23 to Figure 24 are all produced with the kind permission of General Nuclear System Ltd.

Tables

Annexes

1 INTRODUCTION

1.1 Background

1. This report presents my Mechanical Engineering assessment of the generic UK HPR1000 design.

2. The UK HPR1000 is a pressurised water reactor (PWR) design proposed for deployment in GB. General Nuclear System Ltd (GNSL) is a UK-registered company established to implement the Generic Design Assessment (GDA) of the UK HPR1000 design. It does this on behalf of three joint requesting parties (RP):

- China General Nuclear Power Corporation (CGN)
- EDF SA
- General Nuclear International Ltd (GNI)

3. GDA is a process undertaken jointly by the Office for Nuclear Regulation (ONR) and the Environment Agency. Information on the GDA process is provided in a series of documents published on the joint regulators' website (www.onr.org.uk/new-reactors/index.htm). The outcome sought by the RP is a Design Acceptance Confirmation (DAC) from ONR and a Statement of Design Acceptability (SoDA) from the Environment Agency.

4. The GDA commenced in 2017 following a stepwise approach. Major technical interactions started in Step 2 examining the RP's safety case claims. Step 3 examined the supporting arguments. The joint regulators' website published reports on Step 2 and 3 findings.

5. The aim of Step 4 of GDA was to assess a sample of the RP's evidence. This evidence supported, and formed the basis of, the safety and security cases.

6. The full range of items forming part of my assessment, are provided in ONR's GDA Guidance to Requesting Parties (Ref. 1). These include:

- considering issues identified during the earlier Step 2 and 3 assessments;
- judging the design against the Safety Assessment Principles (SAPs) (Ref. 2) and whether the proposed design ensures risks are reduced As Low As Reasonably Practicable (ALARP);
- reviewing details of the RP's design controls and quality control arrangements to secure compliance with the design intent;
- establishing whether the system performance, safety classification, and reliability requirements are substantiated by a more detailed engineering design;
- assessing arrangements for ensuring and assuring that safety claims and assumptions will be realised in the final as-built design; and
- resolving nuclear safety issues or identifying paths for resolution.

7. This report summarises my Mechanical Engineering assessment. It supports ONR's decision on whether to grant a DAC, or otherwise.

8. This assessment focused on the submissions made by the RP throughout GDA, including those provided in response to the Regulatory Queries (RQs) and Regulatory Observations (ROs) I raised. The ROs are published on the GDA's joint regulators' website together with the corresponding resolution plans.

1.2 Scope of this Report

9. This report presents the findings of my Step 4 GDA Mechanical Engineering assessment against the generic UK HPR1000 design.

10. I assessed the Pre-Construction Safety Report (PCSR) (Ref. 3) and its supporting documentation. In line with GDA objectives, I judged whether the safety case justified the generic UK HPR1000 design.

11. I began my Step 4 assessment against the RP's Design Reference 2.1 (DR2.1) PCSR, issued in January 2020. Since then, the RP has updated its safety case and Design Reference, to include Step 4 developments. The submissions I assessed from Design References 2.2 and 3.0 are also identified in Section 4.

1.3 Methodology

12. My assessment methodology follows ONR's guidance for its inspectors on the mechanics of assessment, NS-TAST-GD-096 (Ref. 4).

13. My assessment was undertaken against ONR's How2 Business Management System (BMS). I used ONR's Safety Assessment Principles (SAPs) (Ref. 2) and supporting Technical Assessment Guides (TAGs) (Ref. 4) as the basis for my assessment. Further details are provided in sub-sections 2.4.1 and 2.4.2 of this report. My assessment is consistent with ONR's GDA Guidance to RPs (Ref. 1).

2 ASSESSMENT STRATEGY

14. This section sets out the strategy for my Mechanical Engineering assessment of the UK HPR1000 design and safety case. It identifies the scope of the assessment and the standards and criteria that have been applied.

2.1 Assessment Scope

15. My Step 4 assessment plan (Ref. 5) provides a detailed description of my assessment scope.

16. I sampled the main submissions, within my assessment scope remit, to various degrees of breadth and depth. There is no specific Mechanical Engineering PCSR chapter. Instead, topics extend over several chapters. Hence, I focussed on the relevant PCSR chapters with the greatest safety significance, or where hazards appeared less well controlled.

17. My assessment was influenced by:

- the claims made by the RP;
- my previous experience of similar systems for reactors and other nuclear facilities; and
- any identified gaps in the original submissions made by the RP.

18. An assessment focus has been the RQs (Ref. 6) and ROs (Ref. 7).

2.2 Sampling Strategy

19. In line with ONR's guidance (Ref. 1, Ref. 4, Ref. 8), and my assessment plan (Ref. 5), I chose a sample of the RP's submissions relating to the following Mechanical Engineering themes:

- Heating, Ventilation and Air Conditioning (HVAC) design substantiation;
- Mechanical Engineering schedule including safety categorisation and classification;
- equipment qualification arrangements;
- closure of gaps against Relevant Good Practice (RGP);
- Examination, Inspection, Maintenance and Testing (EIMT) arrangements;
- application of design assurance arrangements;
- application of the ALARP principle when considering design changes;
- reducing the hazards from fibrous material within the loss of coolant accident zone of influence;
- demonstrating nuclear lifts reduce risks ALARP; and
- lifting operations within the Fuel Building (BFX).

20. To satisfy the Mechanical Engineering assessment themes, I identified the following sample of reactor systems (Ref. 5), based on their significance to nuclear safety:

- Secondary Passive Heat Removal System (ASP) [SPRHRS]
- Emergency Feedwater System (ASG) [EFWS]
- Containment Heat Removal System (EHR) [CHRS]
- Containment Leak Rate Testing and Monitoring System (EPP) [CLRTMS]
- Main Control Room Air Conditioning System (DCL) [MCRACS]

- Safety Chilled Water System (DEL) [SCWS]
- Electrical Division of Safeguard Building Ventilation System (DVL) [EDSBVS]
- Diesel Building Ventilation System (DVD) [DBVS]
- Reactor Coolant System (RCP) [RCS]
- Safety Injection System (RIS) [SIS]
- Component Cooling Water System (RRI) [CCWS]
- Essential Service Water System (SEC) [ESWS]
- Liquid Waste Treatment System (TEU) [LWTS]
- Atmospheric Steam Dump System (VDA) [ASDS]
- Main Steam System (VVP) [MSS]
- Fuel Building Handling Equipment (DMK) [FBHES]
- Reactor Building Handling Equipment (DMR) [RBHES]
- Fuel Handling and Storage System (PMC) [FHSS]

21. In addition to these 18 systems, I sampled 22 specific components given their nuclear safety significance. This provided depth to my assessment.

22. Annex 1 illustrates the extent of my Mechanical Engineering assessment sample.

23. I also supported inspectors from other disciplines in closing RQs and ROs. These are discussed within my assessment report.

24. Given its late submission, my support to closing RO-UKHPR1000-0056 Fuel Route Safety Case is presented in sub-section 4.11 of this report.

2.3 Out of Scope Items

25. The Spent Fuel Interim Storage (SFIS) Facility design is at an early stage. Hence, it was not possible to undertake a meaningful Mechanical Engineering assessment.

2.4 Standards and Criteria

26. The relevant standards and criteria adopted within this assessment are principally:

- ONR's SAPs (Ref. 2)
- ONR's TAGs (Ref. 4)
- Relevant national and international standards
- RGP adopted on nuclear facilities

27. The key SAPs and relevant TAGs, national and international standards and guidance are detailed within this section. RGP, where applicable, is cited within the body of the assessment.

2.4.1 Safety Assessment Principles

28. The ONR SAPs constitute the regulatory principles against which ONR judges the adequacy of safety cases. The ONR 2006 edition of the SAPs were benchmarked against the International Atomic Energy Agency's (IAEA) Safety Standards. These SAPs have been updated to reflect subsequent changes in these standards since 2006. For the latest issue see (Ref. 2).

29. The key ONR SAPs used within my Mechanical Engineering assessment were:

- FP Fundamental principles
- MS Leadership and management for safety
- SC Safety cases
- EKP Key Principles
- ECS Safety classification and standards
- EQU Equipment qualification
- EDR Design for reliability
- EMT Maintenance, inspection and testing
- EAD Ageing and degradation
- ELO Layout
- EHA External and internal hazards
- EPS Pressure systems
- EMC Integrity of metal components and structures
- ESS Safety systems
- ECV Containment and ventilation
- ERC Reactor core
- RP Radiological protection
- NT Numerical targets and legal limits

30. Annex 2 of this report identifies the ONR SAPs considered in my assessment.

2.4.2 Technical Assessment Guides

31. The following TAGs were used to inform my assessment (Ref. 4):

- NS-TAST-GD-003 Safety Systems
- NS-TAST-GD-005 ONR Guidance on the Demonstration of ALARP
- NS-TAST-GD-007 Severe Accident Analysis
- NS-TAST-GD-009 Examination, Inspection, Maintenance and Testing of Items Important to Safety
- NS-TAST-GD-019 Essential Services
- NS-TAST-GD-022 Ventilation
- NS-TAST-GD-035 The Limits and Conditions for Nuclear Safety (Operating Rules)
- NS-TAST-GD-036 Diversity, Redundancy, Segregation and Layout of Mechanical Plant
- NS-TAST-GD-037 Heat Transport Systems
- NS-TAST-GD-056 Nuclear Lifting Operations
- NS-TAST-GD-057 Design Safety Assurance
- NS-TAST-GD-077 Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services
- NS-TAST-GD-094 Categorisation of Safety Functions and Classification of Structures, Systems and Components
- NS-TAST-GD-096 Guidance on the Mechanics of Assessment
- NS-TAST-GD-103 Emergency Power Generation

2.4.3 National and International Standards and Guidance

32. ONR's guidance to inspectors recognises developing advice and guidance from:

- the IAEA;
- Western European Nuclear Regulators Association (WENRA);
- European Nuclear Safety Regulators Group (ENSREG);
- International Nuclear Regulators Association;
- Organisation for Economic Cooperation and Development's Nuclear Energy Agency (NEA); and
- other relevant organisations.

33. WENRA safety reference levels are included as RGP within ONR's technical assessment guides.

34. My assessment focussed on the following IAEA publications (Ref. 9, Ref. 10, Ref. 11):

- IAEA Safety Standards, SSG-30 Safety Classification of Structures, Systems and Components in Nuclear Power Plants
- IAEA Safety Standards, SSG-63 Design of Fuel Handling and Storage Systems for Nuclear Power Plants
- IAEA Safety Standards, SSR-2/1 Safety of Nuclear Power Plants: Design

2.5 Use of Technical Support Contractors

35. It is usual in GDA for ONR to use Technical Support Contractors (TSCs). This provides access to independent advice and experience, analysis techniques and models. It also enables ONR's inspectors to focus on regulatory decision making.

36. Table 1 identifies the areas where TSCs supported my assessment.

Table 1: Work packages undertaken by TSCs

Number	Description
1	Provision of Technical Support for the Mechanical Engineering (HVAC Systems) Assessment for GDA of UK HPR1000.
2	Provision of Mechanical Engineering Specialist Resource to Support Step 4 of the UK HPR1000 GDA.

37. The TSC's technical reviews were done under my direction and close supervision. The regulatory judgement on the adequacy, or otherwise, of the generic safety case in this report has been made exclusively by ONR.

2.6 Integration with Other Assessment Topics

38. Regulatory assessment cannot be done in isolation as issues often span multiple disciplines. Hence, I worked with other ONR and Environment Agency inspectors to inform my assessment. This is particularly relevant to the closure of ROs. The key interactions and where relevant, ROs were:

- Civil Engineering: Layout and mechanical plant interactions / reactions (RO-UKHPR1000-0014)
- Conventional Health and Safety: Access and layout issues, for example falls from height (RO-UKHPR1000-0014)
- Electrical Engineering: Input loadings to HVAC thermal performance analysis (RO-UKHPR1000-0039)
- External Hazards: Derivation of extreme weather events to inform the thermal performance analysis of HVAC systems (RO-UKHPR1000-0039)
- Fault Studies: Inputs to Mechanical Engineering schedule and safety categorisation and classification of Structures, Systems and Components (RO-UKHPR1000-0056) and adequacy of EIMT (RO- UKHPR100-0021)
- Fuel and Core: Consequences associated with the safe handling of new and spent fuel (RO-UKHPR1000-0014 and RO-UKHPR1000-0056)
- Human Factors: Operator interfaces with mechanical engineering systems, for example operators' ability to respond / act and adequacy of HVAC systems to provide suitable working conditions (RO-UKHPR1000-0039)
- Electrical, Control and Instrumentation: Equipment qualification limits for HVAC thermal performance analysis (RO-UKHPR1000-0039), and prevention or protection measures within the Spent Fuel Pool (RO-UKHPR1000-0056)
- Internal Hazards: Prevention and mitigation of internal hazards, for example dropped loads, collisions and generation of projectiles (RO-UKHPR1000-0014, RO-UKHPR1000-0039 and RO-UKHPR1000-0056)
- Radiological Protection: dose mitigation during operations including EIMT and use of guidance within HSG253 "The safe isolation of plant and equipment" (RO-UKHPR1000-0012)
- Structural Integrity: Pumps and valve interfaces, for example delivery of containment safety functions
- The Environment Agency: HVAC High Efficiency Particulate Air (HEPA) filter selection (RO-UKHPR1000-0036)

39. Details of, and reference to, the above ROs can be found throughout Section 4 of this report.

40. For information, the ROs relate to:

- RO-UKHPR1000-0012 Identification and Application of Relevant Good Practice Applicable to Mechanical Engineering for the UK HPR1000 Design
- RO-UKHPR1000-0014 Design of Nuclear Lifting Operations to Demonstrate Relevant Risks are Reduced ALARP
- RO-UKHPR1000-0021 Demonstration of the Adequacy of Examination, Inspection, Maintenance and Testing of Structures, Systems and Components Important to Safety
- RO-UKHPR1000-0036 HEPA Filter Type
- RO-UKHPR1000-0039 Performance Analysis of UK HPR1000 Heating, Ventilation and Air Conditioning Systems
- RO-UKHPR1000-0056 Fuel Route Safety Case

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the Generic UK HPR1000 Design

41. The PCSR (Ref. 3) describes the generic UK HPR1000 design. It is a CGN designed, three-loop PWR using the Chinese Hualong technology. The generic UK HPR1000 design has evolved from reactors constructed and operated in China since the late 1980's. These include:

- the M310 design used at Daya Bay and Ling'ao (Units 1 and 2);
- the CPR1000;
- the CPR1000+; and
- the more recent ACPR1000.

42. CGN's first two units (Units 3 and 4) of the HPR1000, Fangchenggang (FCG) Nuclear Power Plant (NPP), are under construction in China. Unit 3 is the reference plant for the generic UK HPR1000 design (FCG3). The design is claimed to have a lifetime of at least 60 years and has a nominal electric output of 1,180 MW.

43. The reactor core contains zirconium clad uranium dioxide (UO_2) fuel assemblies. Reactivity is controlled by a combination of control rods, soluble boron in the coolant and burnable poisons within the fuel. The core is contained within a steel Reactor Pressure Vessel (RPV). It is connected, in a three-loop configuration, to the key primary circuit components. These components include the reactor coolant pumps, Steam Generators (SGs), pressuriser and associated piping.

44. The design includes several auxiliary systems that allow the plant to operate normally. It also includes active and passive safety systems to protect against faults. All these systems are contained within the following dedicated buildings:

- Reactor Building (BRX). This houses the reactor and primary circuit. It comprises double-walled containment with a large free volume.
- Three separate safeguard buildings surround the reactor building and house key safety systems and the main control room.
- Fuel Building (BFX). This is located adjacent to the reactor and contains the fuel handling and short-term storage facilities.
- Nuclear Auxiliary Building (BNX). This contains several systems supporting reactor operations.

45. The above buildings, together with the diesel, personnel access and equipment access buildings, constitute the generic UK HPR1000 nuclear island (see Figure 1).

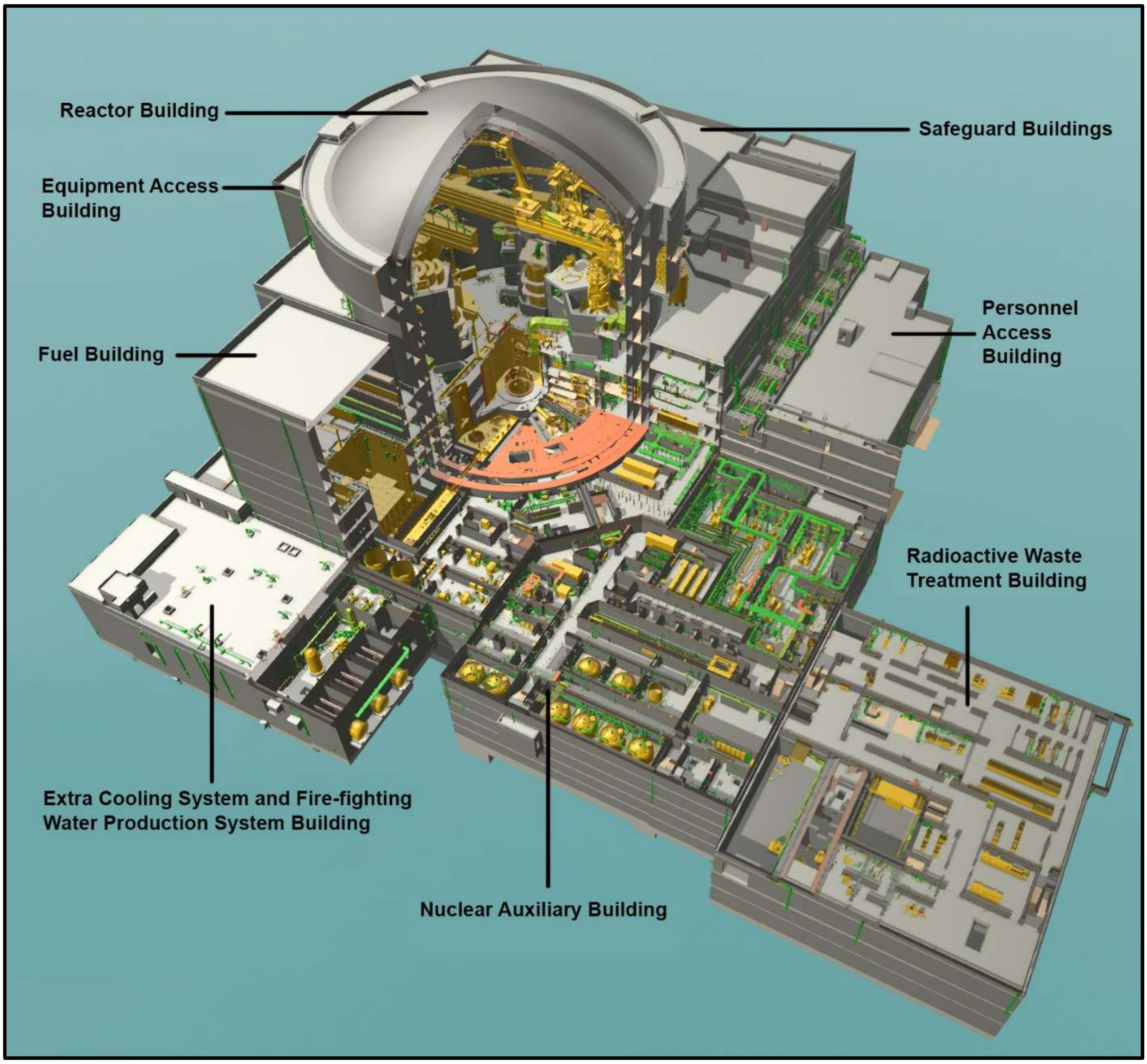

Figure 1: The UK HPR1000 nuclear island‡

3.2 The Generic UK HPR1000 Safety Case

46. This section gives an overview of the generic safety case relevant to my assessment. Details of my assessment can be found in sub-sections 4.1 to 4.11 of this report.

3.2.1 Documentation

47. The UK HPR1000 Safety Case comprises of 'Levels', related to the document types. This is presented in Figure 2. Of particular interest within my Mechanical Engineering assessment are:

Level 1 documents: which includes the PCSR, the Pre-Construction Environmental Report (PCER) and the Generic Security Report (GSR). Combined, these are referred to as the Safety, Security and Environment Report (SSER).

Level 2 documents: which includes design documentation, topic reports, assessment methodology reports, for example System Design Manuals (SDMs) and ALARP demonstration reports.

‡ *Figure taken from the GNSL website www.ukhpr1000.co.uk/the-uk-hpr1000-technology/hpr1000-design/*

Level 3 documents: which includes supplementary references, not referenced in the Level 1 submissions, such as technical specifications.

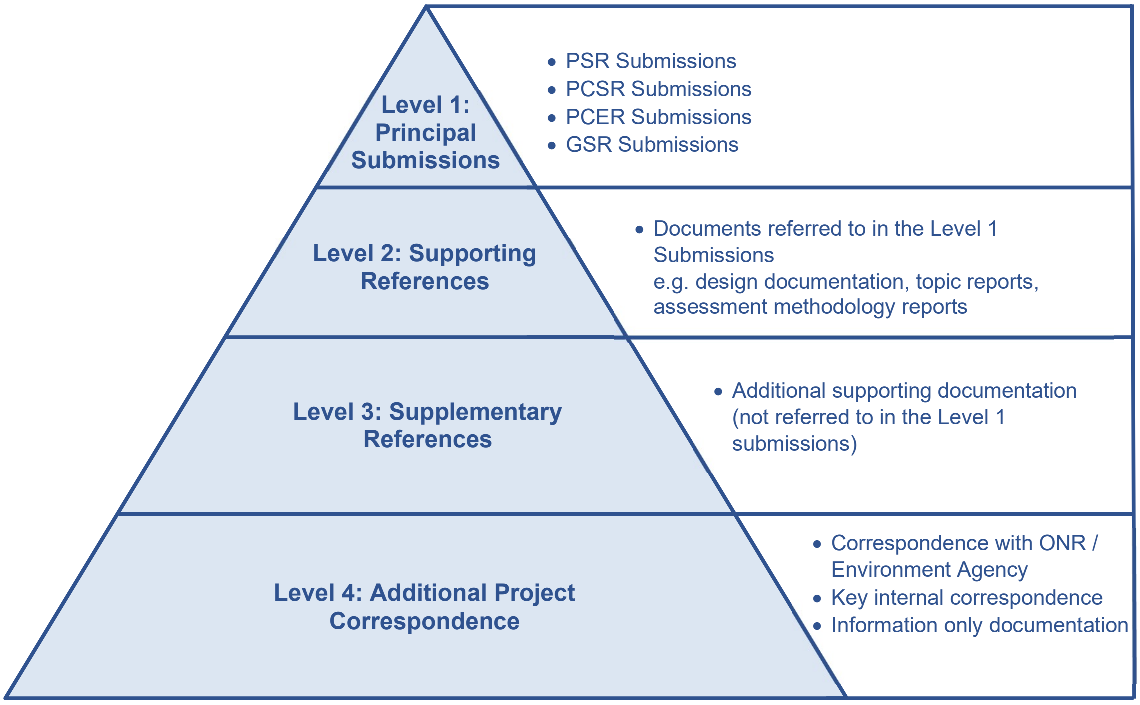

Figure 2: UK HPR1000 safety case documentation levels

48. The classification of these 'Levels' is defined within the RP's "Master Document Submission List (MDSL) Arrangements" (Ref. 12). My Mechanical Engineering assessment considered the Level 1, 2 and 3 documentation regarding the adequacy of the safety case.

3.2.2 Safety Case Structure and Claims

49. Chapter 1 of the PCSR (Ref. 13) sets out the structure of the safety case. It states that the UK HPR1000 safety case maintains a fundamental objective:

"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."

50. In support of this, it sets out two levels of claims:

- Level 1 Claims – these are high level objectives supporting the fundamental objective and cover:
  - Claim 1 Site characteristics
  - Claim 2 Design development and organisational arrangements
  - Claim 3 Nuclear safety
  - Claim 4 Environmental protection, security and conventional safety
  - Claim 5 Decommissioning
- Level 2 Claims – these support the Level 1 claims and are in turn supported within individual chapters of the PCSR by additional claims and arguments.

51. The RP provides arguments and evidence supporting its claims. Many of these claims are within the scope of Mechanical Engineering with a significant bearing on nuclear

safety. Below are the two, key safety case claims. I focussed my assessment on these claims, together with the supporting PCSR chapters. I selected these claims as they specifically relate to nuclear safety, the engineering design and demonstration that risks are ALARP.

- Level 2 Claim 3.3: "The design of the processes and systems has been substantiated and the safety aspects of operation and management have been substantiated." Supported by:
    - PCSR Chapter 6 Reactor Cooling Systems (Ref. 14)
    - PCSR Chapter 7 Safety Systems (Ref. 15)
    - PCSR Chapter 10 Auxiliary Systems (Ref. 16)
    - PCSR Chapter 11 Steam and Power Systems (Ref. 17)
    - PCSR Chapter 23 Radioactive Waste Management (Ref. 18)
    - PCSR Chapter 28 Fuel Route and Storage (Ref. 19)
- Level 2 Claim 3.4: "The safety assessment shows that the nuclear safety risks are ALARP." Supported by:
    - PCSR Chapter 6 Reactor Cooling Systems
    - PCSR Chapter 7 Safety Systems
    - PCSR Chapter 10 Auxiliary Systems
    - PCSR Chapter 11 Steam and Power Systems
    - PCSR Chapter 23 Radioactive Waste Management
    - PCSR Chapter 28 Fuel Route and Storage

52. The RP's Level 2 and Level 3 submissions (see Figure 2) present the arguments and evidence supporting the above claims. These cover the following general areas:

- System design manuals
- Transient analyses
- ALARP demonstration reports
- Compliance gap analyses
- Engineering schedules
- Technical specifications
- Design modifications

53. The specific documents I assessed are referenced within the body of my report (see Section 4 of this report).

54. At the end of GDA, the RP's safety case documentation was updated (consolidated) to ensure that all design modifications made during GDA were reflected[§].

[§] *Note that not all modifications were because of GDA. Some are associated with construction or commissioning operations in the reference plant (FCG3).*

4 ONR ASSESSMENT

Structure of Assessment Undertaken

55. My assessment plan (Ref. 5) describes ten specific design areas (Mechanical Engineering Themes) for Step 4 assessment.

56. My assessment focussed on:

- the nuclear safety related claims made within the PCSR chapters; and
- the arguments and evidence contained within the supporting references.

57. The PCSR comprises 33 chapters. No single PCSR chapter explicitly captures the Mechanical Engineering safety case claims. Instead, these claims are spread across many safety case chapters. Chapter 33 (Ref. 20) of the PCSR contains the ALARP Evaluation. I have not assessed this chapter, as it is the subject of a cross-cutting ONR assessment captured in the Step 4 Summary Report (Ref. 21).

58. My Step 4 assessment plan considered the progress made during Steps 2 and 3 of GDA. It also considered the findings and recommendations from the previous Step 3 assessment (Ref. 22).

59. My assessment included technical (known as Level 4) engagements with the RP, which are reported in Contact Records (CRs). I raised several RQs and led in raising four ROs. The CRs, ROs and RQs are referenced in my assessment report.

60. My Step 4 assessment considered the RP's safety case at Design Reference 2.1 (DR2.1), issued in January 2020. Subsequently the RP's safety case has evolved, as expected, in response to the GDA process. Updates submitted to ONR are as follows:

- December 2020 - Design Reference 2.2 (DR2.2)
- October 2021 - Design Reference 3.0 (DR3.0)

61. I have assessed several submissions in DR2.2 and DR3.0 as identified, where appropriate, in the various sub-sections below. I have also undertaken a consolidation exercise to confirm that the RP has appropriately captured the agreed safety case changes.

62. ONR's oversight of the UK HPR1000 GDA Design Reference is captured in the Step 4 Summary Report (Ref. 21).

Assessment Report Outline

63. Sub-sections 4.1 to 4.10 of this report present my Step 4 assessment. These include my judgements on the RP's response to my RQs.

64. Sub-section 4.11 of this report presents my fuel route safety case assessment. This was based on DR2.2 submissions (post December 2020).

65. Sub-section 4.12 of this report presents my review of the RP's consolidated safety case at DR3.0 (October 2021). This considered whether the RP's revised safety case included the Step 4 assessment outcomes.

66. Where my assessment identifies findings, these are categorised, in accordance with ONR's guidance (Ref. 23) as:

- Assessment Findings

- Minor Shortfalls

67. I identified matters I consider to be normal business. I do not consider these matters significant enough to merit specific recording. I expect the licensee to address them in the site-specific stages. ONR will provide regulatory oversight, as appropriate, applying its SAPs and TAGs.

68. Within this assessment, any reference to the RP's safety case arrangements being revised, is considered to be the responsibility of the licensee.

4.1 Theme 1: Adequacy of the UK HPR1000 Heating, Ventilation and Air Conditioning Design Substantiation

69. My Step 3 assessment (Ref. 22) concluded that the HVAC design had not been demonstrated to align with RGP. It noted that this would be progressed during Step 4.

70. The HVAC systems perform three main safety related functions:

- Support radioactive confinement by limiting the discharge of radioactive material into the environment.
- Maintain ambient conditions (temperature, humidity, and fresh air) within acceptable ranges for personnel and equipment. This supports the operation of systems important to safety.
- Provide chilled water to control the temperature of safety critical equipment.

71. To perform these safety related functions, the HVAC systems should satisfy the following two principles:

Radiological confinement

- Support physical containment by maintaining a negative pressure (depression) within the facility.
- Filter airborne contamination prior to air leaving the facility.
- Ensure interior airborne contamination is within acceptable levels.
- Provide sufficient air quality, to rooms or processes, to reduce the potential for generation of radioactive waste.
- Minimise loose radioactive sources in ventilated areas.
- Minimise airflow through a system. This limits the potential for the spread of contamination release of radioactivity and any associated impact on people and the environment.

Maintaining appropriate environmental conditions

- Maintain acceptable working conditions (temperature, humidity, fresh air) for the duration of the plant life (e.g. allowing for increases in ambient temperature due to climate change).
- Prevent / minimises chronic degradation of plant / equipment, which impacts safety and/or the containment of radioactive materials and waste.
- Control the spread of contamination during normal, fault and post-accident conditions.
- Minimise the release of radioactivity and any associated impact on people and the environment.

72. Additionally, the HVAC must provide chilled water to control the temperature of designated safety critical equipment. Many HVAC systems must perform their safety functions under normal, fault and post-accident conditions.

73. Sources of RGP for ventilation related radiological confinement include:

- SAPs (Ref. 2): these define Engineering Containment and Ventilation (ECV) requirements for nuclear safety, radiation protection and radioactive waste management.
- TAGs (Ref. 4), supporting the SAPs in specific topics on nuclear ventilation:

- NS-TAST-GD-003 Safety Systems
- NS-TAST-GD-005 Demonstration of ALARP
- NS-TAST-GD-009 Examination, Inspection, Maintenance and Testing of items important to safety
- NS-TAST-GD-019 Essential Services
- NS-TAST-GD-022 Ventilation
- NS-TAST-GD-026 Decommissioning
- NS-TAST-GD-037 Heat Transport Systems
- NS-TAST-GD-038 Radiological Protection
- NS-TAST-GD-094 Categorisation of Safety Functions and Classification of Structures and Components

■ National Nuclear Ventilation Forum (NNVF) endorsed guidance and standards. This includes the "Design Guide Ventilation Systems for Radiological Facilities" (Ref. 24) and other HVAC guidance and standards.

Note: ONR's Ventilation TAG, NS-TAST-GD-022, recommends that inspectors review this guidance when making assessments.

■ International guidance provided on nuclear ventilation provided by WENRA, International Standards Organisation (ISO), IAEA and the Nuclear Energy Agency publications. For example:

- IAEA Specific Safety Guide SSG-18 "Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations" (Ref. 25).

  Note: the reactor has a design life of 60 years. Hence, the HVAC design should consider temperature changes over this period.

- WENRA Reference Level I Ageing Management and Reference Level SV concerning internal hazards (Ref. 26)
- ISO 17873:2004 Nuclear Facilities – Criteria for the design and operation of ventilation systems for nuclear installations other than nuclear reactors (Ref. 27)
- BS ISO 26802:2010 Nuclear Facilities. Criteria for the design and operation of containment and ventilation systems for nuclear reactors (Ref. 28)
- IAEA-TECDOC-1744 Treatment of Radioactive Gaseous Waste (Ref. 29)
- OECD-NEA The Safety of the Nuclear Fuel Cycle (Ref. 30)

■ Conventional ventilation and fire safety including UK Building Regulations (Ref. 31). This includes Part L (Conservation of Fuel and Power) and Part F (Ventilation) (see www.gov.uk/topic/planning-development/building-regulations).

■ Dangerous Substances and Explosive Atmospheres Regulations (DSEAR) (Ref. 32).

4.1.1 Assessment

74. The HVAC system capacity is mainly justified through equivalence with the FCG3 reference design. The RP claimed that the HVAC systems would never be exposed to environmental conditions exceeding those of the reference design. Hence, all of UK HVAC Structures, Systems and Components (SSCs) were claimed to meet their nuclear safety functions. I noted that the basis of this was unclear. I raised the following RQs (Ref. 6) to seek clarification:

- RQ-UKHPR1000-0505 queried the HVAC systems and building thermal performance. The following matters required clarification:
  - For heat wave conditions, whether the safety systems remain within their operating temperature range.
  - The adequacy of chiller unit analysis.
- RQ-UKHPR1000-0556 queried the evidence supporting the ventilation system design. The following matters required clarification:
  - How performance is qualified and proven by calculations.
  - The depth of analysis undertaken.
  - The reliance on Computational Fluid Dynamics (CFD) for sizing of HVAC components.

75. I noted the following inadequacy in the RQ responses:

- When using very high-resolution models to consider temperature variations in, for example, single rooms, the boundary data for these calculations were assumed. I considered that the thermal paths, between the environmental heat sources and ultimate heat sinks, should have been included.

76. RO-UKHPR1000-0039 (Performance Analysis of UK HPR1000 HVAC Systems) (Ref. 33) was raised to close gaps in the HVAC systems substantiation. This required the RP to show that the HVAC systems can deliver against the safety demands placed upon them.

77. The RO identified the following Actions (ROA):

ROA.1 Develop an Appropriate UK HPR1000 HVAC Environmental Modelling and Analysis Strategy

- Develop a strategy to analyse a sample of UK HPR1000 HVAC systems.
- Describe how the analysis output will be used (including ALARP considerations and appropriately documenting the work in the generic safety case).

ROA.2 Model and Analyse the UK HPR1000 Heating Ventilation and Air Conditioning Systems

- Using the method identified in ROA.1, analyse and confirm the performance (or otherwise) of the UK HPR1000 HVAC systems against the safety demands.

- Detail and justify any assumptions within the analysis undertaken, including undertaking a suitable sensitivity analysis.
- Undertake an independent verification of the analysis.
- Confirm or otherwise, using the results of the analysis, the level of agreement between the commercial software package and the RP's extant analysis.
- Identify any shortfalls and gaps in the HVAC systems performance against their safety demands.

ROA.3 Undertake a ALARP Analysis for UK HPR1000 HVAC Systems

- Identify any other impacted UK HPR1000 safety systems, ALARP considerations of these impacted systems is outside the scope of the ROA.
- Undertake an optioneering study to identify appropriate solutions to address shortfalls and / or gaps in the UK HPR1000 HVAC systems
- Explain and justify whether any options have been identified as being reasonably practicable to implement.
- Explain which, if any, UK HPR1000 HVAC systems may require modifying.
- Explain how those modifications could be implemented, and how the generic safety case will be updated.

4.1.1.1 Closure of RO-UKHPR1000-0039

78. In response, the RP developed a series of dynamic models. The models illustrated the thermal responses of different rooms serviced by the sampled systems. This used a conservative heat wave condition.

79. The RP used the following process to resolve RO-UKHPR1000-0039:

- develop an analysis strategy;
- model and analyse sampled spaces; and
- undertake an ALARP analysis where gaps were found and identify reasonable options to address any gaps.

80. To address RO-UKHPR1000-0039, the RP undertook a numerical analysis of the following HVAC systems for a postulated heat wave:

- Train A of the Electrical Division of Safeguard Building Ventilation System (DVL) [EDSBVS]
- Train A of the Safety Chilled Water System (DEL) [SCWS]
- Train A of the Diesel Building Ventilation System (DVD) [DBVS]
- Main Control Room Air Conditioning System (DCL) [MCDACS]

81. The DVD [DBVS] represents a 'Type A' ventilation system. 'Type A' systems are temperature controlled.

82. The other HVAC samples represent 'Type B' HVAC systems. 'Type B' systems are enthalpy controlled.

83. Both Type A and Type B HVAC systems were selected for their nuclear safety significance.

84. The following RQs (Ref. 6) were raised, which relate to RO-UKHPR1000-0039.

RQ-UKHPR1000-0334

85. This queried the heat wave boundary condition, which:

- sets the external atmospheric conditions for air drawn in by the HVAC system; and
- influences the building fabric temperature, which in turn is cooled by the HVAC system.

86. The RP's response recognised the importance of defining the extreme weather conditions for a heat wave. It also explained how the daily thermal loads, for this extreme condition, might be interpreted.

87. The extreme ambient conditions provided were:

- extreme temperature (48.5 °C) and
- extreme enthalpy (90 kJ/kg).

88. Combining these two values gives a very low relative humidity, which may not be conservative. The RP responded that:

- extreme temperature and enthalpy provide a bounding, psychrometric envelope; and
- they are not co-incident, i.e. the extreme temperature and extreme enthalpy do not necessarily occur at the same time. They are separate limits for the two different variables.

89. I accepted the RP's approach to relative humidity. I noted the maximum temperature and maximum enthalpy are unlikely to be coincident in the UK.

Note: see further discussion in sub-section 4.1.1.2 of this report on temperature and enthalpy.

RQ-UKHPR1000-0777

90. This RQ queried the Station Black Out (SBO) CFD modelling and similar transient events. This focussed on how CFD supported the performance assessment and whether it complied with RGP. I considered that the RP's response aligned with RGP for CFD modelling regarding target rooms and ventilated enclosures.

91. As part of RO-UKHPR1000-0039, steady-state thermal analysis was undertaken of DVD [DBVS] (Type A system), DVL [EDSBVS], DEL [SCWS] and DCL [MCDACS] (Type B systems). This analysis used a lumped parameter modelling code, which is recognised as RGP for a building's thermal assessment. Transient analysis of the spaces vented by these systems was also considered. This included a range of transient fault and non-fault scenarios. The RP identified the following gaps:

- Insufficient flowrate for some HVAC systems in extreme summer conditions
- Insufficient heating in some rooms in extreme winter conditions, such as staircases and anterooms

92. The RP determined that:

- The current flow rate satisfies the cooling requirement but there is insufficient safety margin (less than 10%). Hence, the ventilation system may need to be enlarged during detailed design to provide the increased flowrate. The RP confirmed that sufficient space existed in the building to address this.

- Additional local heaters are required to resolve the heating related gaps. The additional heater sizing will be determined at site-specific stages (once the site-specific environmental data is known).

93. I consider the above to be normal business as they can be progressed during detailed design and/or site-specific stages.

RQ-UKHPR1000-1622

94. RQ-UKHPR1000-1622 sought clarification on the RP's "HVAC Sample Systems Analysis Report" (Ref. 34). Considering the RP's response, I concluded that:

- The dynamic modelling did not determine if:
    - any horizontal or vertical temperature variations exist within a space; or
    - local high temperatures exist near equipment.

95. I consider this a shortfall. The potential for local temperature variations (peak temperatures) in spaces requires more detailed investigation, for example CFD analysis. I am content that this can be done at the detailed design stage. This is important for qualifying safety related equipment if they are located within localised areas of high temperature. This is also discussed further in the Electrical Engineering Assessment Report (Ref. 35). As site specific information is not currently available to perform this analysis, I have captured this in Assessment Finding AF-UKHPR1000-0128.

96. The modelling includes sensitivity analysis but does not identify cliff-edge effects. A cliff-edge effect is where small increases in a design parameter, beyond the analysis, causes large interior temperature increases. This has HVAC SSC design implications. I have also raised this in Assessment Finding AF-UKHRP1000-128.

97. The HVAC safety case does not contain limits and conditions of safe operation. I do not consider this to be an issue given the level of conservatism within the analysis. The RP recognises that this information should be made available during site-specific stages.

RQ-UKHPR1000-1699

98. This RQ queried whether the DVD [DBVS] HVAC design has sufficient resilience against extreme exterior temperature (cliff-edge effects). The RP determined that a small change in external temperature would not prevent the HVAC system delivering its safety function.

99. For the purposes of GDA, I consider this response satisfactory. However, this judgement is subject to a demonstration that cliff-edge risks are ALARP. Site specific and detailed design information, beyond what is reasonable for GDA, will factor into this demonstration. I have raised this within Assessment Finding AF-UKHPR1000-0128.

100. If shortfalls are identified, the RP claims that there is adequate space for associated design modifications.

RQ-UKHPR1000-1768

101. RQ-UKHPR1000-1768 was raised by ONR's Electrical Engineering assessor. The RQ sought clarification as to whether the maximum room temperatures exceed the equipment's qualification temperature. The RP's response was judged to be adequate for GDA (Ref. 35). Importantly, the RP acknowledged that SSCs should be shown to remain within their qualified temperature ranges during normal, fault and accident conditions.

4.1.1.2 Assessment of Auxiliary Systems and Components

102. In addition to the above HVAC analysis, I sampled the following auxiliary systems:

- Electrical Division of Safeguard Building Ventilation System (DVL) [EDSBVS]
- Main Control Room Air Conditioning System (DCL) [MCRACS]
- Safety Chilled Water System (DEL) [SCWS]

103. These auxiliary systems were sampled given their safety significance to:

- confinement of material;
- air temperature regulation; and
- provision of chilled water for the air conditioning systems.

104. Within these systems, I assessed the following components:

- DCL [MCRACS] HEPA filters. Similar filters are also present in most other HVAC systems given their role in radiological containment.
- DVL [EDSBVS] isolation dampers, present in other systems, provide a physical barrier in fault conditions.
- DEL [SCWS] chiller units that cool both the interior spaces and specific safety critical components.

HEPA Filters

105. The safety function of the HEPA filter is to minimise the spread of radiological contamination by capturing particles within its filter media.

106. For the DCL [MCRACS] the HEPA filters:

- in normal operation perform a Safety Category B[**] function; and
- are Class 2 SSCs.

107. RGP for the HEPA filters includes:

- ONR SAPs (Ref. 2):
  - ECS.5 (Use of experience, tests or analysis) considers the use of SSC testing in the absence of codes and standards.
  - ERL.1 (Form of claims) considers SSC reliability in its operating environment.
  - EMC.3 (Evidence) addresses the integrity of metallic components.

[**] *Category A, B and C functions and Class 1, 2 and 3 SSCs are ONR terminology used in the SAPs (Ref. 2). FC1, FC2 and FC3 function categories and F-SC1, F-SC2 and F-SC3 functional classes are the RP's terminology (Ref. 48).*

  - ECV.10 (Ventilation system safety functions) considers the identification of safety functions for ventilation systems.

- ONR's Ventilation TAG, NS-TAST-GD-022 (Ref. 4)
- NNVF Design Guidance EG_0_1738_1 Ventilation Systems for Radiological Facilities (Ref. 24)
- NNVF Design Guidance EG_1_1702_1 (Design Guide for filters and filter installations in ventilation systems) (Ref. 36)

108. ONR's Ventilation TAG, NS-TAST-GD-022, references the NNVF Design Guidance EG_0_1738_1 (Ref. 24). It refers to the use of cylindrical HEPA filters where reasonably practicable. This is because cylindrical HEPA filters reduce the following radiological and environmental hazards that exist with rectangular HEPA filters:

- Filter by-passing: This is caused by degradation in seal quality achieved with the filter housing.
- Waste volumes and waste management: Rectangular filters have lower flow capacity. For larger ventilation systems more filters are required, ultimately leading to greater waste.
- Energy use: Cylindrical HEPA filters can achieve lower energy usage due to decreased pressure drops across filters.

109. The rectangular filter choice has been the subject of two ROs:

- RO-UKHPR1000-0012 – Identification and Application of Relevant Good Practice Applicable to Mechanical Engineering for the UK HPR1000 Design (led by ONR); and
- RO-UKHPR1000-0036 – HEPA Filter Type (led by the Environment Agency).

110. My assessment focussed on the selection of HEPA filters. I queried how the risk of by-passing was either eliminated or reduced so far as is reasonably practicable. Matters related to the selection of filters, filter by-passing, waste and energy use have also been considered by the Environment Agency (Ref. 37).

111. RQ-UKHPR1000-0514 queried the RP's rectangular filter choice. The RP accepted that circular filters reduce bypass leakage. However, the RP challenged whether the circular filters would produce less waste on disposal. The RP believed that rectangular filters are also better suited to safe-change maintenance procedures. The RP submitted an "Optioneering Report of HEPA Filter Types" (Ref. 38) to justify its rectangular filter preference. For the purposes of GDA, the HEPA filter shape optioneering arguments are considered reasonable. This is however subject to satisfactory demonstration of HEPA filter performance, captured within Assessment Finding AF-UKHPR1000-0128.

112. Related to RQ-UKHPR1000-0514, as part of RO-UKHPR1000-0036 closure (Ref. 37), the RP provided evidence of a design change to its existing HEPA filters (in its Chinese NPPs) to minimise by-pass leakage. However, little post modification data exists to support this claim. I consider this a Minor Shortfall.

113. Substantiation of the RP's claim will require a suitable record of evidence, which I judge is possible post-GDA. The RP's optioneering report (Ref. 38) indicates that the filters are already installed on operating Chinese plants. Therefore, time is needed to gather the evidence. Evidence supporting the minimisation of by-pass leakage claim can be pursued during detailed design and site-specific stages. ONR SAPs ECS.5

(Use of experience, tests or analysis), ERL.1 (Form of claims) and EMC.3 (Evidence) are relevant here.

114. RQ-UKHPR1000-1070 queried the duct inlet air velocity and corresponding dynamic loads on the filter material. For both the Access Building Controlled Area Ventilation System (DWW) [ABCAVS] and Nuclear Auxiliary Building Ventilation System (DWN) [NABVS] systems, the impingement velocity on the filter material exceeds the UK RGP of 10 m/s (Ref. 36). The RP has identified a post-GDA commitment (see CM-SUPP-1708 in the RP's "Post-GDA Commitment List" (Ref. 39)) to enlarge the filter inlet ducting (where necessary) to meet the UK standard. This modification reduces the filter duct entry velocity to acceptable levels and positively impacts the filter life. I consider this commitment to modify the inlet duct acceptable. This judgement is subject to demonstrating even flow and load distribution within the filter housing. I consider this normal business.

115. RQ-UKHPR1000-1222 queried the use the American Society of Mechanical Engineers (ASME) standard, AG-1 FC, for rectangular HEPA filters (see www.asme.org). RGP for rectangular HEPA filters is the ONR Ventilation TAG, NS-TAST-GD-022 and NNVF standards and guidance (Ref. 24, Ref. 36). The NNVF standards and guidance reference the ASME standards and include UK requirements and OPEX from GB licensed sites. Some differences exist between the two filter standards.

116. The ASME standard has a lower pressure drop, at higher flowrate than the equivalent UK rectangular filter. This indicates a more 'open' filter, potentially lowering the particle capture efficiency. The RP's response referenced published, experimental data showing:

- For the high pressure drop area of the filter, the influence of media velocity on efficiency reduces.
- The rectangular HEPA filters proposed have lower maximum media velocity than the UK standard. The performance of the filters is expected to be at least equivalent.
- The proposed UK HPR1000 HEPA filter is more efficient than the UK filter for the low pressure drop area (less than 500 Pa). Additionally, similar capture efficiency exists when either the pressure drops or loading time increases.

117. The RP sought to justify the choice of the ASME AG-1 FC rectangular HEPA filters. However, there is no direct experimental data available to substantiate the claims that the ASME AG-1 rectangular filters are equivalent to the standard cylindrical filters (rectangular performance versus cylindrical performance, which is supported by the NNVF). I consider this a shortfall against ONR SAPs ECS.5 (Use of experience, tests or analysis), ERL.1 (Form of claims) and EMC.3 (Evidence). Manufacturers' detailed design information, beyond what is reasonable for GDA, will is necessary to provide this data. Hence, I have raised this within Assessment Finding AF-UKHPR1000-0128. This is for the licensee to obtain adequate test data to validate the claims and arguments made by the RP during Step 4 of GDA.

118. I judge that the RP has shown alignment with ONR SAP ECV.10 (Ventilation system safety functions). This concerns its provision of filters and controlling dispersal of contamination and concentration of airborne activity to levels that are ALARP.

Isolation Dampers

119. Isolation dampers:

- protect against the release of radiological contamination;
- protect against the spread of fire or smoke;
- remain open during normal operation; and
- close during certain fault conditions providing a containment barrier.

120. In the Electrical Division of Safeguard Building Ventilation System (DVL) [EDSBVS], the isolation dampers:

- perform a Category B safety function or (Functional) Categorisation Class 2 (FC2);
- are Class 2 (F-SC2) SSCs for the normal operation train; and
- are Non-Classified (NC) within the maintenance line (see Table T-3.2-3 in (Ref. 40).

121. RGP for the isolation dampers includes ONR SAPs:

- EKP.5 (Safety measures) explains the hierarchy of safety measures. It explains the bias towards passive safety measures and the need for active engineering safety measures to be automatically initiated.
- ERL.3 (Engineered safety measures) considers the requirement for automatically initiated, rapid protective action in the form of engineered safety measures.
- EDR.2 (Redundancy, diversity and segregation) relates to the design of redundant means to fulfil safety functions.
- ECV.1 (Prevention of leakage) considers preventing or limiting the spread of contamination during normal and fault conditions.
- ECV.3 (Means of confinement) considers containment systems limits and conditions of safe operation.

122. I noted that the Safeguard Building Controlled Area Ventilation System (DWL) [SBCAVS] and the DVL SDMs specify many of the isolation dampers as ‘manual’ rather than automatic close. RQ-UKHPR1000-0506 was raised to seek clarification.

123. The RP confirmed that the isolation dampers:

- are automatically controlled; and
- can be ‘manually triggered’ from the Main Control Room (MCR).

124. I am content that the RP has shown that a diverse means of isolating the damper exists. This aligns with guidance in ONR SAP EDR.2 (Redundancy, diversity and segregation).

125. I have discussed the ‘manual’ activation of isolation dampers with ONR’s Human Factors inspector. I was advised that remote manual initiation is a proven concept. This will be pursued further during site-specific stages (Ref. 41).

126. I am content that the isolation dampers are automatically initiated in line with ONR SAPs EKP.5 (Safety measures) and ERL.3 (Engineered safety measures). I am also content that the RP can show that their function is to limit the spread of contamination

during faults ONR SAPs ECV.1 (Prevention of leakage) and ECV.3 (Means of confinement).

Chiller Units

127. Chiller units provide cooling, within specified limits, during normal operation and fault conditions.

128. For the DEL [SCWS], the chillers:

- perform a Category B safety function; and
- are Class 2 SSCs.

129. Chiller unit RGP includes:

- ONR SAPs (Ref. 2):
  - EKP.3 (Defence in depth) considers prevention of faults in the first instance.
  - EDR.2 (Redundancy, diversity and segregation) relates to the design of redundant means to fulfil safety functions.
  - ERL.4 (Margins of conservatism) considers SSC design conservatism.

130. The following RQs (Ref. 6) queried the chillers' ability to provide sufficient cooling:

- RQ-UKHPR1000-1327 queried the effect of increased exterior temperature on the chiller capacity; and
- RQ-UKHPR1000-1112 queried the impact of internal heat gains from equipment required to show adequate diversity in the HVAC system.

131. RQ-UKHPR1000-1327, raised by External Hazards, queried whether the chillers can accommodate an increase in extreme ambient temperature from 47 °C to 48.5 °C. The RP responded that:

- The chillers are sized on enthalpy only, rather than on temperature.
- Extreme exterior temperature and enthalpy are considered as separate conditions i.e. they are not co-incident. Hence, raising the exterior temperature does not necessarily put additional requirements on the enthalpy.
- A greater extreme exterior temperature increases the building fabric heat gain. This then raises the enthalpy of the recirculated air to the cooling coil by a small amount. Consequently, the temperature increase will only have a small indirect effect on the chillers.
- Under a diurnally[††] varying temperature profile the RO-UKHPR1000-0039 analysis (Ref. 34) shows that the extant chiller sizes are sufficient to manage exterior temperatures.

132. I judge this appropriate for the concept design within GDA. However, the licensee will need to show the chillers can satisfy the 48.5 °C extreme ambient temperature during detailed design. Hence, the licensee will need to consider extreme temperatures in sizing the HVAC systems, as the analysis has used enthalpy as the bounding condition.

[††] *diurnal temperature variation is the variation between a high and low air temperature that occurs during the same day.*

133. During detailed design, the licensee will need to justify the link between temperature, relative humidity and enthalpy for the extreme conditions seen by the HVAC systems. This will require site specific information. I have raised this within the following Assessment Finding:

> AF-UKHPR1000-0128: The licensee shall, during detailed design of the heating, ventilation and air conditioning systems, justify that:
> - local peak internal temperatures are derived from extreme exterior temperature conditions for the site;
> - dependant safety related equipment remains within its qualified temperature limits;
> - they are resilient against extreme exterior temperature, avoiding cliff-edge effects. Examples include flowrates, heating and thermal failures;
> - through testing, the chosen filter's efficiency and pressure drop performance are at least equivalent to that of a modern, cylindrical filter; and
> - the chiller design accounts for temperature, relative humidity and enthalpy during extreme exterior temperature conditions.

134. The blending of exterior and recirculated air, to maintain the space supply air temperature as the exterior temperature increases, is an important consideration. The RP confirmed that the proportion of air recirculated is determined by the fresh air requirements. Blending will be considered further at the site-specific stages. I consider this reasonable and to be normal business.

135. RQ-UKHPR1000-1112 queried:

- the chiller capacity requirements; and
- the level of diversity in the chiller units.

136. The RP estimated that, based on the FCG3 reference design, the cooling loads will increase by 3%. The DCL [MCRACS], DVL [EDSBVS] and DEL [SCWS] chiller capacities were considered within RO-UKHPR1000-0039 and shown to be adequate.

137. With respect to diversity and segregation, the RP stated that:

- At this stage, specific manufacturers have not been selected.
- It recognises that design assurance arrangements would need to be in place to ensure suppliers do not to share common sub-suppliers for critical components.
- Additional segregation is provided by operating equipment in different parts of the plant.

138. I discuss design assurance within sub-section 4.6 of this report.

139. I am satisfied that the RP has addressed RGP for the chiller units. It has satisfied my expectations regarding ONR SAPs:

- EKP.3 (Defence in depth)
- EDR.2 (Redundancy, diversity and segregation)
- ERL.4 (Margins of conservatism).

4.1.1.3 General

140. General HVAC RGP includes ONR SAPs (Ref. 2):

- ECV.10 (Ventilation system safety functions) considers prevention of faults in the first instance.
- EDR.2 (Redundancy, diversity add segregation) relates to the design of redundant means to fulfil safety functions.
- EDR.3 (Common cause failure) considers reliability of SSCs.
- ELO.4 (Minimisation of the effects of incidents) considers minimising interactions between failed SSCs and other plant.

141. During GDA Step 4, I submitted other RQs (Ref. 6) outside the scope of RO-UKHPR1000-0039. These RQs are summarised below.

RQ-UKHPR1000-0555

142. RQ-UKHPR1000-0555 queried what analysis will be undertaken to substantiate air flow and quality in the vicinity of the external inlets. I consider ONR SAP ECV.10 (Ventilation system safety functions) relevant here as it considers the siting of intakes and the effects of discharges from other nearby facilities.

143. The RP stated that ‘rogue exhausts’ are mitigated by ensuring that the air inlets are:

- lower than exhausts;
- as far away as possible from exhausts; and
- ideally on different faces of the building.

144. The RP investigated whether the DVD [DBVS] exhaust outlets and diesel stack exhausts adversely influence the DCL [MCRACS] and DVL [EDSBVS] inlets (Ref. 34). The modelling highlighted that the rogue exhaust would increase the temperature of the air intake to the Safeguard Building. This in turn increases the coils’ cooling requirement. The cooling coils are claimed to have a 10% design margin. This margin is greater than the additional cooling load resulting from the rogue exhaust.

145. The results of the CFD study are recognised to be influenced by many factors such as building topography, wind direction and wind speed. Hence, the modelling should be revisited during detailed design and/or site-specific stages. I judge this to be acceptable for GDA and in line with ONR SAP ECV.10 (Ventilation system safety functions). I consider progression of this to be normal business.

RQ-UKHPR1000-1598

146. RQ-UKHPR1000-1598 queried whether the DCL [MCRACS] and DVL [EDSBVS] system layout had adequate diversity and separation from potential turbine missiles. The MCR and Remote Shutdown Station (RSS) are served by separate HVAC systems. Both HVAC systems are located on the top floor of Safeguard Building C. The RP’s “Turbine Missiles Safety Assessment Report” (Ref. 42) indicated that a high trajectory missile could impact Safeguard Building C. I consider ONR SAPs EDR.2 (Redundancy, diversity add segregation), EDR.3 (Common cause failure) and (ELO.4 Minimisation of the effects of incidents) to be relevant.

147. The RP confirmed that:

- Diversity is maintained through different plant configurations.

- Segregation is maintained through installing DCL [MCRACS] Train C and DVL [EDSBVS] Train C in different rooms.
- The Smoke Control System (DFL) [SCS] would not be adversely impacted by this fault. This system has no safety function, and its loss will not affect plant safety.
- The possibility of losing DVL [EDSBVS] train C and all three DCL [MCRACS] trains simultaneously is extremely low. Should it happen, there would be no detriment to safety as the RSS can be ventilated by either DVL [EDSBVS] train C or train A. If DVL [EDSBVS] train C failed, it will be switched to DVL [EDSBVS] train A to maintain the temperature of the RSS. Hence, a missile could not credibly impact both DVL [EDSBVS] trains A and C at the same time.

148. I have discussed this with the ONR Internal Hazards inspector, who is content with this response (Ref. 43) and content that further analysis can be undertaken as normal business.

149. The RP has satisfied my expectations regarding ONR SAPs:

- EDR.2 (Redundancy, diversity add segregation)
- EDR.3 (Common cause failure)
- ELO.4 (Minimisation of the effects of incidents)

4.1.2 Strengths

150. The RP's design has evolved, progressing through previous iterations. Experience from FCG3 is being carried across to the generic UK HPR1000 design (ONR SAPs MS.4 (Learning) and SC.7 (Safety case maintenance)). This experience is shown by a high-level of technical understanding of nuclear HVAC evidenced by the RP in its submissions during Step 4 of GDA.

HEPA Filters

151. In reviewing UK RGP for filter testing procedures, the RP has adapted its processes to align with UK RGP (Ref. 24).

Isolation Dampers

152. The RP stated that in the HVAC system design, all accident actions are automatically controlled. Also, if necessary, all actions can be manually operated from the Main Control Room.

Chiller Units

153. The RP has shown the chiller units are sized for the most demanding conditions. Also, the RP's plans to diversify the chillers are appropriate. Finally, the impact of extra heat gains resulting from the incorporation of additional equipment related to diversity is appropriate.

4.1.3 Outcomes

154. The RP has shown good knowledge of UK RGP for nuclear ventilation, alignment with the SAPs, and made use of NNVF guidance and standards.

155. The RP has adequately addressed my concerns raised within RO-UKHPR1000-0039, which I consider closed (Ref. 44).

156. The RP adapted its modelling procedures to quantify the cooling capacity of the HVAC equipment. Its analyses showed the HVAC systems' resilience to extreme heat wave conditions. It also identified areas where margins need improvement and that systems could be modified appropriately.

157. I have raised one Assessment Finding, discussed in sub-section 4.1.1 that relates to:

- Qualification of equipment important to safety during the extreme weather conditions of the site.
- Detrimental cliff-edge effects.
- Comparing test evidence for chosen filters against RGP.
- The connection between temperature and enthalpy for extreme conditions.

158. I have identified one Minor Shortfall in paragraph 112. This relates to collating performance data from Chinese plants. This follows a modification to its HEPA filter design, to reduce by-passing.

159. The Assessment Findings are listed in Annex 3.

4.1.4 Conclusion

160. For RO-UKHPR1000-0039, the RP has:

- developed an appropriate strategy to analyse the performance of the HVAC systems;
- adequately implemented the strategy;
- undertaken independent verification of the HVAC performance analysis; and
- suitably addressed my concerns raised within this RO.

161. The RP has shown for the generic design, that its choice of rectangular HEPA filters is not likely to lead to a detriment to nuclear or environmental safety. This requires further substantiation during detailed design.

162. For isolation dampers the RP has shown that a diverse means of operation exists i.e. automatic and manually initiated.

163. For chillers, the RP has shown that:

- they are appropriately sized for the postulated extreme exterior conditions;
- it has arrangements in place to ensure diversity through the design process; and
- there is adequate capacity to deal with postulated extra heat gains.

164. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's substantiation of the heating, ventilation and air conditioning system design is sufficient from a Mechanical Engineering perspective.

165. I have identified several matters that the licensee will need to address during the detailed design. I have captured these in an Assessment Finding.

4.2 Theme 2: Adequacy of the Mechanical Engineering Schedule

166. My Step 3 assessment (Ref. 22) concluded that:

- An adequate Mechanical Engineering Schedule (referred to in my report as the 'ME Schedule') had not been delivered.
- Whilst the safety case architecture was better understood, the 'golden thread' of safety functional requirements was difficult to establish.

167. My ME Schedule assessment considered the suitability of the RP's:

- categorisation and classification methodology; and
- safety function requirement traceability (golden thread) including;
  - safety function identification and associated safety categorisation;
  - SSC identification and associated safety classification; and
  - SSC performance requirements.

168. ME Schedule RGP includes:

- The Management of Health and Safety at Work Regulations 1999 (MHSWR) (Ref. 45) Regulation 4 and Schedule 1.
- ONR SAPs (Ref. 2):
  - FP.6 (Prevention of accidents)
  - SC.2 (Safety case process outputs)
  - SC.4 (Safety case characteristics)
  - EKP.3 (Defence in depth)
  - EKP.4 (Safety function)
  - EKP.5 (Safety measures)
  - ECS.1 (Safety categorisation)
  - ECS.2 (Safety classification of structures, systems and components)
  - ECS.3 (Codes and standards)
  - ECS.5 (Use of experience, test or analysis)
  - EDR.2 (Redundancy, diversity and segregation)
  - EDR.3 (Common cause failure)
  - EAD.2 (Lifetime margins)
  - ERL.1 (Form of claims)
  - ERL.4 (Margins of conservatism)
  - EMT.6 (Reliability claims)
  - EMC.13 (Materials)
  - EMC.25 (Leakage)
  - ECV.1 (Prevention of leakage)
  - ECV.3 (Means of confinement)
  - ERC.1 (Design and operation of reactors)
  - EHA.5 (Design basis event operating states)

- EHT.1 (Design)
- EHT.2 (Coolant inventory and flow)
- NT.1 (Assessment against targets)

■ ONR TAGs (Ref. 4):

- NS-TAST-GD-003 Safety Systems
- NS-TAST-GD-005 Guidance on the Demonstration of ALARP
- NS-TAST-GD-019 Essential Services
- NS-TAST-GD-035 Limits and Conditions for Nuclear Safety (Operating Rules)
- NS-TAST-GD-094 Categorisation of Safety Functions and Classification of SSCs

■ IAEA standards and guidance:

- IAEA, Safety of Nuclear Power Plants: Design, Specific Safety Requirements, SSR-2/1 (Ref. 11);
- IAEA Safety Standards Series SSG-30 – Safety Classification of SSCs in Nuclear Power Plants (Ref. 9); and
- IAEA Application of the Safety Classification of SSCs in Nuclear Power Plants, TECDOC 1787 (Ref. 46).

4.2.1 Assessment

4.2.1.1 UK HPR1000 Categorisation and Classification Methodology

169. The RP's categorisation and classification methodology (Ref. 47) designates the category of the safety functions as either:

■ safety functions, which relate to functional delivery; or
■ design provisions, which relate to pressure boundary.

170. This approach differs from ONR guidance on Categorisation and Classification of SSCs, NS-TAST-GD-094 (Ref. 4). Nevertheless, it is consistent with IAEA guidance and therefore RGP (Ref. 9).

171. Figure 3 shows the RP's process overview for categorisation of safety functions and classification of SSCs.

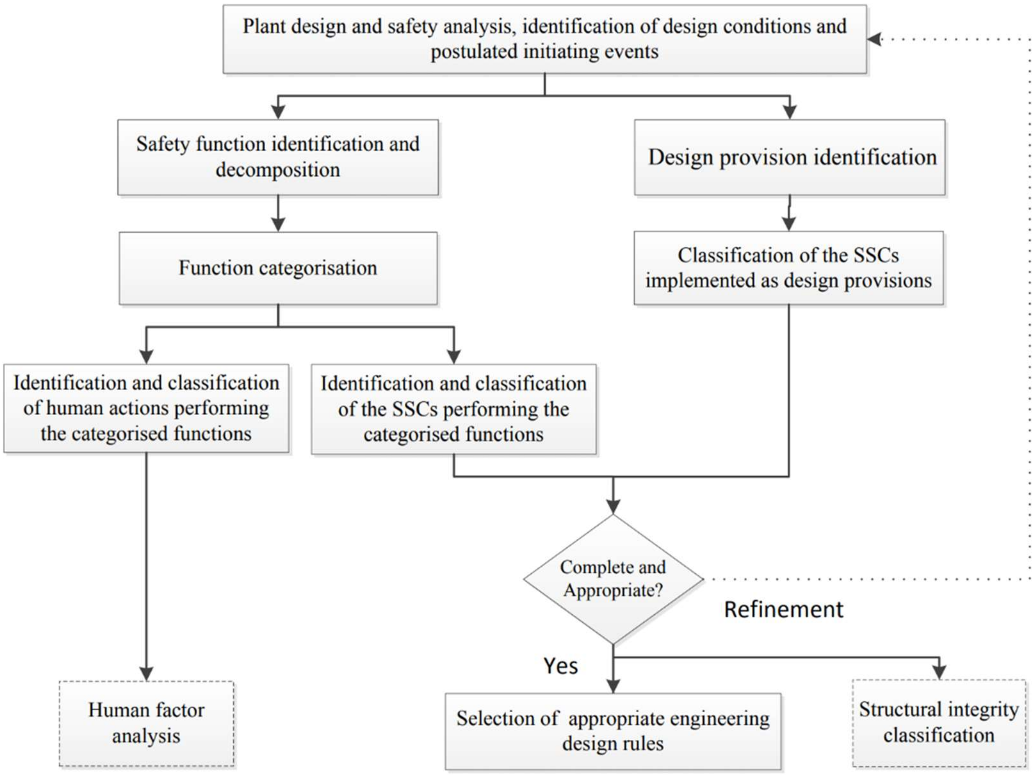

Figure 3: Requesting Party's safety categorisation and classification process overview

172. **Table 2** and **Table 3** below distinguish between the ONR and the RP's categorisation and classification terminology.

Table 2: Safety function category definitions

ONR Safety Function Categorisation basis	RP's Safety Function Category
Category A	FC1
Category B	FC 2
Category C	FC 3

Table 3: Structure, system or component classification definitions

ONR SSC Classification	RP's SSC Classification	RP's Design Provision Classification
Class 1	F-SC1	B-SC1
Class 2	F-SC2	B-SC2

ONR SSC Classification	RP's SSC Classification	RP's Design Provision Classification
Class 3	F-SC3	B-SC3

173. For the purposes of GDA, I consider the RP's "Methodology of Safety Categorising and Classification" (Ref. 47) satisfies:

- International guidance (Ref. 9) and (Ref. 46); and
- ONR guidance on Categorisation and Classification of SSCs, NS-TAST-GD-094 (Ref. 4).

  Note: ONR's guidance provides greater focus on preventing a fault occurring (defence in depth Levels 1 and 2) and thereby limiting the demand on protection measures.

174. However, I consider the RP's methodology was being incorrectly applied. Whilst its methodology requires a balance between preventative and protective safety measures to be implemented, no guidance is included as to how this will be undertaken. I consider that this has resulted in a lack of justification for its design decisions. Examples of shortfalls in this area are provided in the following sub-sections.

175. RO-UKHPR1000-0004 (Ref. 48) was raised in parallel to address gaps in the generic UK HPR1000 safety case. My Mechanical Engineering assessment has been used to inform its outcome.

176. The assessment of RO-UKHPR1000-0004 is detailed within the ONR Cross-Cutting report (Ref. 49).

4.2.1.2 UK HPR1000 Safety Function Requirement Traceability (Golden Thread)

177. During Step 3, the safety function traceability (golden thread) within the RP's safety case was unclear.

178. To show its approach to identifying safety functions and SSC classification, the RP produced its "Duty Schedule" (Ref. 50) and "ME Schedule" (Ref. 51) for the following SSCs:

- Safety Injection System (RIS) [SIS]
- Emergency Feed Water System (ASG) [EFWS]
- Main Control Room Air Conditioning System (DCL) [MCRACS]

179. These Mechanical Engineering SSCs (e.g. pumps, valves, heat exchangers and filters), were chosen as a sample given their nuclear safety significance.

180. I applied ONR SAP EKP.4 (Safety functions) and EKP.5 (Safety measures) against the RP's "Requirement Management Summary Report" (Ref. 52). Figure 4 shows the flow of information between the various schedules. This presents the RP's approach to safety case traceability (golden thread).

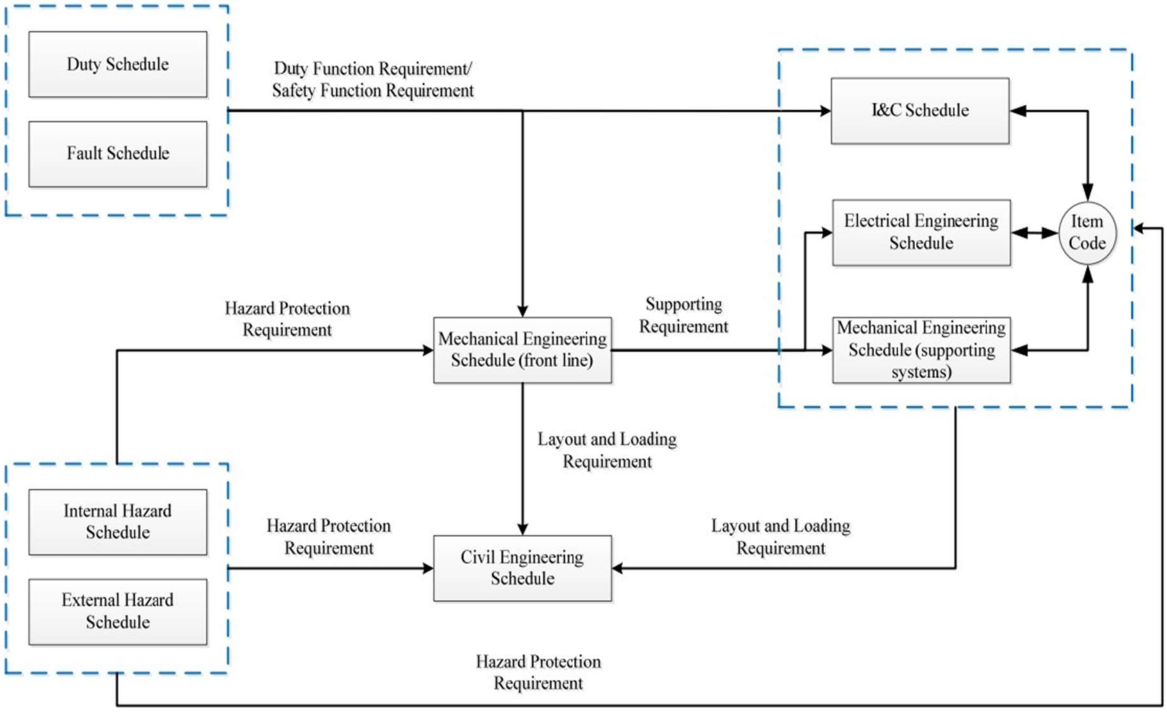

Figure 4: RP schedule interactions

181. The RP's various schedules use a coding system to link SSC performance requirements. The RP provided definitions of its coding system (see **Table 4**).

Table 4: UK HPR1000 function code definitions

Function Code	Function Code Definitions
FFR	Fault Function Requirements
SFR	Severe Accident Function Requirements
AFR	Assistant Safety Function Requirements. These are safety function requirements: ■ not included in either the fault schedule or the severe accident analysis; but ■ necessary in the implementation of the safety function requirements claimed in the fault schedule or severe accident analysis.
DFR	Duty Function Requirements
OFR	Other Function Requirements that are not related to safety

182. To show application of the coding system, ONR agreed that a sample be included within the safety case. The RP has committed to fully implement the coding system

during site-specific stages (see CM-SSER-0412 in the RP's "Post-GDA Commitment List" (Ref. 39)).

183. To confirm that safety functions for both normal operation (duty functions) and fault conditions were captured, I assessed the RP's "Duty Schedule" (Ref. 50) and "ME Schedule" (Ref. 51).

184. My assessment of these schedules identified gaps. These gaps included the:

- completeness of safety functions;
- identification of SSC performance requirements; and
- basis of SSC performance requirements.

185. RQ-UKHPR1000-1662 (Ref. 6) was raised to seek clarification.

186. The RP's response provided an ASG [EFWS] example that provided a:

- safety function description;
- unique safety function identification code (ASG-FFR-03); and
- link to the applicable transient analysis.

SSC Performance – Transient Analysis

187. ONR's Fault Studies inspector confirmed the RP's transient analysis was judged to be adequate (Ref. 53). This confirmed the support of the SSC performance requirements via the transient analyses.

SSC Performance – Engineering Design Basis

188. To assess the RP's SSC engineering design basis, I sampled the Safety Injection System (RIS) [SIS] Residual Heat Removal (RHR) heat exchanger. The heat exchanger's safety function is to cool the primary circuit during both normal and fault conditions. Normal reactor shutdown (duty function) is its most demanding performance condition i.e. thermal transfer (see RQ-UKHPR1000-1189 (Ref. 6)).

189. The ME Schedule (see (Ref. 51), part number RISi250EX) identified the RHR heat exchanger performance requirement as 8.963 MW. However, the RP could not show its engineering basis of design (design basis).

190. In a technical meeting (Ref. 7), when queried against the expectations of ONR SAP SC.4 (Safety case characteristics), the RP stated that:

- the reference plant (FCG3), and the engineering substantiation that supports it, provide the basis for the design; and
- the safety case did not reference the supporting engineering performance analysis.

191. To address this shortfall, the RP updated its safety case to reference its Mechanical Engineering design basis, but only for the sampled SSCs. This included updating its ME Schedule (Ref. 51) and SDMs. The RP provided reference to FCG3 data to support a sample of performance requirements. However, these documents were not formally part of my assessment.

192. The RP has justified its design basis through the RQ responses (for example in RQ-UKHPR1000-1697 and RQ-UKHPR1000-1189 (Ref. 6)). However, the RP was unable to provide the design basis for all my Mechanical Engineering sample (Annex 1).

Hence, I was unable to conclude that the design basis had been sufficiently demonstrated for my Mechanical Engineering sample.

193. I consider this a shortfall against ONR SAP SC.4 (Safety case characteristics). Detailed design information, beyond what was practicable during GDA, will be required to provide the demonstration. I have raised this as an Assessment Finding:

AF-UKHPR1000-0129: The licensee shall, during detailed design, produce a strategy and plan to justify the Mechanical Engineering design basis for all safety related systems and components. From this, information shall be provided for an agreed sample to address the following: ■ evidence validating performance requirements; ■ limits and conditions necessary in the interest of safety; ■ qualification and testing requirements; and ■ any other requirements necessary to meet or maintain the safety case, for example examination, inspection, maintenance and testing.

194. This Assessment Finding should be considered in conjunction with AF-UKHPR1000-0133 in sub-section 4.3.1 of this report.

195. The RP's arrangements for requirements capture are assessed within the ONR Cross-Cutting Report (Ref. 49), which raises related Assessment Findings.

Safety Function Requirement Traceability Conclusion

196. For safety case function traceability (golden thread), I consider the RP has:

- linked its various schedules (Figure 4); and
- applied unique identification codes for fault, duty and confinement safety functions.

197. However, I consider the RP has not sufficiently justified the Mechanical Engineering SSC design basis during GDA. This does not satisfy ONR SAP SC.4 (Safety case characteristics).

198. Given this gap, I have raised the Assessment Finding AF-UKHPR1000-0129.

4.2.1.3 Application of Categorisation and Classification Methodology – Safety Categorisation

199. In sub-section 4.2.1.1, I conclude that the RP's "Methodology of Safety Categorisation and Classification" (Ref. 47) is suitable. This sub-section details my assessment of its application for a sample of SSCs.

200. RGP associated with categorisation and classification includes:

- ONR SAPs (Ref. 2):
  - FP.6 (Prevention of accidents) considers that reasonably practicable steps must be taken to prevent and mitigate nuclear radiation accidents.
  - SC.4 (Safety case characteristics), which states the safety case should identify all the limits and conditions necessary in the interests of safety (operating rules).
  - EKP.3 (Defence in depth) considers the prevention of faults in the first instance.

- EKP.5 (Safety measures) considers the implementation of reliable and effective safety measures such that subsequent barriers need not be called upon.
- ECS.1 (Safety categorisation) considers safety categorisation of SSCs.

  Note: equipment providing the function to prevent propagation of failures should be assigned to the higher class.

- ECS.2 (Safety classification of structures, systems and components) considers the identification and safety classification of SSCs.
- EMC.21 (Safe operating envelope) considers that components and structures should be operated and controlled within defined limits and conditions (operating rules) derived from the safety case.
- ERC.1 (Design and operation of reactors) relates to confinement.
- NT.1 (Assessment against targets) considers targets from effective doses for any person arising from a design basis fault sequence associated with people on and off site.
- RP.7 (Hierarchy of controls) considers the optimisation of protection against dose to employees, in accordance with The Ionising Radiations Regulations 2017 (IRR17) (Ref. 54).

■ ONR's TAGs including:

- Guidance on Categorisation of Safety Functions and Classification of SSCs, NS-TAST-GD-094 (Ref. 4) states:
  - Focus should be on fault prevention.
  - Where not reasonably practicable, duty function class can be reduced in favour of the protection function class. Nevertheless, the principle of prevention remains and justification of reducing the duty function class is required in these circumstances.
  - Classification of earlier barriers, in the defence in depth hierarchy, should not take credit for later ones.
  - Doses should be based on unmitigated consequences.
- Guidance on Essential Services NS-TAST-GD-019 (Ref. 4). This suggests:
  - Focusing on preventing a fault occurring (defence in depth Levels 1 and 2).
  - Limiting the demand on protection measures.
  - The integrity of the essential services equipment supporting a preventative SSC should not be lowered simply because protective measures exist.
- Guidance on the Demonstration of ALARP NS-TAST-GD-005, Annex 2 which, for new reactor designs, expects the following four main areas to be addressed:
  - There is a clear conclusion that there are no further reasonably practicable improvements that could be implemented, and therefore the risk has been reduced to ALARP

  - RGP: the RP must set out the standards and codes used and justify them to the extent that we can ‘deem’ them RGP when viewed against our SAPs.
  - Options: firstly, an examination of the RP’s rationale for the evolution of the design, using its forerunners as a baseline, looking at why certain features were selected and others rejected and how this process has resulted in an improved design from a safety perspective. Secondly the RP needs to address the question “what more could be done?” and provide an argument of “why they can’t do it” (i.e. why it is not reasonably practicable).
  - Risk assessment: the use of risk targets in isolation is not an acceptable means of demonstrating ALARP and we expect to see risk assessments used to identify potential engineering and/or operational improvements as well as confirming numerical levels of safety.

- IAEA guidance:

  - IAEA SSR-2/1 (Ref. 11). This states that a “design shall be such as to ensure, as far as is practicable, that the first, or at most the second, level of defence is capable of preventing an escalation...”
  - IAEA SSG-30 (Ref. 9). This states that “for anticipated operational occurrences, in order to avoid ‘over-categorization’, the assessment of the consequences should be made with the assumption that all other independent functions are performed correctly and in due time…”
  - IAEA TECDOC 1787 (Ref. 46). This considers that to avoid SSC over-classification, the classification of SSCs performing both normal and fault safety functions can be made using judgement.

201. To assess the RP’s application of its categorisation and classification methodology (Ref. 47), against the RGP identified above, I sampled the:

- Reactor Coolant System (RCP) [RCS];
- Chemical Volume Control System (RCV) [CVCS]; and
- Spent Fuel Pool Crane hoist load path safety function classification.

202. This sample allowed me to assess the RP’s safety categorisation and classification of normal (duty) functions.

Reactor Coolant Pump Shaft Seal Injection Safety Categorisation and Classification

203. The reactor coolant pumps provide a cooling function to the reactor. The reactor coolant pump shaft seal (which I term ‘shaft seal’) fulfils an important role in confinement of radioactive material. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

204. When considering the ability of the shaft seal to deliver its safety function, I noted:

- The shaft seal is a Category A safety function (Ref. 55).
- On loss of both RCV [CVCS] injection water and Component Cooling Water System (RRI) [CCWS], the reactor coolant pump is shut down after two minutes (Ref. 56).

- The emergency shaft seal injection cooling safety function is Category B. The RP clarified this at a technical meeting in June 2021 (Ref. 7)
- The RCV [CVCS] system supplies the filtered shaft seal injection fluid and is a Category C safety function. The RP also clarified this at the technical meeting in June 2021 (Ref. 7)
- The RCV [CVCS] supports all three reactor coolant pumps via a common supply.

205. Figure 5 provides an overview of the RCV [CVCS] and shaft seal injection.

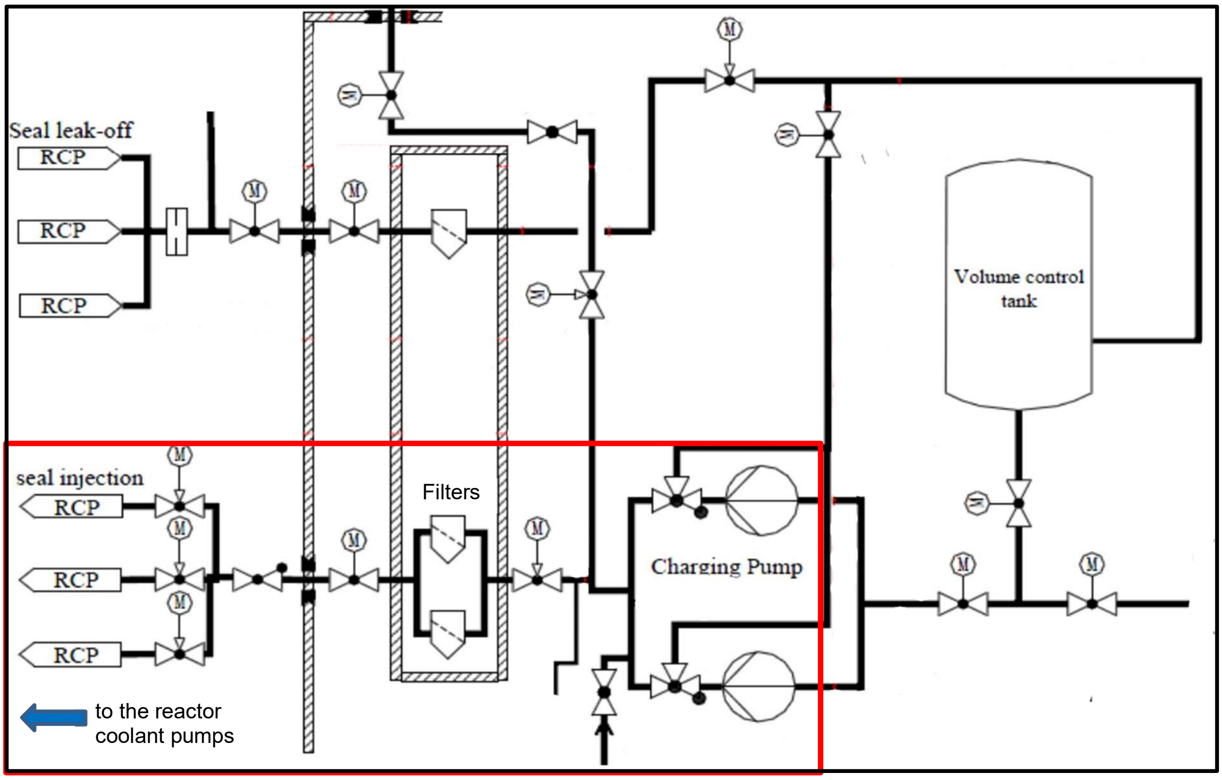

Figure 5: RCV [CVCS] reactor coolant pump shaft seal injection schematic

206. Figure 6 provides an overview of the shaft seal injection and its safety designation.

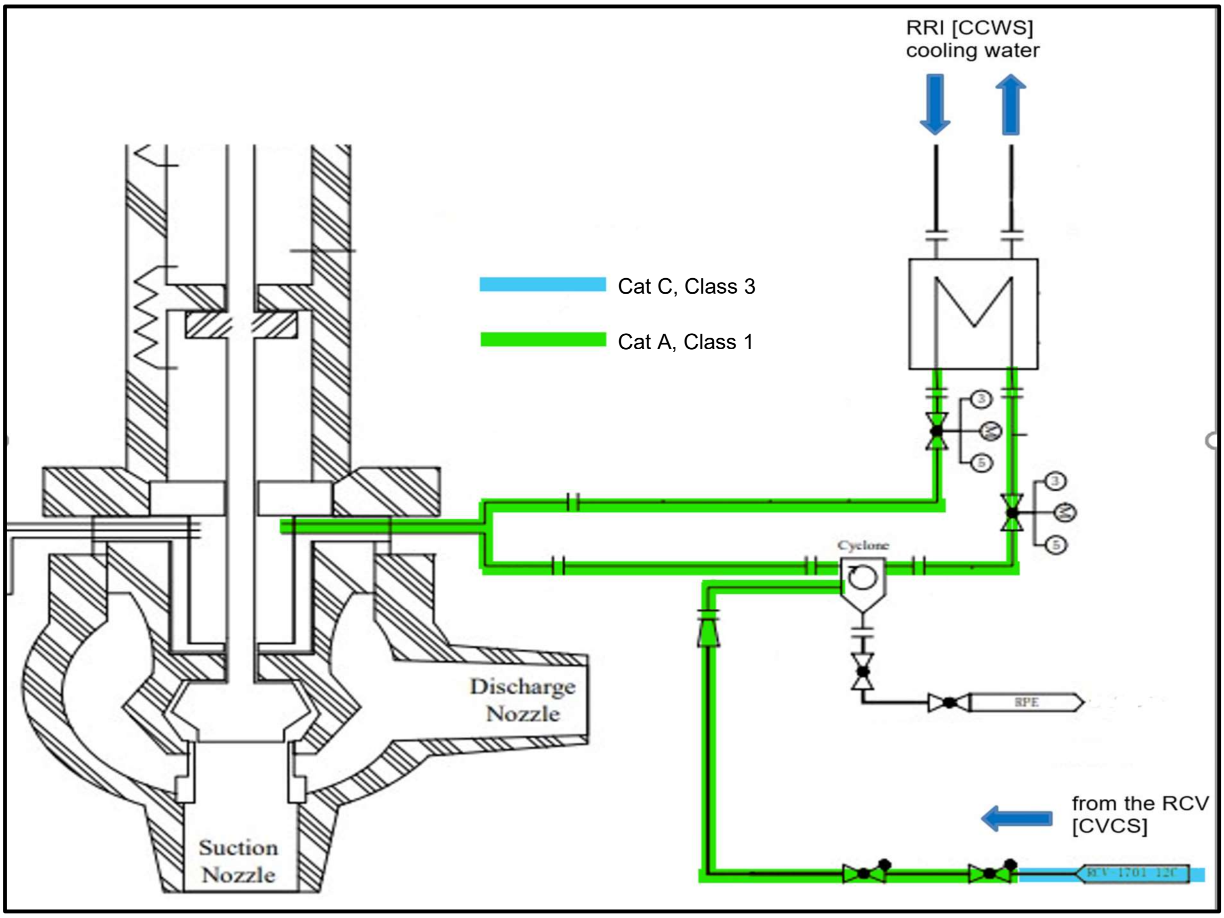

Figure 6: Shaft seal injection categorisation and classification

Integrity of the shaft seal

207. As noted, the RCV [CVCS] is designated as providing a Category C safety function. I queried the suitability of this given the integrity of the shaft seal is a Category A safety function.

208. During a technical meeting in May 2021 (Ref. 7) the RP explained its approach. Figure 7 details its decision-making process. Following this approach results in a ‘medium’ consequence if a Level 3 safety measure is successful.

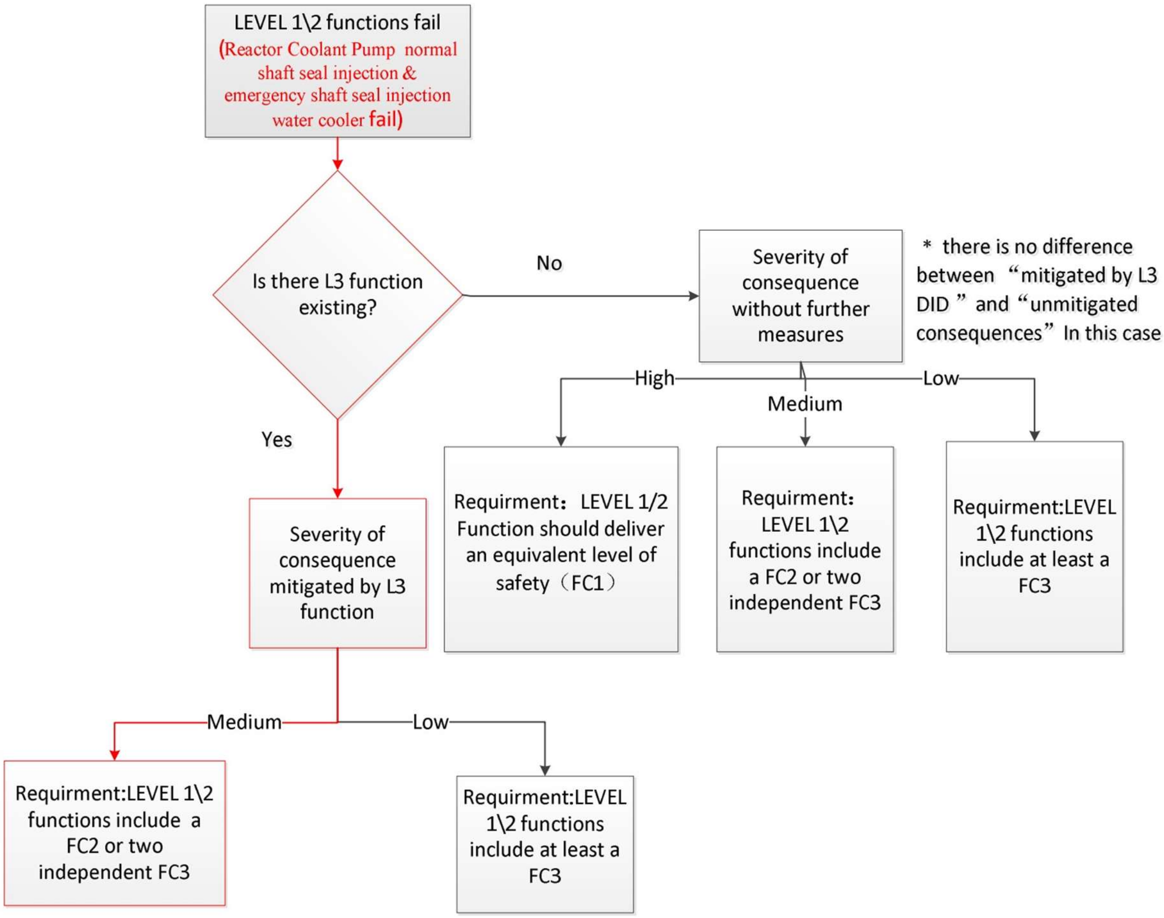

Figure 7: RCV [CVCS] reactor coolant pump seal injection safety function classification

209. Figure 8 details the shaft seal injection arrangement. The RP explained that upon loss of the RCV [CVCS] shaft seal injection function:

- A passive feed-screw on the reactor coolant pump maintains seal injection fluid flow.
- This flow cools the seal via the RRI [CCWS] heat exchanger at a reduced pressure.
- The filtration of the shaft seal injection is lost.
- The RIS [SIS] exists as a further Level 3 protection measure upon loss of seal integrity.

210. Hence upon loss of the RCV [CVCS], the original cooling and filtration safety functions are lost. The cooling function is maintained via the reactor coolant pump's feed-screw and the RRI [CCWS] heat exchanger.

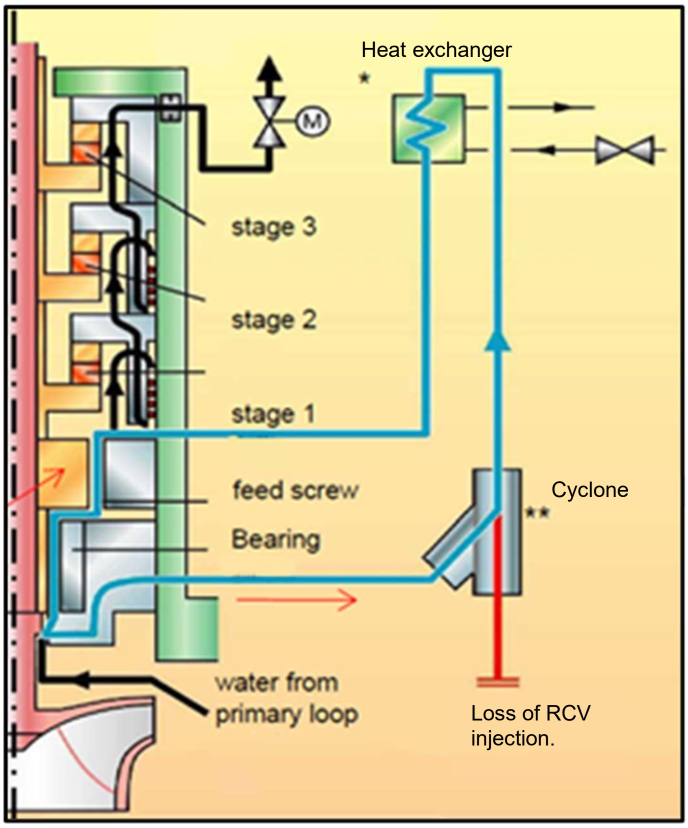

Figure 8: Reactor coolant pump closed-loop seal injection schematic

211. The "Reactor Coolant Pump Equipment Specification" (Ref. 56) states that the pump can operate with the following systems available:

- RCV [CVCS] and RRI [CCWS], which deliver seal injection cooling and filtration.
- RCV [CVCS] only, which delivers seal injection cooling and filtration.
- RRI [CCWS] only, which delivers seal injection cooling but filtration is lost.

Note: the feed-screw continuously operates providing flow.

212. I consider these systems to be essential services for the reactor coolant pump. I consider that for the reactor coolant pump seal to stay within its limits and conditions of safe operation and deliver its safety function, it should be cooled (to maintain the thermal barrier) and kept clean (to prevent damage). The only means to achieve the cooling and cleaning is via the RCV [CVCS].

213. One aspect of failure to clean the shaft seal injection fluid, is seal debris build up and degradation. The RP's safety case indicates that the reactor coolant pumps may operate in their degraded state for an 'undefined period' (Ref. 57). The consequences of losing the RCV [CVCS] is that the shaft seal may require replacing and may lead to a significant dose to the operator. Controlling dose to employees is a legal requirement under Regulation 9(2) of IRR17 (Ref. 54). First and foremost, this should be done via engineering means where reasonably practicable. I consider that the lack of defined limits and conditions for safe operation within the safety case is a shortfall against ONR SAPs:

- SC.4 (Safety case characteristics)
- EMC.21 (Safe operating envelope)
- ERC.1 (Design and operation of reactors)

- RP.7 (Hierarchy of control measures)

214. To conclude my review of the shaft seal integrity, upon loss of the RCV [CVCS] the RP has not justified:

- That the shaft seal's safety function can continue to be delivered. This is because upon RCV [CVCS] failure, the filtration function is lost.
- The duration that the reactor coolant pump can operate without compromising its safety function.

215. I consider this to be a shortfall against ONR SAPs:

- EKP.5 (Safety measures).
- SC.4 (Safety case characteristics)
- EMC.21 (Safe operating envelope)
- ERC.1 (Design and operation of reactors)
- RP.7 (Hierarchy of control measures)

216. I have therefore raised this within Assessment Finding AF-UKHPR1000-0134.

<u>Evidence supporting the categorisation and classification of mechanical equipment</u>

217. As identified above, the RCV [CVCS] provides an essential service (cooling and filtration) to the reactor coolant pump. I sought evidence supporting the RCV [CVCS] categorisation and classification.

218. ONR does not prescribe a particular categorisation and classification methodology for the RP to follow. However, I have used ONR's guidance to inspectors, relevant to this topic, to consider the adequacy of the RP's approach (see paragraph 200). This includes the following guidance within ONR's TAGs:

- The integrity (i.e. safety classification) of essential services, supporting preventative measures, not to be lowered simply because a protective measure exists (see NS-TAST-GD-019).
- For SSCs delivering preventative functions, as part of normal operation they should initially be considered as a principal means of delivering the safety function (see NS-TAST-GD-094).
- Where the safety classification of a preventative measure is lowered due to a protective measure, an ALARP justification is required (see NS-TAST-GD-094).

219. I noted the RP's categorisation and classification methodology (Ref. 47) requires:

- the balance between prevention and protection to be considered; and
- consideration of a preference for prevention over protection systems.

220. In the scenario described above (see paragraph 204), the following systems support the delivery of the reactor coolant pump sealing function (Category A):

- RCV [CVCS] is a Category C safety function (cooling and filtration safety function)
- RRI [CCWS] is a Category B safety function (cooling safety function)
- Reactor coolant pump's feed screw is a Category B safety function (supports the cooling safety function) – I have inferred this from the classification of the heat exchanger as it is not clearly identified in the RP's documentation.

221. I could not identify where the RP had considered the balance between prevention and protection in its design choices for the shaft seal injection function. This shortfall is discussed in paragraph 174.

222. I have identified the Class 3 RCV [CVCS] as the primary means of supporting the delivery of the shaft seal's Category A safety function. This is because it is the only system that is currently capable of cleaning and cooling the shaft seals. The RCV [CVCS] supplies, cools and filters the seal injection fluid.

223. From a Mechanical Engineering perspective, the importance of SSCs in delivering safety categories is identified in Figure 9 below.

		Prominence of the SSC in the		
		Principal means	Significant means	Other means
	Category A	Class 1	Class 2	Class 3
	Category B	Class 2	Class 3	
	Category C	Class 3		

Figure 9: Table 3 from NS-TAST-GD-094 – Initial SSC classification

224. As identified above, the principal means of delivering a Category A safety function is normally via a Class 1 SSC. From ONR's guidance, an SSC making a significant contribution to fulfilling a Category A safety function should be Class 2.

225. To conclude, RP has not provided suitable evidence to support whether:

- the RCV [CVCS] safety category (Category C) is suitable to support delivery of the shaft seal Category A safety function; and
- reasonably practicable measures exist to increase the reliability of the safety related systems delivering shaft seal integrity.

226. I consider this to be a shortfall against ONR SAPs:

- EKP.5 (Safety measures);
- ECS.1 (Safety categorisation); and
- ECS.2 (Safety classification of structures, systems and components).

227. I have therefore raised this in Assessment Finding AF-UKHPR1000-0130.

<u>Conclusion</u>

228. For the shaft seal injection safety function, the RP has been unable to show:

- That it has suitably applied its own categorisation and classification methodology (see paragraphs 217 and 219).
- That the seal can maintain its safety function upon loss of the RCV [CVCS] (see paragraph 222).
- Whether the RCV [CVCS] can support delivery of the shaft seal's Category A safety function (see paragraph 225).

229. I have therefore raised these within Assessment Findings AF-UKHPR1000-0130 and AF-UKHPR1000-0134.

Spent Fuel Pool Crane Hoist Load Path Safety Categorisation and Classification

230. My assessment of the Spent Fuel Pool Crane (SFPC) considered application of dose consequences in its classification.

231. Sub-chapters 4.10 and 4.11 of this report consider lifting equipment classification. These identify:

- associated RGP;
- safety categorisation and classification shortfalls; and
- an Assessment Finding to manage the shortfalls.

232. The RP's "Classification of the Typical Cranes" (Ref. 58) references on-site radiological consequences. These consequences include SFPC hoist failures (Ref. 59). I identified the following shortfalls:

- The use of mitigated rather than unmitigated consequences was not explained. This may lead to incorrect SFPC safety categorisation.
- The incorrect radiological consequence has been used to derive the hoist safety classification. This could lead to an incorrect classification.

233. The RP's "Summary of the Fuel Route Safety Case" (Ref. 60) indicates the use of its HVAC system to reduce off-site dose during fuel handling accidents. I note the following shortfalls:

- I consider the HVAC system to be a Level 4 mitigation in this scenario (ONR SAP EKP.3 (Defence in depth)). Note the RP's categorisation and classification methodology (Ref. 47) requires a Level 3 protection measure.
- The RP uses the HVAC system to reduce the off-site radiological consequences of a SFPC hoist load path failure (ONR SAP NT.1 Target 4 – Design basis fault sequences – any person). This reduces the SFPC hoist load path safety function category.

<u>Conclusion</u>

234. I judge that the SFPC hoist load path may have been incorrectly safety categorised and classified. This is because the RP has not used suitable radiological consequences. The licensee should use unmitigated radiological consequences to derive the lifting equipment's safety category. During detail design, this safety category should be used to inform the lifting equipment's safety classification.

235. I consider this to be a shortfall against ONR SAP NT.1 Target 4.

236. I have therefore raised this within Assessment Finding AF-UKHPR1000-0130.

Application of Categorisation and Classification Methodology Conclusion

237. To conclude, I accept that the RP's methodology aligns with RGP. However, I have identified the following shortfalls in its application:

- For the reactor coolant pump shaft seal safety function, the RP has not provided suitable evidence:
  - That it has correctly applied its own safety categorisation and classification methodology (see paragraphs 217 and 219).

  - That the seal can maintain its safety function upon loss of the RCV [CVCS] (see paragraph 225).
  - Whether the RCV [CVCS] can support delivery of the shaft seal's Category A safety function (see paragraph 225).
- When designing lifting equipment, the RP has not shown the use of unmitigated radiological consequences to identify the correct safety category.

238. I consider these to be shortfalls against the following ONR SAPs:

- EKP.3 (Defence in depth)
- ECS.1 (Safety categorisation)
- ECS.2 (Safety classification of structures, systems and components)
- SC.4 (Safety case characteristics)
- EMC.21 (Safe operating envelope)
- ERC.1 (Design and operation of reactors)
- NT.1 (Assessment against targets)

239. Given the above shortfalls, I have raised the following Assessment Finding. This is because, during site-specific stages, the licensee will need to develop and implement its own categorisation and classification arrangements:

AF-UKHPR1000-0130: The licensee shall, during site-specific stages, produce a strategy and plan to demonstrate suitable application of its safety categorisation and classification arrangements for Mechanical Engineering systems and components. From this, information shall be provided for an agreed sample to demonstrate how the licensee:

- where reasonably practicable, prioritises prevention over protection in its application of defence in depth; and
- considers unmitigated radiological consequences when categorising safety functions.

240. The specific qualification aspects of the shaft seal injection and its supporting systems are captured with Assessment Finding AF-UKHPR1000-0134 in sub-section 4.3.1.

4.2.1.4 Mechanical Engineering Schedule SSC Assessment

241. I assessed the following Mechanical Engineering equipment, which was chosen given their importance to nuclear safety.

Emergency Feedwater System (ASG) [EFWS] Containment Isolation Valves

242. The ASG [EFWS] containment isolation valves' functions are to:

- prevent back flow from the Steam Generator (SG) to the ASG [EFWS] during normal operations (Category A / Class 1);
- allow ASG [EFWS] to SG flow during a range of accident conditions;
- allow commissioning tests to be undertaken; and
- fulfil an important confinement and support cooling during normal operation and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant here.

243. ASG [EFWS] containment isolation valve RGP for the ME Schedule includes ONR SAPs:

- EHA.5 (Design basis event operating states) considers the potential impact of the design basis hazards on SSCs.
- EMC.25 (Leakage) considers the means to detect, locate, monitor and manage leakage.
- EMT.6 (Reliability claims) considers EIMT provisions for SSCs through life.
- ERC.1 (Design and operation of reactors) considers radioactive material confinement.

244. I applied ONR SAP EHA.5 (Design basis event operating states) against the ASG [EFWS] containment isolation check valve design (Ref. 61) and (Ref. 62). I noted that environmental conditions were not suitably considered. RQ-UKHPR1000-1289 was raised to seek clarification.

245. The RP responded that:

- accident conditions, including thermal and radiation exposures, are derived from Design Basis Analysis (DBA) and Severe Accident Analysis (SAA);
- relevant calculations were in progress; and
- the design will be assessed against these parameters to show SSCs can deliver their performance requirements.

246. I consider this response acceptable. This is subject to considering the environmental conditions when they are available. I have identified this as a Minor Shortfall as site-specific data is required.

247. Valve flow coefficient is a key technical parameter. This impacts valve pressure drop for a given flow rate. I noted the use of imperial valve flow coefficient parameters in the safety case (Ref. 63) alongside metric parameters. RQ-UKHPR1000-1290 (Ref. 6) was raised to seek clarification.

248. The RP confirmed that the imperial term was widely used in the reference power station's (FCG3) data sheets. It agreed to use metric units early in Step 2 of GDA. I consider this acceptable for GDA. However, I have raised the use of both units as a Minor Shortfall. Using both metric and imperial units may lead to avoidable error traps. Hence, I consider it appropriate for the licensee to consider as it is a GDA requirement (Ref. 1).

249. I applied ONR SAP EMT.6 (Reliability claims) and EMC.25 (Leakage) against the safety case (Ref. 64). It was unclear how containment isolation check valve surveillance was achieved. RQ-UKHPR1000-RQ1290 (Ref. 6) was raised to seek clarification.

250. The RP responded that:

- pressure and temperature instrumentation monitored the check valve seal;
- this instrumentation would initiate an alarm if normal temperature and pressure conditions were exceeded; and
- elevated temperature and pressure would infer check valve seal leakage.

251. I consider this response acceptable.

252. I applied ONR ERC.1 (Design and operation of reactors) against the “Requisition and List for Nuclear Island Isolation Valves” (Ref. 65). I noted that it did not include the requirement for valve stem sealing. To maintain containment isolation, I considered valve stem leakage should be prevented. RQ-UKHPR1000-1290 and RQ-UKHPR1000-1717 (Ref. 6) were raised to seek further clarification.

253. The RP acknowledged that the safety case would be updated to include the valve stem sealing requirement. I consider this response suitable and have raised this as a Minor Shortfall for the licensee to consider.

254. For ASG [EFWS] containment valves, although I have identified Minor Shortfalls, I consider the RP has considered:

- Performance requirements from design basis hazards. This satisfies ONR SAP EHA.5 (Design basis event operating states).
- How through-life EIMT and identification of leaks will be achieved. This satisfies ONR SAPs:
  - EMT.6 (Reliability claims); and
  - EMC.25 (Leakage).
- Radiological material confinement. This satisfies ONR SAP ERC.1 (Design and operation of reactors).

Secondary Passive Heat Removal System (ASP) [SPHRS] Condenser

255. The ASP [SPHRS] condenser:

- has a safety function to remove heat from the primary circuit, via the secondary system, in fault conditions following ASG [EFWS] failure (Category C / Class 3); and
- fulfils an important cooling role during accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

256. ASP [SPHRS] condenser RGP for the ME Schedule includes ONR SAPs:

- ERL.4 (Margins of Conservatism) considers SSC design conservatism.
- ECS.5 (Use of experience, test or analysis) considers use of SSC testing in the absence of codes and standards.
- EHT.2 (Coolant inventory and flow) considers sufficient coolant inventory and flow.

257. The ASP [SPHRS] uses three condensers (one per train) that:

- are located within a common water tank; and
- continuously remove heat for 72 hours following loss of SG main and emergency feedwater.

258. I considered that the sizing basis of the ASP [SPHRS] condenser and tank were unclear and not identified in the safety case (Ref. 63) and (Ref. 66). RQ-UKHPR1000-1154 (Ref. 6) was raised to seek clarification.

259. The RP’s response clarified:

- the condenser capacity;

- the maximum thermal demand on the condenser (depending upon conservatisms) is 16.7% less than capacity; and
- tank inventory is calculated based on:
  - an operating duration considering decay heat power uncertainty; and
  - a conservative water temperature.

260. Whilst conservatism is applied to the design of the ASP [SPHRS] condenser, the basis has not been justified. I consider this a design basis shortfall against ONR SAPs:

- ECS.5 (Use of experience, tests or analysis); and
- ERL.4 (Margins of conservatism).

261. This design basis shortfall is already captured within Assessment Finding AF-UK HPR1000-0129.

Containment Heat Removal System (EHR) [CHRS] Containment Heat Removal Pump

262. The EHR [CHRS] containment heat removal pump:

- has a safety function to reduce containment temperature and pressure during fault, accident and severe accident conditions (Category C / Class 3); and
- fulfils an important cooling role during accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

263. EHR [CHRS] RGP for the ME Schedule includes ONR SAPs:

- ERL.4 (Margins of conservatism) considers SSC design conservatism.
- EDR.2 (Redundancy, diversity and segregation) considers whether suitable SSC reliability has been achieved.
- EDR.3 (Common cause failure) considers reliability of SSCs.
- EHT.1 (Design) considers suitability of heat transport systems.
- SC.2 (Safety case process outputs) considers suitability of access to safety case information.

264. I applied ONR SAPs ERL.4 (Margins of conservatism) and EHT.1 (Design) to the EHR [CHRS] safety case (Ref. 67). I considered the EHR [CHRS] performance requirements were unclear. RQ-UKHPR1000-1260 and RQ-UKHPR1000-1580 (Ref. 6) were raised to seek clarification.

265. The RP explained that the calculated EHR [CHRS] flowrate contained the following uncertainties:

- Measurements (2%)
- Electrical grid frequencies (1%)
- General engineering conservatisms (7%)

266. I consider the basis of these margins of conservatism to be unclear. This a shortfall against ONR SAP ERL.4 (Margins of conservatism) and EHT.1 (Design). This design basis shortfall is already captured within Assessment Finding AF-UK HPR1000-0129.

267. I applied ONR SAP SC.2 (Safety case process outputs) to the EHR [CHRS] back-flushing safety case (Ref. 68). I could not identify the method of back flushing the strainer. RQ-UKHPR1000-1580 (Ref. 6) was raised to seek clarification.

268. The RP responded by including a schematic (Figure 10) within its safety case (Ref. 69).

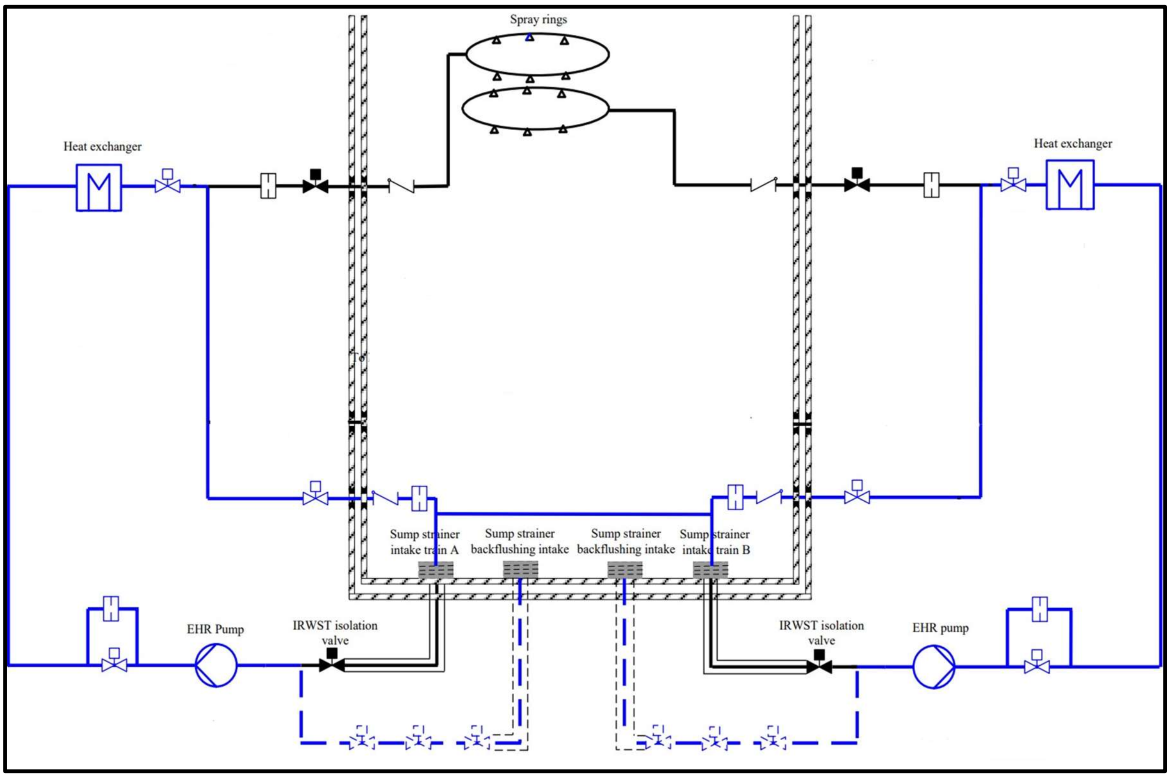

Figure 10: EHR [CHRS] back-flushing schematic

269. I consider that adding this schematic sufficiently explains the back-flushing arrangement.

270. When applying EDR.2 (Redundancy, diversity and segregation) and EDR.3 (Common cause failure) to the EHR [CHRS] arrangements, I noted:

- the EHR [CHRS] and RIS [SIS] pumps are supplied by independent but similar strainers in the In-Containment Refuelling Water Storage Tank (IRWST);
- the RIS [SIS] system is used to back-flush the EHR [CHRS] in the event of blockage; and
- a blocked RIS [SIS] strainer may prevent back-flushing of the EHR [CHRS] strainer.

271. Given the similarity between the EHR [CHRS] and RIS [SIS] strainer design, and shared IRWST location, I considered resilience to Common Cause Failure (CCF) had not been shown. RQ-UKHPR1000-1580 (Ref. 6) was raised to seek clarification.

272. The RP responded:

- The RIS [SIS] strainers respond to Design Basis Condition (DBC) accidents.
- The EHR [CHRS] strainers respond to Design Extension Conditions (DEC).
- As their operating conditions are independent, they will not be blocked at the same time.

- Changes to use Reflective Metallic Insulation (RMI) in the reactor building will reduce the likelihood of fibrous material strainer blockage.

273. Given that DEC follow DBC, I consider the likelihood of both EHR [CHRS] and RIS [SIS] strainer blockage is high. Hence, EHR [CHRS] strainer back-flushing would not be possible if the RIS [SIS] strainers are blocked. This does not only relate to RMI but could occur due to debris from several sources, given the feed is from the sump.

274. This does not satisfy ONR SAPs EDR.2 (Redundancy, diversity and segregation) and EDR.3 (Common cause failure). I consider that licensee design choices are required to address this shortfall. The Fault Studies Assessment Report (Ref. 70) discusses the strainers from a fault analysis perspective. Within the report, the Fault Studies inspector has raised an Assessment Finding in relation to optimisation of the IRWST filtration system. I consider that this captures the identified shortfalls (see paragraph 273).

275. For the EHR [CHRS] system, I consider the RP has provided suitable information to explain its function. This satisfies ONR SAP SC.2 (Safety case process outputs).

Containment Leak Rate Testing and Monitoring System (EPP) [CLRTMS] Equipment Access Hatch

276. The Equipment Access Hatch (EAH):

- provides reactor building access for equipment required for outage work during shutdown;
- during all other operational and accident scenarios, the hatch's safety function is to remain closed to maintain the containment building pressure boundary (Category A / Class 1); and
- fulfils an important confinement role during all normal and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant as it:
    - maintains external leak tightness; and
    - limits radionuclide release to the environment.

277. EAH RGP for the ME Schedule includes:

- ONR SAP ECV.3 (Means of confinement) considers containment systems limits and conditions of safe operation; and
- NS-TAST-GD-035 (Ref. 4) Limits and Conditions for Nuclear Safety (Operating Rules), which provides guidance regarding operational safety limits and conditions implemented at nuclear facilities.

278. During a severe accident, the EAH confines radioactive material inside the containment building under elevated pressures and temperatures. I noted conflicting EAH performance requirements in the safety case in Revision A of the SDM (Ref. 71) and Revision B of the Equipment Specification (Ref. 72). RQ-UKHPR1000-1066 (Ref. 6) was raised to seek clarification.

279. The RP confirmed the correct design pressure and temperature of the EAH. It then updated the safety case in Revision C of the SDM (Ref. 71). These values represent the limits and conditions of safe operation for the EAH.

280. For the EAH, I consider the RP has shown suitable limits and conditions of safe operation. This satisfies:

- ONR SAP ECV.3 (Means of confinement); and
- ONR TAG NS-TAST-GD-035 Limits and Conditions for Nuclear Safety (Operating Rules).

Main Control Room Air Conditioning System (DCL) [MCRACS] HEPA Filters

281. The DCL [MCRACS] HEPA filters:

- have a safety function to limit the radiological contamination carried to the MCR during accident conditions (Category B / Class 2);
- limit air borne particulate in the MCR during normal operations; and
- fulfil an important confinement role during accident conditions in limiting radionuclide contamination of the MCR. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

282. DCL [MCRACS] RGP for the ME Schedule includes:

- ONR SAP ECV.3 (Means of confinement) considers the establishment of limits and conditions (operating rules) for containment systems.
- ONR guidance on Ventilation, NS-TAST-GD-022 (Ref. 4), which considers the control and spread of contamination during normal, fault and post-accident conditions.

283. For the DCL [MCRACS] HEPA filters, the safety case link (golden thread) between safety functions and SSC performance requirements was unclear. Hence, the limits and conditions of safe operation relevant to the HEPA filter were not defined (Ref. 73). RQ-UKHPR1000-0644 (Ref. 6) was raised to seek clarification.

284. The RP stated that the DCL [MCRACS] filters' safety function required:

- removal of radioactive material from the MCR air supply; and
- was identified as a Category B Safety Function (with identification code DCL-E-02-R3).

285. I consider the RP's response identifies an appropriate DCL [MCRACS] safety function. However, I noted:

- The associated coding (DCL-E-02-R3) is inconsistent with the RP's "Confinement Schedule" (Ref. 74) and ME Schedule (Ref. 51).
- The MCR radiological limits and conditions of safe operation were not identified. This information is required to identify the HEPA filter performance requirements.

286. I consider that the RP's inconsistent application of a coding system is a Minor Shortfall. This is because it does not undermine my confidence in the safety of the generic design. In addition, the RP has already committed to fully implement the coding system during site-specific stages (see CM-SSER-0412 in the RP's "Post-GDA Commitment List" (Ref. 39)).

287. I consider that the failure to identify MCR radiological limits and conditions of safe operation, to be a shortfall against ONR SAP ECV.3 (Means of confinement). To design the containment system, the licensee should fully understand the safe limits

and conditions of operation. I have incorporated the limits and conditions aspect of this within Assessment Finding AF-UKHPR1000-0129.

Reactor Coolant System (RCP) [RCS] Reactor Coolant Pump

288. The reactor coolant pump:

- has a safety function to supply coolant flow to transfer thermal power from the reactor core to the SGs (Category A / Class 1); and
- fulfils an important cooling role and supports confinement during normal operation. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

289. Reactor coolant pump ME Schedule RGP includes:

- ONR SAPs:
  - ECS.2 (Safety classification of structures, systems and components) considers appropriate SSC classification to prevent propagation of failures;
  - ERL.4 (Margins of conservatism) considers conservatism in SSC design;
  - EHT.2 (Coolant inventory and flow) considers sufficient coolant inventory and flow; and
  - ECV.1 (Prevention of leakage) considers the containment of radioactive material.
- Industry guidance:
  - ANSI/HI 9.6.1-2017 (Ref. 75) including, Available Net Positive Suction Head (NPSH-A) and Required Net Positive Suction Head (NPSH-R).

Reactor Coolant Pump ME Schedule Assessment: Performance Requirements

290. I applied ONR SAPs ERL.4 (Margins of conservatism) and EHT.2 (Coolant inventory and flow) to the reactor coolant pump performance (Ref. 76).

291. Industry guidance (Ref. 75) recommends that:

- suitable Net Positive Suction Head (NPSH) margins for rotodynamic pumps are identified; and
- coolant pump NPSH-A (available) should be greater than its NPSH-R (required) for electric power generation.

292. I noted the RP's safety case:

- was unclear regarding the NPSH-R value;
- was unclear regarding the heat removal margin relating to the specified flowrates and output pressure head; and
- stated that the reactor coolant pump provides a best efficiency point (BEP) flowrate of 25,450 m^3/h at an output pressure head of 88.2 m.

293. RQ-UKHPR1000-0963, RQ-UKHPR1000-1064, RQ-UKHPR1000-1534 and RQ-UKHPR1000-1697 (Ref. 6) were raised to seek clarification.

294. The RP responded stating the:

- Highest NPSH-R value is approximately 50% of the NPSH-A, which is a sufficient margin.
- reactor coolant pump optimum flow condition (Best Estimate) is circa 25,450 m^3/h per loop (fixed speed pump).
- Primary circuit hydraulic loads are calculated using a Mechanical Engineering flowrate of 26,500 m^3/h per loop.
- Accident analysis thermal (TH) flowrate is 24,000 m^3/h per loop.

295. **Table 5** provides the safe margin approximations presented by the RP.

Table 5: reactor coolant pump flowrate margins

Flowrate Definition	Flowrate Value m^3/h per loop	Safe Margin to BE Flowrate
Mechanical Engineering (ME) flowrate	~ 26,500	Approximately 4%
Best Estimate (BE) flowrate	~ 25,450	Reference point
Thermal (TH) flowrate	~ 24,000	Approximately 6%

296. **Table 5** shows estimated safety margins for the reactor coolant pump loop flowrates. As shown the reactor coolant pump BE flowrate has:

- ~ 6% increased flowrate compared with that used to determine thermal performance of the primary circuit; and
- ~ 4% reduced flowrate compared with that used to calculate mechanical loads within the primary circuit.

297. I consider that **Table 5** shows sufficient primary circuit flow margin. This satisfies ONR SAPs EHT.2 (Coolant inventory and flow) and ERL.4 (Margins of conservatism). Demonstration of the reactor coolant pump performance will be provided during site-specific stages by the licensee. I consider this to be captured in Assessment Findings AF-UKHPR1000-0133 and AF-UKHPR1000-0134.

Reactor Coolant Pump ME Schedule Assessment: Mechanical Seal Leakage

298. I applied ONR SAPs ECV.1 (Prevention of leakage) and EHT.2 (Coolant inventory and flow) to my assessment of the reactor coolant pump mechanical seal. The reactor coolant pump incorporates a three-stage mechanical seal. The following information was unclear:

- The engineering basis of the seals’ performance requirements.
- The limits and conditions of safe operation.

299. RQ-UKHPR1000-0985 (Ref. 6) was raised to seek clarification.

300. The RP responded that:

- The leakage limit is derived using CFD.
- The CFD analysis conservatively reflects the reactor coolant pump seal flow restrictions and behaviour.
- Loss of primary circuit inventory through seal leakage can be compensated by the:
  - Chemical Volume Control System (RCV) [CVCS]; and
  - Safety Injection System (RIS) [SIS].
- reactor coolant pump seal leakage is collected by the Nuclear Island Vent and Drain System (RPE) [VDS].

301. I note that the:

- RP claims the RPE [VDS] tanks and sumps are sized to avoid effluents overflow under maximum flow conditions (Ref. 77); and
- the RPE [VDS] sump pump capacity is circa 65% of the maximum reactor coolant pump seal leakage rate.

302. I consider the RPE [VDS] pump capacity does not satisfy ONR SAP ECV.1 (Prevention of leakage). This should be considered during detailed design. I have therefore raised an Assessment Finding:

AF-UKHPR1000-0131: The licensee shall demonstrate, during detailed design, that the capacity of the Nuclear Island Vent and Drain System sump pump is sufficient to ensure that the tanks do not overflow.

Reactor Coolant System (RCP) [RCS] Severe Accident Dedicated Valves

303. The Severe Accident Dedicated Valves (SADVs):

- have a safety function to depressurise the Reactor Coolant System (RCP) [RCS], by opening in severe accident conditions (Category C / Class 3);
- have a safety function to maintain the pressure boundary in normal operations (Category A / Class 1); and
- fulfil an important role protecting the primary circuit from over-pressurisation during severe accidents. ERC.1 (Design and operation of reactors) is relevant.

304. Figure 11 and Figure 12 show the SADV layout.

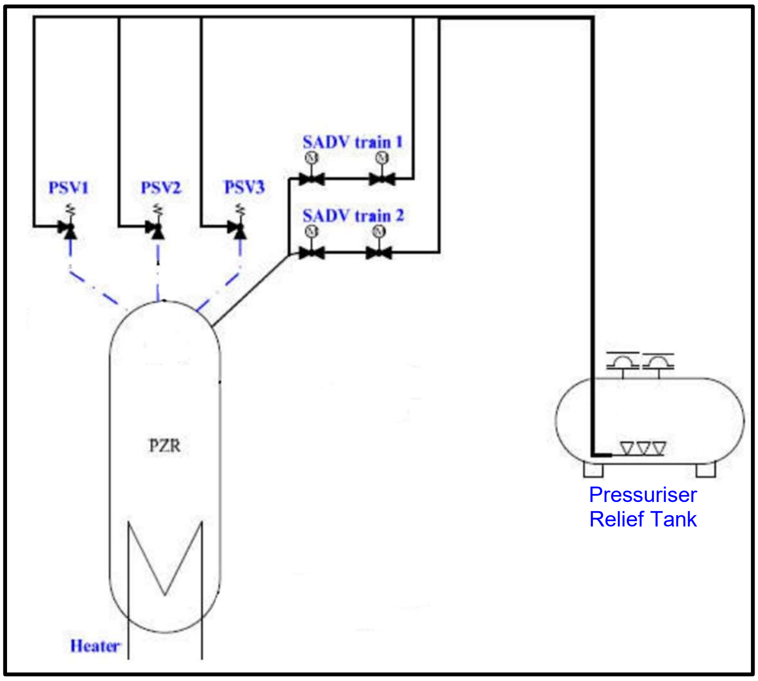

Figure 11: UK HPR1000 Pressuriser Safety Valves and SADV schematic

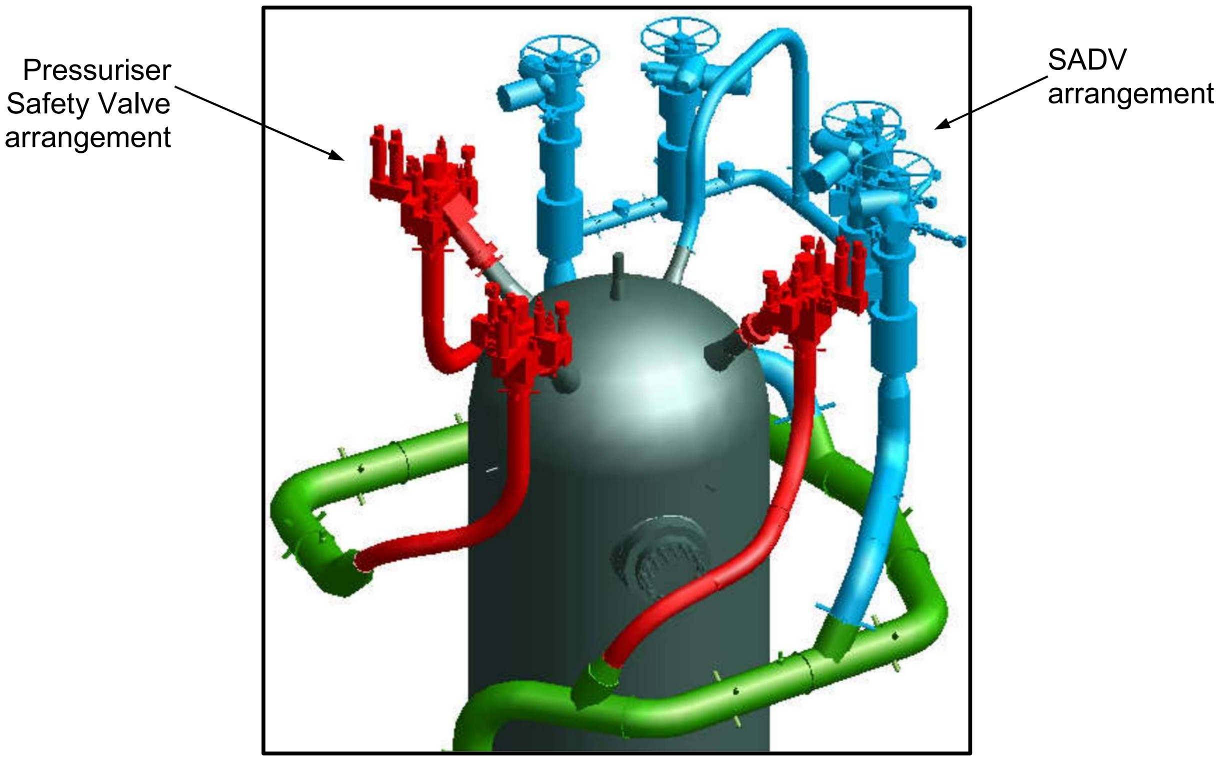

Figure 12: Pressuriser Safety Valve (red) and SADV (blue) arrangement

305. SADV RGP for the ME Schedule includes:

- ONR SAP ECS.3 (Codes and standards) considers application of appropriate codes and standards; and
- ONR's Severe Accident Analysis TAG NS-TAST-GD-007 (Ref. 4) considers suitable SSC severe accident qualification and substantiation (see NS-TAST-GD-007 paragraph 5.51).

306. The SADV specifications (Ref. 57) and (Ref. 78) did not clearly identify how the following temperature parameters were used in the design:

- Normal operating temperature
- Design temperature
- Temperature for valve opening
- Maximum operating temperature to remain open during severe accidents

307. RQ-UKHPR1000-1347 (Ref. 6) was raised to seek clarification. The RP clarified the:

- temperature at which the SADVs operate;
- temperature at which the SADVs must remain open (maximum operating temperature), which is circa four times the design temperature;
- reference plant (FCG3) supplier has shown, by analysis, that SADVs remain open at the maximum operating temperature;
- design temperature complies with RCC-M B3132.2 (Ref. 79); and
- SADVs' 'water plug' limits the inlet temperature to circa 20% of the design temperature during normal operations.

308. I noted that the RP has used a superseded standard (RCC-M 2007) (Ref. 79) in its response. I have identified this as a Minor Shortfall against ECS.3 (Codes and standards). The licensee may address this shortfall during site-specific stages.

309. For the SADVs, I consider the RP has shown its understanding of the predicted environmental temperatures (including harsh environments). This satisfies ONR's Severe Accident Analysis TAG (Ref. 4).

Reactor Coolant System (RCP) [RCS] Control Rod Drive Mechanism

310. The Control Rod Drive Mechanisms (CRDMs):

- have a safety function which contributes to reactivity control during normal, fault and accident conditions (Category A / Class 1);
- release the Rod Control Cluster Assembly (RCCA), following a Postulated Initiating Event (PIE), to facilitate and maintain sub-critical reactor core conditions;
- support confinement of radioactive material as part of the primary circuit pressure boundary; and
- fulfil an important role controlling reactivity and confining radioactive material. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

311. Figure 13 shows the main CDRM assembly. Its significant components comprise:

- Rod position indicator assembly
- Pressure housing assembly
- Latch assembly
- Coil stack assembly
- Drive rod assembly

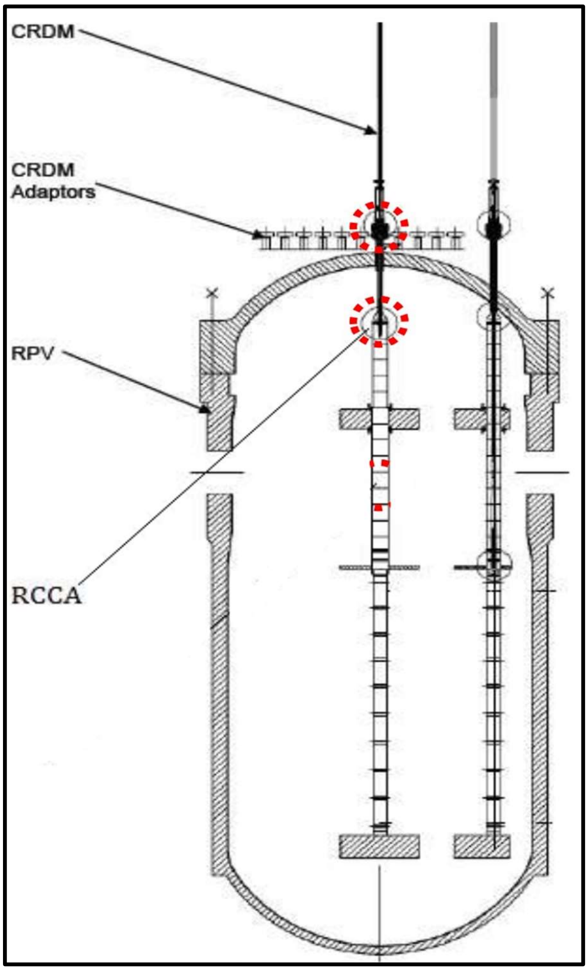

Figure 13: Location of CRDM within the reactor pressure vessel

312. CRDM ME Schedule RGP includes ONR SAPs:

- ECS.1 (Safety categorisation) considers safety categorisation of SSCs;
- ECS.2 (Safety Classification of structures, systems and components) considers safety classification of SSCs;
- EHA.5 (Design basis event operating states) considers SSC performance during simultaneous design basis events and operating conditions; and
- EAD.2 (Lifetime margins) considers degradation processes and their effects on SSCs.

313. I applied ONR SAP EAD.2 (Lifetime Margins) to assess whether CRDM ageing and degradation had been considered. I found no evidence of this within the RP's "Equipment Qualification Methodology" (Ref. 80). This is a shortfall against ONR SAP EAD.2 (Lifetime margins).

314. In response to RO-UKHPR1000-0048 (Ref. 81), the RP has committed to consider degradation and wear mechanisms when applying its revised EQ methodology (Ref. 80).

315. I applied ONR SAPs ECS.1 (safety categorisation) and ECS.2 (Safety classification of structures, systems and components) to my assessment of the CRDM's categorisation and classification. I identified that the link between the CRDM Safety Functional Requirements (SFRs) and their performance requirements was unclear (Ref. 69). Examples include the:

- number of CRDM operations;
- control rod drop times;
- control rod position indicator accuracy; and
- CRDM performance requirements.

316. The RP's safety case (Ref. 82) also considered the CRDM coil stack as a non-classified (NC) component. Given its nuclear safety contributions, the CRDM coil stack classification required explanation.

317. RQ-UKHPR1000-1184, RQ-UKHPR1000-1185, and RQ-UKHPR1000-1426 (Ref. 6) were raised to seek further clarification.

318. The RP responded that the CRDM coil stack:

- supports normal shutdown;
- supports core power regulation;
- achieves and maintains the UK HPR1000 core final state conditions in Design Extension Conditions (DEC-A) including:
  - Small Break Loss of Cooling Accident (SB-LOCA);
  - Loss of Residual Heat Removal function;
  - Station Black Out (SBO); and
  - Total Loss of Cooling Chain (TLOCC).
- classification (Class 3) is in accordance with the RP's "Categorisation and Classification Methodology" (Ref. 47).

319. In its response, the RP also acknowledged that safety functions had not been fully populated within its documentation.

Note: the RP's methodology acknowledges that functions, which would lead to unacceptable consequences should be classified as F-SC1 where no other Category 1 function exists.

320. I consider the CRDM's safety functions and performance requirements are not complete. This is a shortfall against ONR SAPs:

- ECS.1 (Safety categorisation)
- ECS.2 (Safety classification of structures, systems and components)

321. I applied ONR SAP EHA.5 (Design basis event operating states) to my assessment of the RCS [RCP] SDM (Ref. 57) and Revision A of the CRDM Technical Specification (Ref. 82). I noted the CRDM coil stack had not been assigned a seismic category. RQ-UKHPR1000-1426 (Ref. 6) was raised to seek further clarification.

322. The RP responded that the CRDM coil stack has no performance requirements associated with seismic withstand.

323. I consider that failure of the CRDMs have significant implications on nuclear safety. Hence, the RP's lack of CRDM coil stack seismic justification is a shortfall against ONR SAP EHA.5 (Design basis event operating states).

324. For the CRDMs, I judge the RP's design choices are not appropriately justified. I have therefore raised this in an Assessment Finding:

AF-UKHPR1000-0132: The licensee shall demonstrate, during detailed design, that: ■ the control rod drive mechanism safety functions and performance requirements are complete; and ■ the coil stack seismic withstand is appropriate.

325. For the CRDMs, I consider the RP has not considered degradation processes. This does not align with ONR SAP EAD.2 (Lifetime margins). However, I consider this normal business given this is captured within the RP's revised EQ methodology (Revision C) (Ref. 80). Tolerance to degradation mechanisms now require verification testing[‡‡].

326. I also consider the RP has not:

- Identified all safety functions and appropriately classified the associated SSCs. This does not satisfy ONR SAPs:
  - ECS.1 (Safety categorisation)
  - ECS.2 (Safety classification of structures, systems and components)
- Justified the coil stack seismic category. This does not satisfy ONR SAP EHA.5 (Design basis event operating states).

327. I have captured these shortfalls in Assessment Finding AF-UKHPR1000-0132.

Safety Injection System (RIS) [SIS]: General

328. The RIS [SIS]:

- has a safety function to provide borated water from the IRWST Tank to the RCP [RCS] in a fault or accident condition (Category A / Class 1);
- makes-up the inventory of the accumulator in normal operating conditions (Note: this SSC safety function is not recognised); and
- fulfils an important role removing heat from the core. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

329. RIS [SIS] ME Schedule RGP includes ONR SAPs:

- EKP.3 (Defence in depth) considers preventing deviations from normal operation and failures;
- EKP.4 (Safety functions) considers identification of safety functions including all normal and fault sequences; and
- ECS.3 (Codes and standards) considers use of appropriate codes and standards.

Safety Injection System (RIS) [SIS] Duty Functions: Engineering Design Basis

330. I applied ONR SAP EKP.4 (Safety functions) in my assessment of the RP's Duty Schedule (Ref. 50). In Tables T-5-1 and T-6-1 in (Ref. 50), I identified gaps against the Mechanical Engineering SSC's design basis. An example of this is seen in RCV-DFR-01. This relates to the IRWST supplying the RCV [CVCS] control tank when the

[‡‡] *Verification tests should enable detrimental degradation mechanisms to be identified.*

volume is low. However, no performance requirements are identified in the schedule relating to this supply.

331. I consider this a gap against ONR SAP EKP.4 (safety function). The licensee is required to resolve this as part of Assessment Finding AF-UKHPR1000-0129 concerning the design basis.

Safety Injection System (RIS) [SIS] Application of the Principles of Prevention

332. I applied ONR SAP EKP.3 (Defence in depth) to my assessment of the RP's Duty Schedule (Ref. 50). This considered the identification and categorisation of normal (duty) safety functions.

333. RIS-OFR-12 ('ordinary function', see **Table 4**) requires the medium head safety injection pump to fill the accumulator from the IRWST (Ref. 50).

Note: The accumulator injects borated water into the primary circuit under fault and accident conditions (Ref. 83). The accumulator has a Class 1 safety designation.

334. To maintain reactor operations the accumulator must be filled to a designated volume (limits and conditions of safe operation). Without the Medium Head Safety Injection (MHSI) pump maintaining this volume, the accumulator would be unable to fulfil its safety function and reactor shutdown would be required.

335. Hence, I consider RIS-OFR-12 should be designated as a duty function. This is a shortfall against ONR SAP EKP.3 (defence in depth). This shall be addressed as part of Assessment Finding AF-UKHPR1000-0129.

Safety Injection System (RIS) [SIS] Medium-Head Safety Injection Pump

336. The RIS [SIS] MHSI pump forms part of the RIS [SIS] system.

337. I applied ONR SAP ECS.3 (Codes and standards) to my assessment of Revision C of the "Technical Specification for MHSI Pumps" (Ref. 84). The MHSI pump uses its pumped fluid to lubricate and cool its seal. A 15 ml/h leakage limit is specified. I considered the following MHSI pump information was unclear:

- the basis of the 15 ml/h seal leakage limit;
- the seal leakage detection method; and
- consideration of seal damage from debris in pumped fluid.

338. RQ-UKHPR1000-RQ1708 (Ref. 6) was raised to seek clarification.

339. The RP responded that the MHSI pump:

- can operate indefinitely with a 15 ml/h leakage rate;
- seal leakage is collected via the Nuclear Island Vent and Drain System (RPE [VDS]) system. The leakage volume can be determined by the liquid level of the RPE [VDS] tank; and
- uses a cyclone separator to remove particulate from the pumped fluid (see Figure 14). This function will be subject to equipment qualification.

340. I consider this response acceptable subject to suitable qualification. I consider this to be normal business.

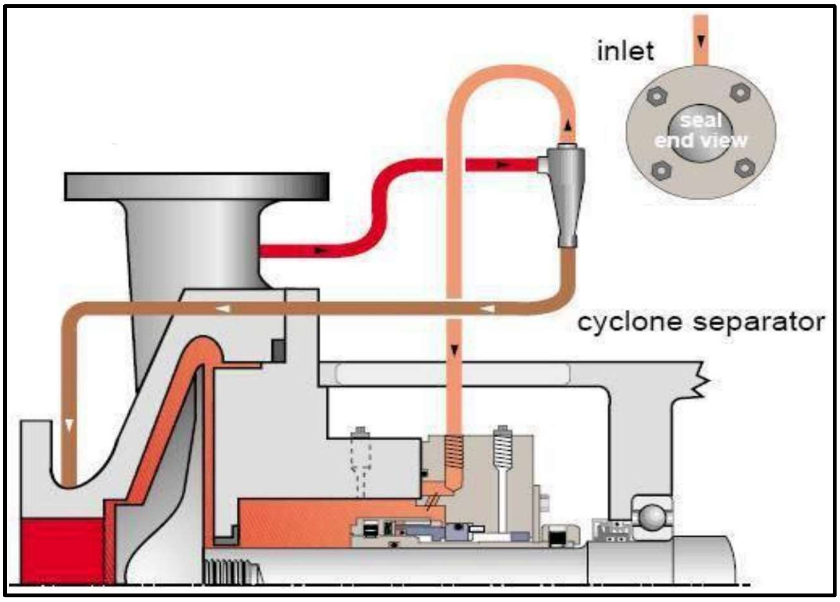

Figure 14: MHSI pump seal flush schematic

341. The RIS [SIS] MHSI pump is:

- Safety Function Class 1;
- Boundary Class 2; and
- Mechanical Code Classification of M2, Revision C of (Ref. 84).

342. By comparison, the Containment Heat Removal System (EHR) [CHRS] pump has:

- Safety Function Class 3;
- Boundary Class 2; and
- Mechanical Code Classification of M2 (Ref. 85).

343. As seen above, I noted SSCs with different functional class had the same mechanical code classification. RQ-UKHPR1000-1182 (Ref. 6) was raised to seek clarification.

344. The RP stated that its approach (Ref. 47):

- aligns with IAEA guidance TECDOC-1787 (Ref. 46); and
- relates to the Boundary Classification (B-SC) not the Functional Safety Class (F-SC).

345. I am satisfied the RP's approach aligns with RGP (Ref. 46).

346. For the RIS [SIS] MHSI pump, I am content the RP has considered seal performance and degradation. This satisfies ONR SAP ECS.3 (Codes and standards).

Safety Injection System (RIS) [SIS] Residual Heat Removal Heat Exchanger

347. The RIS [SIS] Residual Heat Removal (RHR) heat exchangers have a safety function to remove residual heat from the core in normal and accident conditions (Category A / Class 1)

348. RHR heat exchanger ME Schedule RGP includes ONR SAPs:

- ERL.4 (Margins of conservatism) considers suitable uncertainties should be included in a safety case; and
- EHT.1 (Design) considers design requirements for heat transport SSCs.

349. I considered that the conservatisms applied to the performance requirements of the RHR heat exchanger were unclear in Revision B of the SDM (Ref. 83). RQ-UKHPR1000-1189 and RQ-UKHPR1000-1424 (Ref. 6) were raised to seek clarification.

350. For the RHR heat exchangers, the RP:

- provided sizing calculations;
- confirmed a 19.15% fouling conservatism had been applied; and
- confirmed when the most challenging scenario occurs after normal reactor shutdown. This is most onerous when:
    - two RHR heat exchanger trains operate;
    - the RCP [RCS] primary coolant is circa 20% of the average core temperature; and
    - the reactor coolant pumps are not operating.

351. For the RIS [SIS] RHR heat exchangers, I consider that the RP has identified suitable performance requirements and uncertainties. This satisfies ONR SAPs:

- ERL.4 (Margins of conservatism)
- EHT.1 (Design)

Essential Service Water System (SEC) [ESWS] Centrifugal Pump

352. The Essential Service Water System (SEC) [ESWS] centrifugal pump:

- has a safety function to provide cooling water for the Component Cooling Water System (RRI) [CCWS] in both normal and accident conditions (Category A / Class 1); and
- fulfils an important role supporting removal of heat from the reactor core during normal and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

353. SEC [ESWS] pump ME Schedule RGP includes ONR SAPs:

- EMC.13 (Materials) considers SSC material suitability; and
- ERL.1 (Form of claims) considers SSC reliability in its operating environment.

354. Given it pumps seawater, I considered that the SEC [ESWS] system and pump are vulnerable to:

- accelerated corrosion mechanisms; and
- damage by entrained organic and inorganic debris.

355. The SEC [ESWS] system technical specification (Ref. 86) did not include the pump's:

- impeller material (RCC-M M3405) suitability; and

- maximum tolerable particulate size.

356. RQ-UKHPR1000-1092 and RQ-UKHPR1000-1384 (Ref. 6) were raised to seek clarification.

357. The RP responded that the:

- Pipework materials are typically manufactured using reinforced steel, concrete and rubber coated carbon steel.
- Pump impeller material will be changed to a suitable material.
- Upstream pump filtration uses a 3 mm travelling band screen mesh size (based on Chinese plant operational experience (OPEX)).
- Qualification specification will include an 'impurity test' to verify pump performance.

358. I consider this response suitable as:

- the steel pipework is protected by concrete or rubber preventing damage;
- a suitable pump impeller material can be specified during detail design (normal business); and
- The 3 mm mesh size is considered reasonable given the related OPEX.

Note: qualification is required during site-specific stages, which I consider normal business.

359. For the SEC [ESWS], I consider the RP has shown the materials are compatible with the operating environment. This satisfies ONR SAPs:

- EMC.13 (Materials)
- ERL.1 (Form of claims)

Atmospheric Steam Dump System (VDA) [ASDS] Silencer

360. The VDA (ASDS) silencer:

- has a safety function to operate when the main steam relief control valve (MSRCV) relieves system overpressure during DBC and accident conditions (Category A / Class 1);
- reduces noise generated by steam escaping from the VDA [ASDS] system; and
- fulfils an important role supporting the removal of heat from the core during atmospheric steam dumping. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

361. ME Schedule RGP for the VDA [ASDS] silencer includes ONR SAP ERL.4 (Margins of conservatism), which relates to design margins of conservatism.

362. The silencer and the silencer shell (Figure 15) both receive steam from the:

- main steam relief control valve (MSRCVs) via the main steam relief isolation valve (MSRIV); and
- main steam safety valve (MSSV).

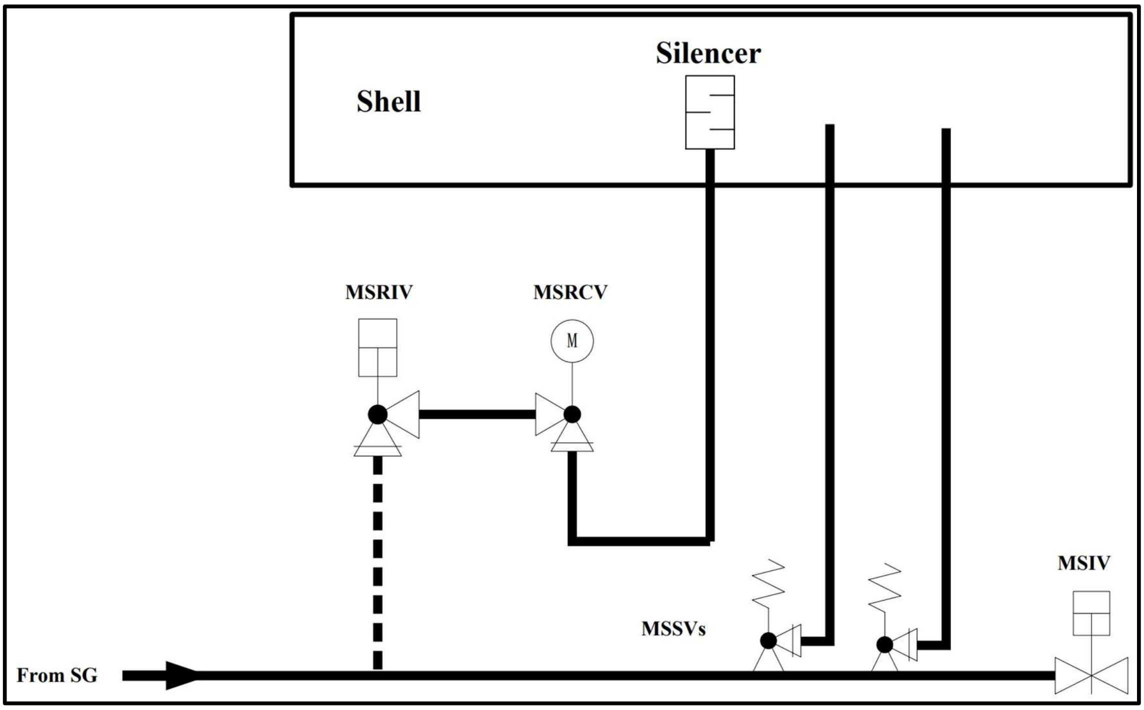

Figure 15: VDA [ASDS] silencer schematic

363. The silencer design pressure is 5.4 MPa(g). I could not identify how the design pressure related to the maximum upstream pressures. RQ-UKHPR1000-1153 (Ref. 6) was raised to seek clarification.

- The RP confirmed, via calculation (Ref. 6), that the VDA [ASDS] silencer design pressure was appropriate. I consider the RP's response suitable as it shows:
  - suitable consideration of pressure losses in the system; and
  - suitable MSRIV conservatisms for pressure and flow.

364. I noted that:

- silencers are provided for the VDA [ASDS] to reduce noise produced during steam discharging to protect personnel; and
- MSSVs do not discharge via a silencer.

365. I consider the lack of MSSV discharge silencer should be assessed by the licensee during site-specific stages. I have identified this as a Minor Shortfall.

366. For the VDA [ASDS] silencer, I consider the RP has shown suitable margins of conservatism. This satisfies ONR SAP ERL.4 (Margins of conservatism).

Main Steam System (VVP) [MSS] Main Steam Isolation Valve

367. The Main Steam Isolation Valves (MSIVs):

- have a safety function to isolate each Main Steam Line (MSL) preventing SG steam flow to the Steam Header (Category A / Safety Class 1).
- allow sufficient MSL flow when open; and
- fulfil an important role during normal and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant through support of:

- removal of core heat
- control of reactivity; and
- confinement of radioactive material.

368. MSIV RGP for the ME Schedule includes:

- ONR SAPs:
  - EDR.2 (Redundancy, diversity and segregation) considers demonstration of reliability of safety functions.
  - EDR.4 (Single failure criterion) relates to avoidance of single random failures preventing safety function delivery;
  - ERL.4 (Margins of Conservatism) considers application of uncertainties in SSC performance requirements; and
  - ERC.1 (Design and operation of reactors) considers fundamental safety functions for design and operation of reactors.
  - SC.4 (Safety case characteristics) considers application of RGP in the safety case.
- ONR TAGs:
  - NS-TAST-GD-036 Redundancy, Diversity, Segregation and Layout of Mechanical Plant considers whether:
    - an SSC performs its safety function in the presence of a single passive or active component failure; and
    - a design has adequate levels of redundancy to ensure it performs a required safety function.
  - NS-TAST-GD-005 Guidance on the Demonstration of ALARP (As Low as Reasonably Practicable) considers whether:
    - no further reasonably practicable improvements can be implemented to reduce risks ALARP; and
    - suitable optioneering has been undertaken to evaluate design suitability.

369. I applied ONR SAPs ERC.1 (Design and operation of reactors) and ERL.4 (Margins of conservatism) to the MSIV performance requirements. The MSIV requirement to close in less than 5 seconds, as identified in the ME Schedule (Ref. 51), was unclear. RQ-UKHPR1000-1051 (Ref. 6) was raised to seek clarification.

370. The RP responded stating that the MSIV's:

- closure time (5 seconds) is applied in the transient model (see PCSR V1 sub-chapter 12.9.1.1); and
- validation testing will satisfy the procurement specification.

371. I noted that the RP's transient analysis has been assessed by ONR's Fault Studies inspector who considered it suitable (Ref. 53).

372. I applied ONR SAPs EDR.2 (Redundancy, diversity and segregation) and EDR.4 (Single failure criterion) to my assessment. I also considered guidance within ONR's

TAGs for redundancy, diversity, segregation and layout of mechanical plant, and the demonstration of ALARP.

373. The RP's "Methodology of Safety Categorisation and Classification" (Ref. 47) mandates that the Single Failure Criterion (SFC) be applied for Functional Safety F-SC1 (Class 1) and F-SC2 (Class 2) SSCs.

374. As each MSL contains a single MSIV, compliance with the SFC was unclear. RQ-UKHPR1000-1113 (Ref. 6) was raised to seek clarification.

375. The RP responded stating that:

- For Steam Generator Tube Rupture (SGTR) a single MSIV, per MSL train, does not satisfy SFC.
- The MSIV actuator includes two drainage manifolds. Each drainage manifold can be used to initiate valve closure which complies with SFC.
- PWR reactor design OPEX (e.g. EPR, AP1000 and CPR1000) use a single MSIV per MSL.
- MSIV in-service testing requires functional performance demonstration.

376. The RP also prepared an optioneering report (Ref. 87), which considered diversification of the MSIV. This report does not appear to consider redundancy within the MSL or discuss the consequences of event recovery i.e. potential dose implications.

377. The Fault Studies Assessment Report (Ref. 70) considered the MSIVs and the RP's optioneering report. It noted a shortfall in consideration of redundancy within the optioneering. However, the assessment concludes that the RP's consideration of diversity, comparing other modern PWR designs, is sufficient for GDA.

378. I consider that the optioneering undertaken for the MSIV configuration requires improvement. The outcome of this may not significantly change the valve configuration or design. However, the safety case currently does not provide a robust justification. The radiological consequences for MSIV failure to close does not appear to have been sufficiently considered. For example, contamination of the secondary circuit equipment requiring repair and clean-up. Hence, I have identified this as a Minor Shortfall. The licensee should consider improving the optioneering, arguments and evidence for the design and configuration of MSIVs, justifying the design reduces risks ALARP. I consider ONR SAP SC.4 (Safety case characteristics) applicable.

379. I consider the above Minor Shortfall to also be against ONR SAPs EDR.2 (Redundancy, diversity and segregation) and EDR.4 (Single failure criterion).

4.2.2 Strengths

380. The RP has implemented approaches to demonstrate safety function traceability. For example, in its Duty Schedule (Ref. 50) and ME Schedule (Ref. 51).

4.2.3 Outcomes

381. My assessment has resulted in the RP making the following improvements:

- It developed a Duty Schedule (Ref. 50) identifying normal operation (Level 1 - Defence in depth) safety functions for a sample of Mechanical Engineering SSCs.

- It developed an ME Schedule (Ref. 51) identifying safety functions for a sample of Mechanical Engineering SSCs.
- The SEC [ESWS] pump impeller material specification was changed to duplex stainless-steel ASTM A890 / A890M Gr.5A.
- The SEC [ESWS] pump qualification has been changed to include testing with pumped fluid impurities.

382. I have raised four Assessment Findings, discussed in sub-section 4.2.1. I consider that these matters need to be resolved by the licensee during detailed design. These relate to:

- underpinning the Mechanical Engineering SSC design basis;
- providing evidence that the reactor coolant pump shaft seal injection system is designed to deliver its safety functions, and that unmitigated dose is used to safety categorise and classify systems and components;
- ensuring the RPE [VDS] pump is adequately sized to prevent tank overflow; and
- identification and classification of CRDM functions and components.

383. I have also identified six Minor Shortfalls. These are described in paragraphs 246, 248, 253, 308, 365 and 378. These apply to the following Mechanical Engineering systems and components:

- ASG [EFWS] Containment Isolation Valves
- RCP [RCS] Severe Accident Dedicated Valves
- VVP [MSS] Main Steam Safety Valves
- VVP [MSS] Main Steam Isolation Valves

384. The Assessment Findings are listed in Annex 3.

4.2.4 Conclusion

385. I judge, for the purposes of GDA, that the RP has:

- produced a suitable categorisation and classification methodology;
- without justification, not prioritised prevention over protection when categorising and classifying Mechanical Engineering SSCs; and
- implemented a coding system to trace the safety functions.

Note: an exhaustive list of Mechanical Engineering SSC safety functional requirements remains outstanding.

386. Overall, for the purpose of GDA, I conclude that the RP’s submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the adequacy of the RP’s Mechanical Engineering Schedule is sufficient from a Mechanical Engineering perspective.

387. I have identified several matters that the licensee will need to address during the detailed design. I have captured these in four Assessment Findings.

4.3 Theme 3: Adequacy of Equipment Qualification Arrangements

388. My Step 3 assessment (Ref. 22) found mechanical equipment qualification (EQ) arrangements as an area for improvement. It concluded:

- During Step 4, further evidence is required to demonstrate that the UK HPR1000 asset management arrangements are adequate. This will include the methodology for equipment qualification.

389. EQ RGP includes:

- UK Law including:
  - Health and Safety at Work Act 1974 (HSWA) (Ref. 88); and
  - Management of Health and Safety at Work Regulations 1999 (MHSWR) (Ref. 45).
- ONR Safety Assessment Principles (SAPs) (Ref. 2):
  - EQU.1 (Qualification procedures)
  - EMT.3 (Type testing)
  - EMT.4 (Validity of equipment qualification)
  - EHA.5 (Design basis event operating states)
  - EHA.9 (Earthquakes)
  - ERC.1 (Design and operation of reactors)
  - EMC.13 (Materials)
  - EMC.22 (Materials compatibility)
- ONR Technical Assessment Guides (TAG) (Ref. 4):
  - NS-TAST-GD-057 Design Safety Assurance
  - NS-TAST-GD-098 Asset Management
  - NS-TAST-GD-094 Categorisation of Safety Functions and Classification of Structures, Systems and Components
  - NS-TAST-GD-102 Emergency Power Generation
- Industry Guidance:
  - IAEA Safety Reports Series No.3 – Equipment Qualification in Operational Nuclear Power Plants (Ref. 89)
  - The American Society of Mechanical Engineers (ASME) – QME-1, Qualification of Active Mechanical Equipment Used in Nuclear Facilities (Ref. 90)
  - Electrical Power Research Institute (EPRI) – Plant Support Engineering: Equipment Qualification Reference Manual (Ref. 91)

390. EQ is a fundamental requirement of the UK's approach to safety assessment for nuclear facilities. Reducing risks ALARP[§§] is a requirement of HSWA (Ref. 88) and MHSWR (Ref. 45).

[§§] *HSWA and MHSWR use the term "so far as is reasonably practicable" (SFAIRP). ONR and HSE consider SFAIRP and ALARP to be interchangeable.*

391. ASME QME-1 guidance (Ref. 90) specifically concerns EQ of active[***] components. As GDA relates to the concept design, my assessment used IAEA (Ref. 89) and EPRI (Ref. 91) guidance given their relevance to EQ.

392. I assessed Revision A of the RP's "Equipment Qualification Methodology" (Ref. 80). I identified the following RGP gaps:

- identifying environmental conditions (in both normal and accident states);
- conservative derivation of SSC performance requirements, for example 'mission times';
- configuration control of qualification evidence for all stages of equipment lifecycle;
- monitoring requirements to identify when 'qualified life' re-assessment is required;
- EQ preservation arrangements; and
- EQ method justification, for example the use of OPEX.

393. RO-UKHPR1000-0048 (Ref. 81) was raised to:

- explain ONR's regulatory expectations;
- improve the RP's EQ arrangements; and
- seek EQ demonstration for Mechanical Engineering SSCs.

394. The RO actions were:

ROA.1 Develop an improved EQ methodology

In response to this ROA the RP should demonstrate how:

- EQ RGP requirements are managed for each stage of the UK HPR1000 lifecycle;
- EQ arrangements satisfy ONR's view of EQ RGP; and
- any EQ RGP shortfalls identified are to be addressed, and by when.

ROA.2 Demonstrate implementation of this methodology

In response to this ROA, the RP should demonstrate how safety case EQ requirements, for the SSC's identified in this RO, are addressed by the design and achieved in practice[†††].

395. I sampled the following systems and components given their relevance to nuclear safety:

- Emergency Feedwater System (ASG) [EFWS]
- Containment Leak Rate Testing and Monitoring System (EPP) [CLRTMS]
- Main Control Room Air Conditioning System (DCL) [MCRACS]
- Reactor Coolant System (RCP) [RCS]

[***] *In the context of EQ, "active" mechanical equipment contains moving parts.*
[†††] *Note that the RO Action included examples of what should be considered. For further information see www.onr.org.uk/new-reactors/index.htm*

- Safety Injection System (RIS) [SIS]
- Emergency Diesel Generators (EDGs)

4.3.1 Assessment

4.3.1.1 Closure of RO-UKHPR1000-0048

RO-UKHPR1000-0048 ROA.1 Closure

396. RO-UKHPR1000-0048 ROA.1 required the RP to show how EQ:

- RGP requirements are managed;
- arrangements satisfy RGP; and
- RGP shortfalls are addressed.

397. To address the above, the RP produced an “Equipment Qualification RGP Compliance Analysis Report” (Ref. 92).

398. This report identified RGP gaps against:

- configuration control of EQ lifetime data;
- links between EQ and EIMT; and
- links between suitably qualified and experienced personnel and EQ.

399. My feedback on the analysis report (Ref. 93) noted additional gaps.

400. To address these gaps, the RP improved its EQ Methodology (Ref. 80) to identify:

- a graded approach to EQ arrangements based on SSC classification;
- methods by which EQ is achieved;
- environmental parameters for normal, fault and accident conditions;
- mission time[‡‡‡] for SSCs;
- qualified life[§§§] for SSCs;
- verification tests;
- implementation tests;
- preservation requirements; and
- that data configuration control is required.

401. Figure 16, provides a pictorial overview of EQ considerations.

[‡‡‡] *Mission time is the duration for which SSC performance is required without EIMT.*
[§§§] *Qualified Life is the duration for which the SSC performance is required during a specific set of service conditions. EIMT activities are permitted to preserve qualified life.*

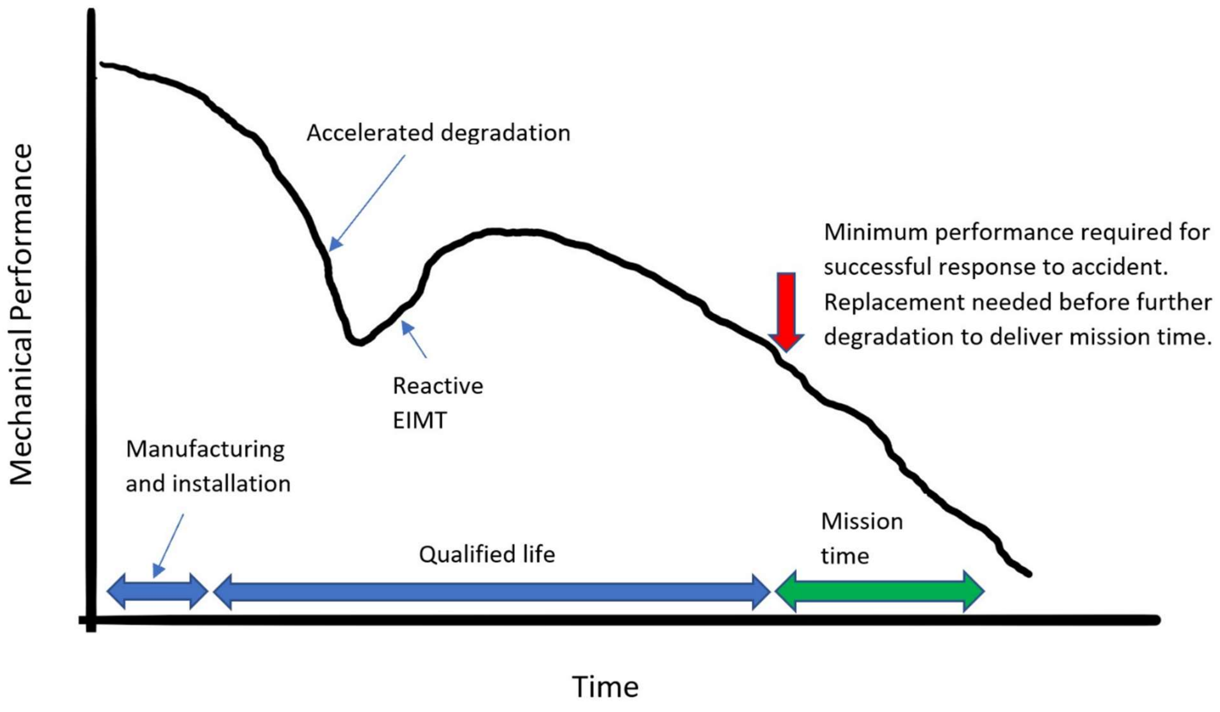

Figure 16: Equipment qualification illustration

402. The RP's EQ categories are summarised in **Table 6**. I consider these to be suitable as they link plant operating environments and conditions with Mechanical Engineering SSCs.

Table 6: EQ category definitions

EQ Category	SSC Location	Operating conditions
K1	Inside containment	■ Normal conditions ■ Accident conditions ■ Post-accident conditions ■ Seismic conditions
K2	Inside containment	■ Normal conditions ■ Seismic conditions
K3	Outside containment	■ Normal conditions ■ Seismic conditions
K3ad	Outside containment	■ Normal conditions ■ Accident conditions ■ Post-accident conditions ■ Seismic conditions
SA	Dependant on 'K' designation	■ Severe accident conditions ■ Post severe accident conditions ■ Seismic conditions

403. The RP's seismic categories are summarised in **Table 7** and **Table 8**:

Table 7: Seismic category definitions

Seismic Category	Definition
SSE1	■ Function Class 1 SSCs ■ Function Class 2 SSCs ■ Function Class 3 SSCs where: • Second line protection system for reaching safe state; • Severe accident management
SSE2	■ Where seismic failure of SSC results in internal hazard on SSE1 SSC.

Table 8: Seismic performance definitions

Seismic Performance Requirements	Application	Requirement
Operability (O)	Active SSC	■ Fulfil safety functions.
Functional capacity (F)	Active and passive SSCs	■ Deformation permitted; and ■ Fulfil safety functions.
Integrity (I)	Active and passive SSCs	■ Fulfil safety functions.
Stability (S)	Active and passive SSCs	■ Withstand loads that lead to orientation change.

404. I consider the RP's seismic definitions in **Table 8** overlap. However, as the generic design is at concept stage, I do not consider this a significant GDA gap. Further clarification may be sought during site-specific stages as part of normal business.

405. My assessment concluded that the RP's response to RO-UKHPR1000-0048 ROA.1 was appropriate. This satisfies ONR SAP EQU.1 (Qualification procedures), which considers the arrangements and their implementation to qualify equipment.

406. RO-UKHPR1000-0048 ROA.2 required the RP to demonstrate how its EQ methodology (Ref. 80) is applied. In response the RP submitted its:

- "Environmental Requirements for Equipment Qualification" (Ref. 94); and
- EQ Schedule (Ref. 95).

EQ Environmental Requirements Report

407. The environmental report, (Ref. 94) identifies operating conditions for mechanical equipment. These conditions cover normal operations, accidents and severe accidents.

408. I consider that this document identifies suitable EQ environmental conditions. This satisfies ONR SAP EQU.1 (Qualification procedures).

EQ Schedule for Sampled Mechanical Engineering SSCs

409. The RP's Mechanical Engineering EQ schedule (Ref. 95) identifies:

- Key EQ phases for:
  - verification – First of a Kind (FOAK) SSC testing;
  - implementation – Subsequent SSC testing;
  - preservation – EQ through-life maintenance (ONR SAP EMT.4 (Validity of equipment qualification);
  - performance requirements linked to the safety case (duty, fault and severe accident functions); and
  - the EQ method (how EQ is achieved).

410. However, the RP's EQ schedule (Ref. 95) does not fully capture:

- performance parameters;
- how each test demonstrates the performance parameters (see Table 9 for examples); and
- when the EQ tests are required i.e. during:
  - verification phase;
  - implementation phase; or
  - preservation phase.

Table 9: EQ gaps in sampled mechanical systems

UK HPR1000 System / component	EQ Shortfall
Emergency Feedwater System (ASG) [EFWS], Containment Isolation Valve	■ Pressure retaining duty function not identified.
Reactor Coolant System (RCP) [RCS], Pressuriser Safety Valve (PSV)	■ Pilot valve operation with entrained debris not identified.
RCP [RCS], reactor coolant pump	■ Shaft seal integrity fault condition testing is unsuitable. ■ Through flow test (when impeller stopped) is not identified. ■ FOAK endurance testing is unsuitable.

UK HPR1000 System / component	EQ Shortfall
Containment Leak Rate Testing and Monitoring System (EPP) [CLRTMS], Equipment Access Hatch	■ Mission time qualification not identified.
Safety Injection System (RIS) [SIS], Medium Head Safety Injection pump	■ FOAK endurance testing is unsuitable.

411. To address the EQ shortfalls identified above, design choices, site-specific and manufacturers' information will be required by the licensee. I have therefore raised the following Assessment Finding:

> AF-UKHPR1000-0133: The licensee shall, during site-specific stages, produce a strategy and plan to justify equipment qualification for all safety related Mechanical Engineering systems and components. From this, information shall be provided for an agreed sample to address the following:
> - the performance requirements and their traceability;
> - how testing demonstrates the required performance; and
> - when testing is undertaken i.e. during verification, implementation or preservation phases.

412. This Assessment Finding should be considered in conjunction with AF-UKHPR1000-0129 in sub-section 4.2.1 of this report.

RO-UKHPR1000-0048 ROA.2 Closure

413. My assessment concluded that the RP's RO-UKHPR1000-0048 ROA.2 submissions:

- identify environmental conditions for EQ;
- provide an EQ schedule (Ref. 95), which identifies:
  - key phases of EQ;
  - performance requirements; and
  - how EQ will be achieved.
- do not identify:
  - how each test demonstrates performance; and
  - when the tests are undertaken i.e. during the verification, implementation, or preservation phase.

414. I consider gaps exist in the RP's Mechanical Engineering EQ schedule (Ref. 95). This does not align with expectations of ONR SAP EQU.1 (Qualification procedures). This is captured in Assessment Finding AF-UKHPR1000-0133.

RO-UKHPR1000-0048 Assessment Conclusions

415. My RO-UKHPR1000-0048 assessment concludes that the RP has:

- improved its EQ methodology; and
- implemented suitable EQ for GDA.

416. I have raised Assessment Finding AF-UKHPR1000-0133 to address EQ gaps during detailed design.

4.3.1.2 Equipment Qualification SSC Assessment

417. I assessed the following equipment, which was chosen because of their importance to nuclear safety.

Emergency Feedwater System (ASG) [EFWS] Containment Isolation Valves

418. The ASG [EFWS] containment isolation valves:

- have a safety function to prevent back flow from the SG to the ASG [EFWS] during normal operations (Category A / Class 1);
- allow ASG [EFWS] to SG flow during a range of accident conditions;
- allow commissioning tests to be undertaken; and
- fulfil an important confinement role and support cooling during normal operation and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

419. ASG [EFWS] containment isolation valve EQ RGP includes ONR SAPs:

- EHA.5 (Design basis event operating states) considers analysis of bounding design basis events; and
- EQU.1 (Qualification Procedures) considers suitability of qualification procedures.

420. I applied ONR SAPs EHA.5 (Design basis event operating states) and EQU.1 (Qualification procedures) to the containment isolation valve qualification criteria. The K3 qualification designation, for both inside and outside containment valves, was unclear. RQ-UKHPR1000-RQ1288 (Ref. 6) was raised to seek clarification.

421. The RP responded:

- The outside containment isolation valves have a K3+SA category. This requires the valves to perform under seismic and severe accident conditions.
- The non-return valve inside containment has a K1+SA category (functional seismic and severe accident).

422. I consider the K1+SA EQ category for the non-return valve to be acceptable.

423. The EQ schedule (Ref. 95) did not explain how the containment isolation valves would be qualified. For example, through testing, analysis (calculation), operating experience or a combined method.

424. The RP has made improvements to its EQ methodology (Ref. 80), which captures the principles of selecting the qualification method. I consider the application of this is normal business for a licensee.

425. For the ASG [EFWS] containment isolation valves, I consider the RP has:

- Identified the design basis events operating states. This satisfies ONR SAP EHA.5 (Design basis event operating states).
- Not suitably identified the qualification method. This does not satisfy ONR SAP EQU.1 (Qualification procedures). However, I judge that this can be addressed through application of the revised EQ methodology (Ref. 80).

Containment Leak Rate Testing and Monitoring System (EPP) [CLRTMS]
Equipment Access Hatch

426. The Equipment Access Hatch (EAH):

- provides reactor building access for outage work equipment during shutdown;
- during all other operational and accident scenarios, the hatch's safety function is to remain closed to maintain the containment building pressure boundary (Category A / Class 1); and
- fulfils an important confinement role during all normal and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant here as it:
    - maintains external leak tightness; and
    - limits radionuclide release to the environment.

427. EAH EQ RGP includes ONR SAPs:

- EMC.13 (Materials) relates to the suitability of materials;
- EMC.22 (Material compatibility) considers material compatibility during operations and maintenance;
- EQU.1 (Qualification procedures) considers the arrangements and their implementation to qualify equipment;
- EHA.9 (Earthquakes) considers weakening of a safety function following an earthquake; and
- ERC.1 (Design and operation of reactors) considers the confinement of radioactive material.

428. I applied ONR SAPs EMC.13 (Materials) and EMC.22 (Material compatibility) to my assessment of the EAH leak-tightness. This is reliant upon the EPDM[****] seal integrity. Revision D of the EAH specification (Ref. 72) states "anti-rust oil" or "other effective methods proved by practices" could be used as temporary protection against seal surface corrosion.

429. I noted the use of hydrocarbon oil is not specifically prohibited. This is despite its incompatibility with EPDM. Incorrectly specified products may degrade the seal. RQ-UKHPR1000-1067 (Ref. 6) was raised to seek clarification.

430. The RP responded that:

- seals are removed and stored following factory testing;
- the EAH sealing surfaces will be coated with grease for temporary protection;
- all grease will be removed from the seals before reinstatement onsite; and
- no sealing surface corrosion protection is required when the plant is in operation.

431. I consider incompatibility issues between EPDM seals and EAH surface treatments have been addressed.

432. I applied ONR SAP EQU.1 (Qualification procedures) when assessing the functional performance of the EAH seal. The EAH specification (Ref. 72) states seal performance shall be shown by a "tightness test on a scaled-down model".

[****] *Ethylene Propylene Diene Monomer*

433. The suitability of the proposed testing, to show meaningful seal performance, was unclear. RQ-UKHPR1000-0707 (Ref. 6) was raised to seek clarification.

434. The RP responded that the seal test:

- used the same seal cross section as the complete assembly; and
- provided a seal leakage rate per unit length.

435. Given an equivalent seal profile is used in the test, I consider this response acceptable.

436. Within the EAH specification (Ref. 72), Table T-4.8-7 states a five-year seal service life. Appendix 1A of the RP's EQ schedule (Ref. 95) claims the seal should fulfil its sealing function "at least a year after the accident" (its 'mission time'). Hence, the seal is required to deliver its safety function for approximately six years (5 + 1 years). This requirement is not included in the EAH specification (Ref. 72). Given this is a design choice, the licensee should capture all requirements related to its EAH seal qualification during detailed design. I consider this to be captured with AF-UKHPR1000-0133.

437. I applied ONR SAPs EQU.1 (Qualification procedures) and EHA.9 (Earthquakes) to the lifting device, which opens and closes the EAH. The lifting device did not appear to be seismically qualified and plastic deformation was permitted. RQ-UKHPR1000-RQ-1068 and RQ-UKHPR1000-RQ-1240 (Ref. 6) were raised to seek clarification.

438. The RP responded that the lifting device:

- operates (either electrically or manually) to close the EAH after an earthquake;
- is seismically qualified to remain within elastic limits;
- includes auxiliary components, not required for lifting, which:
  - are allowed to deform; and
  - include measures to stop loosening and missile generation.

439. I consider the RP's time at risk argument acceptable. This is because there is a low probability of a seismic event during the EAH opening or closing operations.

Note: the time at risk is < 2 hours per outage every ~18 months.

440. I also consider the consequence of localised plastic deformation, of limited auxiliary components, is not detrimental to nuclear safety.

441. Appendix 1B-3 of the EQ schedule (Ref. 95) contains valve details. Their link with the EAH is unclear. This should be corrected during site-specific stages. This shortfall is covered by Assessment Finding AF-UKHPR1000-0133, which concerns application of the EQ methodology.

442. For the EAH EQ, I consider the RP has shown how:

- Materials used during manufacture are suitable and compatible. This satisfies ONR SAPs:
  - EMC.13 (Materials)
  - EMC.22 (Materials compatibility)

- Physical testing is suitable. This satisfies ONR SAP EQU.1 (Qualification procedures).
- Seismic performance is considered. This satisfies ONR SAP EHA.9 (Earthquakes).

443. For EAH EQ, I consider the RP has not shown suitable qualification of its confinement requirement for its mission time. This does not satisfy ONR SAPs:

- EQU.1 (Qualification procedures)
- ERC.1 (Design and operation of nuclear reactors)

444. This gap shall be addressed as part of Assessment Finding AF-UKHPR1000-0133.

Reactor Coolant System (RCP) [RCS] Reactor Coolant Pump

445. The reactor coolant pump:

- has a safety function to supply coolant flow to transfer thermal power from the reactor core to the SGs (Category A / Class 1); and
- fulfils an important cooling role and supports confinement during normal operation. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

446. Reactor coolant pump RGP includes ONR SAPs:

- EQU.1 (Qualification procedures) considers the application of EQ procedures to demonstrate safety functional performance;
- EMT.3 (Type Testing) considers type testing conditions, which should be equal to, at least the most onerous design condition;
- ECM.1 (Commission testing) considers commissioning test requirements; and
- ERC.1 (Design and operation of reactors) considers fundamental safety functions associated with reactor design and operations including:
  - control of reactivity;
  - removal of heat; and
  - confinement of radioactive material.

447. I assessed Revision B of the FOAK reactor coolant pump test and analysis requirements (Ref. 96) and judged these unsuitable because the:

- EQ method for the pump's operation without motor cooling was unclear;
- EQ method for the response to reverse flow conditions was unclear;
- operational endurance test justification is not sufficient; and
- seismic performance testing was not justified.

448. RQ-UKHPR1000-1383 (Ref. 6) was raised to seek further clarification of the reactor coolant pump design and operation.

<u>EQ method for reactor coolant pump operation without motor cooling</u>

449. The RP confirmed that the reactor coolant pump operation, with no motor cooling, will be verified by type-testing. I consider this acceptable, subject to the EQ schedule (Ref. 95) being updated during normal design development. I have identified this as a Minor Shortfall**.**

EQ method for reverse flow conditions

450. The RP clarified the reactor coolant pump anti-reverse rotation design, has a proven history of operation. I am content the RCP [RCS] system level testing analysis, and supporting OPEX data, is currently sufficient to verify the anti-reverse function for GDA. However, the RP had not planned to qualify this during commissioning.

451. The reactor coolant pump anti-reverse function requires demonstration, at the system level, to satisfy ONR SAP ECM.1 (Commissioning tests). I have captured this in Assessment Finding AF-UKHPR1000-0134.

Endurance testing

452. The EQ schedule (Ref. 95), identifies a full-load operational endurance test duration. I noted the reactor coolant pump qualification for the AP1000 included more than 1,600 running hours and 600 stop-start cycles (see link below)[††††]. The generic UK HPR1000 design reactor coolant pump endurance tests:

- are less than 1% of the intended 25,000 hours operational life; and
- do not sufficiently consider degradation mechanisms.

453. I consider RP's justification for its reactor coolant pump endurance testing to be inadequate. This does not align with ONR SAP EMT.3 (Type-testing). I have also captured this in Assessment Finding AF-UKHPR1000-0134.

Seismic performance

454. Following a seismic event, the reactor coolant pump is required to provide adequate coolant flow during coast down.

455. The RP responded that the reactor coolant pump's seismic analysis demonstration will not be compromised because:

- Mating surfaces between rotor and stator will not interfere.
- Bearings can still maintain complete fluid lubrication.
- Bearing loads remains within the acceptable capacity range.
- The reactor coolant pump performance would be justified by analysis. The RP consider it is not reasonably practicable to physically test the pump's response i.e. the test bench would be too large.
- The reactor coolant pump coast down performance is physically tested under normal conditions during the full-load test.

456. I considered the RP's response has not shown reactor coolant pump coast down performance following a seismic event. This does not satisfy ONR SAP EQU.1 (Qualification procedures).

457. Resolution of the identified shortfalls will require licensee design choices, which can be made during detailed design and site-specific stages. The EQ documentation of the reactor coolant pumps will need to identify suitable requirements. I have raised the qualification aspects of the reactor coolant pump within Assessment Finding AF-UKHPR1000-0134. Assessment Finding AF-UKHPR1000-0133 is also considered to be applicable.

[††††] www.westinghousenuclear.com/uknuclear/about/news/view/ap1000%C2%A+E-rcp-reaches-full-qualification

Reactor Coolant Pump Seal Qualification

458. I applied ONR SAP ERC.1 (Design and operation of reactors) during technical discussions (Ref. 7). I identified concerns relating to reactor coolant pump seal qualification.

459. The reactor coolant pump seal is cooled and lubricated with water from the Chemical and Volume Control System RCV [CVCS]. This maintains an effective seal between the reactor coolant pump shaft and the primary circuit fluid. Following RCV [CVCS] system failure, the RP claims the pump operation can continue. This will result in the following:

- The seal cooling function being maintained by the reactor coolant pump shaft feed screw (see Figure 8 for the schematic). The reactor coolant pump seal injection becomes a closed loop system driven by the reactor coolant pump shaft feed screw at a circa 5% lower pressure than the RCV [CVCS] (Ref. 97).
- The lubrication filtration function is lost.
- The reactor coolant pump seal injection is cooled by the component cooling water system (RRI [CWCS]).

460. Losing seal filtration may degrade the reactor coolant pump seal integrity. This is currently noted in the SDM (Ref. 57) as an undefined period. This period could be the maximum time between outages.

461. Under loss of RCV [CVCS], the reactor coolant pump performance may be degraded by filtration loss. I consider the impact of reactor coolant pump seal debris build-up has not been sufficiently considered. This does not satisfy ONR SAP ERC.1 (Design and operation of reactors). The licensee will need to satisfy itself that this is sufficiently considered during detailed design. To address the identified shortfalls, I have raised the following Assessment Finding:

> AF-UKHPR1000-0134: The licensee shall demonstrate, during site-specific stages, that the reactor coolant pump's:
>
> - shaft seal injection and its supporting systems, are suitably designed and qualified to deliver their safety functions;
> - anti-reverse function is validated during system commissioning;
> - endurance test is sufficient to qualify its operational life; and
> - seismic coast down qualification method is appropriate.

462. This Assessment Finding should be considered with AF-UKHPR1000-0130 in sub-section 4.2.1 of this report.

463. For the reactor coolant pump, I consider the RP has not shown suitable:

- Consideration of commissioning requirements to support qualification. This does not satisfy ONR SAP ECM.1 (Commissioning tests).
- Endurance testing to support qualification. This does not satisfy ONR SAP EMT.3 (Type-testing).
- Seismic qualification. This does not satisfy ONR SAP EQU.1 (Qualification procedures).
- Evidence that core heat removal can be maintained. This does not satisfy ONR SAP ERC.1 (Design and operation of reactors).

464. Given these gaps, I have raised Assessment Finding AF-UKHPR1000-0134.

Reactor Coolant System (RCP) [RCS] Pressuriser Safety Valves and Severe Accident Dedicated Valves

465. The Pressuriser Safety Valves (PSVs):

- have a safety function to provide RCP [RCS] overpressure protection during all normal operation and accident conditions (Category A / Class 1);
- allow primary circuit heat removal by opening (through 'feed and bleed' operation) during accident conditions;
- maintain the pressure boundary in normal operation and accident conditions; and
- fulfil an important role protecting the primary circuit from over-pressurisation in all conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

466. The SADVs:

- have a safety function to depressurise the Reactor Coolant System (RCP [RCS]), by opening in severe accident conditions (Category C / Class 3);
- have a safety function to maintain the pressure boundary in normal operations (Category A / Class 1); and
- fulfil an important role protecting the primary circuit from over-pressurisation during severe accidents. ERC.1 (Design and operation of reactors) is relevant.

467. Figure 11 and Figure 12 in Theme 2 (sub-section 4.2.1) provide an overview of the PSV and SADVs.

468. PSV and SADV EQ RGP includes ONR SAPs:

- EQU.1 (Qualification procedures) considers the demonstration that individual items can perform their safety functions under operational conditions; and
- ERC.1 (Design and operation of reactors) considers fundamental safety functions associated with reactor design and operations.

Pressuriser Safety Valves

469. The pressuriser is fitted with three parallel PSVs. Each PSV actuates using the following pilot valve types:

- Spring operated (passive)
- Solenoid operated (remotely activated)

470. PSV opening relies on the pilot valve operating correctly. I noted the pilot valve was not qualified against primary circuit debris. This relates to a feed and bleed scenario where primary circuit fluid may also be passing through the valve as opposed to the pressuriser steam bubble[‡‡‡‡]. This fluid may contain debris. RQ-UKHPR1000-1225 (Ref. 6) was raised to seek clarification.

471. The RP stated that:

- the pressuriser steam bubble is debris-free;
- the presence of debris, during feed and bleed operation, preventing PSV closure is recognised; and

[‡‡‡‡] *The pressuriser stream bubble accommodates pressure changes within the primary circuit.*

- primary circuit cleanliness was not considered, as a feed and bleed parameter, in its safety analysis.

472. Debris minimisation is normal business for any licensee. However, not showing the PSV pilot valve is resilient to debris is a shortfall against ONR SAP EQU.1 (Qualification procedures). I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0135: The licensee shall demonstrate, during detailed design, that the pressuriser safety valve and its pilot valve are qualified for “feed and bleed” operations, when liquid may pass through the valves.

<u>Severe Accident Dedicated Valves Operating Temperature</u>

473. The SADVs are required to:

- remain closed during normal operations (Class 1); and
- open when temperatures are well above normal operational values (Class 3).

474. The SADV specifications, (Ref. 98) and (Ref. 99), state different operating temperatures (see sub-section 4.2.1.4 in Theme 2 of this report). It was unclear:

- what temperature related to which safety function i.e. open and closed; and
- how the SADVs remain open at the elevated temperature.

475. RQ-UKHPR1000-1227, RQ-UKHPR1000-1347 and RQ-UKHPR1000-1715 (Ref. 6) were raised to seek clarification.

476. The RP confirmed:

- the SADV qualification temperature for remaining open; and
- they remain open as the valve design will not backwind.

477. SADV opening is designated a Category C / Class 3 SSC. Using normal industry standards, to qualify SADV opening, may be appropriate. However, the requirement to stay closed (in normal operations) and open (in a severe accident) must be independently qualified. This is because the requirement to stay closed is a Category A safety function. I consider this normal business.

478. For the SADVs, I consider the RP has shown it understands qualification requirements at elevated temperatures. This satisfies ONR SAP EQU.1 (Qualification procedures).

Safety Injection System (RIS [SIS]) In-Containment Refuelling Water Storage Tank Strainer

479. The RIS [SIS] strainers:

- have a safety function (Category A / Class 1) to filter the:
  - MHSI pump supply;
  - low head safety injection (LHSI) pump supply; and
  - supply to the containment heat removal (EHR) [CHRS] strainer for back-flushing.
- fulfil an important role preventing debris challenging the heat removal safety functions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

480. RIS [SIS] strainer EQ RGP includes:

- ONR SAP EQU.1 (Qualification procedures) relates to proving the SSCs can perform their safety function; and
- ONR Technical Assessment Guide NS-TAST-GD-094 Categorisation of Safety Functions and Classification of SSCs (Ref. 4) provides guidance on how qualification should be commensurate with the SSC's categorisation and classification.

481. I applied ONR SAP EQU.1 (Qualification procedures) to my assessment of the RP's "Equipment Classification List of Safety Injection System (RIS)" (Ref. 100). This states the RIS [SIS] strainer should "provide relatively clean water for safety injection". Strainer filtration performance requirements were not identified. RQ-UKHPR1000-RQ-0674 (Ref. 6) was raised to seek clarification.

482. The RP responded that:

- The IRWST may contain debris following an accident.
- The strainer design removes intolerable debris from the supply to the MHSI and LHSI pumps.
- The "Technical Specification for Medium Head Safety Injection Pumps" (Ref. 84) includes strainer performance requirements.

483. I am satisfied the safety case identifies RIS [SIS] strainer performance requirements. This satisfies ONR SAP EQU.1 (Qualification procedures).

484. The equipment classification list (Ref. 100) identified the RIS [SIS] strainers' EQ category as 'not applicable' (N/A). RQ-UKHPR1000-0674 and RQ-UKHPR1000-0788 (Ref. 6) were raised to seek clarification.

485. The RP stated that passive SSCs have no EQ category. Annex 2 of ONR's Categorisation and Classification TAG, NS-TAST-GD-094 (Ref. 4) indicates all SSCs undertaking safety functions should be proportionately qualified.

486. To address this gap, the RP updated its EQ methodology (Ref. 80) to Revision C. This updater required qualification of both active and passive SSCs. I consider this normal business.

487. For the RIS [SIS] strainer, EQ requirements and safety designation have been identified. This satisfies ONR SAP EQU.1 (Qualification procedures).

Safety Injection System (RIS [SIS]) Medium-Head Safety Injection Pump

488. The RIS [SIS] MHSI pump:

- has a safety function to provide borated water from the IRWST Tank to the RCP [RCS] in a fault or accident condition (Category A / Class 1);
- makes-up inventory of the accumulator in normal operating conditions (Note: this SSC safety function is not recognised); and
- fulfils an important role removing heat from the core. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

489. MHSI pump EQ RGP includes ONR SAP EQU.1 (Qualification procedures). This considers the application of EQ procedures to demonstrate safety functional performance.

490. The MHSI pump's operational endurance test is less than 5% of its mission time. 'Mission time' is the duration for which SSC performance is required without EIMT. RQ-UKHPR1000-1627 (Ref. 6) was raised to seek clarification.

491. The RP's response stated that the mission time has been selected based on the worst-case running time for the MHSI pump. Whilst this is conservative, the endurance test duration is less than 5% of this running time.

492. The RP's response did not justify how the MHSI pump's endurance test was sufficient. As an example, I would expect the endurance testing duration to be sufficient to show that safety related wear mechanisms have stabilised. This provides assurance that the pump can deliver its safety function.

493. The RP has not determined a running time based on an accident condition. Rather, it chose a worst-case duration from RGP (Ref. 91). The RP did not justify why its endurance testing is sufficient. Hence, I consider this to be a shortfall against ONR SAP EQU.1 (Qualification procedures).

494. I judge that the licensee will therefore need to consider this further during detailed design, to show that the endurance test duration is appropriate. I have therefore raised this as an Assessment Finding:

AF-UKHPR1000-0136: The licensee shall demonstrate, during detailed design, that the medium head safety injection pump's: ■ mission time is justified; and ■ endurance test shows that it can meet its required mission time.

Safety Injection System (RIS [SIS]) Residual Heat Removal Heat Exchangers

495. The RIS [SIS] RHR heat exchangers:

- have a safety function to remove residual heat from the core in normal and accident conditions (Category A / Class 1); and
- fulfil an important role in core heat removal. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

496. RIS [SIS] RHR heat exchanger RGP includes ONR SAP EQU.1 (Qualification procedures), which relates to the application of EQ procedures relevant to the SSCs safety classification.

497. I noted the following RIS [SIS] RHR heat exchanger EQ category designation shortfalls:

- The RIS [SIS] System Design Manual, (Ref. 83) Table T-4A-3, states EQ category as 'not applicable'.
- The EQ schedule (Ref. 95) states the EQ category as K3.

498. Recognising that the RIS [SIS] RHR heat exchangers are required to function during normal and accident conditions, I consider:

- The EQ category to be insufficient; and
- A K3ad EQ category should be considered.

499. This does not satisfy ONR SAP EQU.1 (Qualification procedures). This EQ designation shortfall does not undermine my confidence in the RHR heat exchanger performance. Hence, I have identified this as a Minor Shortfall**.**

Emergency Diesel Generators

500. The three EDGs:

- have a safety function to provide backup electrical supply in Loss of Offsite Power (LOOP) condition (Category A / Class 1).
- fulfil an important role in supporting safety systems controlling reactivity, core heat removal and confinement of radioactive material during LOOP conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

501. EDG EQ RGP includes:

- ONR SAP EQU.1 (Qualification procedures) considers the application of EQ procedures to demonstrate safety functional performance; and
- ONR's Emergency Power Generation TAG, NS-TAST-GD-103 (Ref. 4), which provides guidance on demonstration of safety functional requirements of EDGs.

502. It was not possible to understand the following from the "Technical Specification for the Emergency Diesel Generator" (Ref. 101):

- The qualification criterion for seismic response.
- The justification for endurance test duration.
- The basis for the ambient temperature extremes.

503. RQ-UKHPR1000-0984 and RQ-UKHPR1000-1758 (Ref. 6) were raised to seek further clarification.

<u>EDG seismic qualification</u>

504. In its response, the RP stated:

- It uses testing, analysis and combined methods to seismically qualify SSCs with a K3 EQ category.
- The EDGs and shock absorber mounting system are qualified by analysis.
- The EDG qualification satisfies IAEA No. NS-G-1.6, Seismic Design and Qualification for Nuclear Power Plants guidance (Ref. 102).

Note: K3 equipment is installed outside the primary containment boundary. It therefore needs to function under normal operation and seismic conditions.

505. I am content this seismic approach satisfies international RGP (Ref. 102). However, this is subject to a seismic analysis. This analysis should consider the Floor Response Spectra of the Diesel Generator Buildings, which I consider to be normal business.

506. Whilst recognising that the EDGs are required to function during accident and severe accident conditions, I consider:

- the EQ category to be insufficient; and
- a K3ad+SA EQ category should be considered.

507. This does not satisfy ONR SAP EQU.1 (Qualification procedures).

508. This EQ designation shortfall does not undermine my confidence in the EDG performance. Hence, I have identified this as a Minor Shortfall**.**

EDG endurance testing

509. In its response, the RP stated that its technical specification (Ref. 101) includes the duration of the full-load operational endurance test. This endurance test is circa 1% of the EDG's operational life.

510. Given the pedigree of the conventional EDG design, I consider this satisfactory. However, this judgement is subject to a full systems test being undertaken for all operational conditions. I consider this to be normal business.

EDG qualification temperature

511. In its response, the RP stated that its "Generic Site Related Design Values" (Ref. 103), includes an extreme outdoor air temperature range of -22 °C to 48.5 °C. These temperatures are used to qualify the EDG. During factory acceptance testing, the output power is adjusted to compensate for the operating temperature under test conditions.

512. I consider this response appropriate as it defines the EDG's qualification temperature requirements.

Overall EDG EQ conclusion

513. For EDGs I consider the RP has suitably identified EQ requirements. This satisfies ONR SAP EQU.1 (Qualification procedures).

4.3.2 Strengths

514. The RP has improved its understanding of EQ RGP.

4.3.3 Outcomes

515. As a result of my assessment, the RP:

- Improved its EQ Methodology
- Developed an EQ Schedule
- Linked EQ to mechanical SSC performance requirements

516. The RP has addressed my concerns raised within RO-UKHPR1000-0048, which I consider closed (Ref. 104).

517. RO-UKHPR1000-0048 has addressed gaps in the RP's EQ methodology. However, for site-specific stages, further improvements in EQ implementation are required.

518. I have raised four Assessment Findings in sub-section 4.3.1 concerning:

- application of the RP's EQ methodology;
- demonstrating reactor coolant pump anti-reverse function during system commissioning;
- sufficiency of reactor coolant pump endurance test;
- sufficiency of reactor coolant pump seismic coast down tests;
- managing risks relating to the reactor coolant pump seal debris;
- managing risks relating to PSV pilot valve debris; and

- MHSI pump endurance testing.

519. I have identified three Minor Shortfalls in paragraphs 449, 499 and 508. I am content these can be addressed during site-specific stages. These apply to the EQ arrangements, which should consider:

- a reactor coolant pump type test for operation without motor cooling;
- the RIS [SIS] RHR heat exchanger EQ designation; and
- the EDG EQ designation.

520. The Assessment Findings are listed in Annex 3.

4.3.4 Conclusion

521. I judge that the RP has:

- improved its understanding of EQ requirements;
- shown suitable EQ methodology implementation for GDA; and
- addressed my concerns raised in RO-UKHPR1000-0048.

522. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the adequacy of the RP's equipment qualification arrangements are sufficient from a Mechanical Engineering perspective.

523. I have identified several matters that the licensee will need to address during the detailed design. I have captured these in four Assessment Findings.

4.4 Theme 4: Gaps Against Mechanical Engineering Relevant Good Practice

524. Theme 4 assessed the RP's identification and application of RGP. This progressed from my Step 3 GDA conclusion (Ref. 22) that an adequate demonstration of RGP had not been provided. I would expect the generic safety case to demonstrate that the design has implemented Mechanical Engineering RGP during GDA.

525. Typical sources of RGP include:

- Approved Codes of Practice (ACoP) and guidance
- Published regulatory guidance
- Standards produced by national or international standards setting organisations
- Guidance agreed by a body or professional institute representing an industrial / occupational sector
- Unwritten sources such as well-defined and well-established standard practices adopted by an industrial / operational sector

526. If properly implemented, satisfying RGP should lead to an adequate demonstration that relevant risks are reduced ALARP. Identifying and implementing RGP is one recognised route to satisfy the law. ONR's ALARP guidance, NS-TAST-GD-005, has further information (Ref. 4).

527. As a result of my Step 3 finding, RO-UKHPR1000-0012 was raised (Ref. 105) to ensure the RP clearly articulates how any gaps or shortfalls against RGP may impact the generic UK HPR1000 design. The RO actions were:

ROA.1 Prepare a strategy for the comprehensive analysis of the relevant good practice applicable to the mechanical engineering UK HPR1000 reference design

- Submit a strategy to comprehensively analyse relevant good practice applicable to the UK HPR1000 mechanical engineering design.
- Provide clear links to the "mechanical engineering safety case" being made for UK HPR1000 i.e. relevant SSCs, safety function categorisation, SSC safety classification etc.
- Demonstrate its strategy has been developed with appropriate input from Suitably Qualified and Experienced Persons (SQEPs) familiar with the UK mechanical engineering nuclear safety context.

ROA.2 Undertake an analysis of the UK HPR1000 reference design against relevant good practice associated with mechanical engineering

- Identify the UK HPR1000 sources of mechanical engineering RGP.
- Consider relevant Operational Experience Feedback (OEF) and Operational Experience (OPEX) and justify its applicability.
- Provide a compliance / gap analysis that identifies where the UK HPR1000 design does not meet mechanical engineering RGP.
- Document the rationale / justification for the conclusions reached in the UK HPR1000 generic safety case.
- Demonstrate its RGP compliance / gap analysis has been undertaken with appropriate input from SQEP familiar with the UK mechanical engineering nuclear safety context.

ROA.3 Undertake a mechanical engineering RGP compliance / gap analysis against the UK HPR1000 generic design

- Identify UK HPR1000 SSCs where mechanical engineering RGP is not satisfied in the UK context (i.e. the shortfalls / gaps).
- Explain the significance of the shortfalls / gaps identified against mechanical engineering RGP. For example, whether design modifications might be required.
- Explain how the identified gaps, will be addressed during GDA.

528. In summary, RO-UKHPR1000-0012 required any gaps in RGP to be identified and adequately addressed by the RP, to demonstrate the generic UK HPR1000 design reduces relevant risks ALARP.

4.4.1 Assessment

4.4.1.1 Closure of RO-UKHPR1000-0012

529. To address ROA.1, the RP submitted its strategy for the analysis of RGP, first in December 2019 and finally in March 2020 (Ref. 106). This strategy set out the scope and process by which its alignment with RGP would be analysed. I judged the RP's strategy to be adequate for GDA.

530. For ROA.2, the RP undertook its analysis of the generic UK HPR1000 design's mechanical SSCs against RGP. Six ALARP demonstration reports were provided to underpin the RP's assessment and development of the generic UK HPR1000 design:

- ALARP Demonstration for Reactor Coolant System (Ref. 107);
- ALARP Demonstration Report for Safety Systems (Ref. 108);
- ALARP Demonstration for Auxiliary Systems (Ref. 109);
- ALARP Demonstration Report for Steam and Power (Ref. 110);
- ALARP Demonstration Report for Radioactive Waste Management (Ref. 111); and
- ALARP Demonstration Report of the PMC [FHSS] SSCs (Ref. 112).

531. These documents presented:

- the Reference Design;
- the RP's analysis of options; and
- its review of RGP and OPEX from operating sites and its decision-making process to avoid or reduce risk ALARP.

532. Finally, to address ROA.3, the RP assessed whether the extant design aligns with the RGP. Revision B of its "List of Gaps for Mechanical Engineering against RGP" (Ref. 113), presents the results of its assessment. This referenced:

- six ALARP demonstration reports;
- four optioneering study reports (Ref. 114, Ref. 115, Ref. 116, Ref. 117); and
- four impact assessment reports (Ref. 118, Ref. 119, Ref. 120, Ref. 121). These documents explained how the identified gaps would be taken forward.

533. The RP identified 53 gaps against RGP for Mechanical Engineering SSCs. The list of gaps document (Ref. 113) references the compliance analyses (Ref. 122, Ref. 123, Ref. 124, Ref. 125). These were produced by the RP to generate the list of gaps.

534. From my assessment, I judge the RP has:

- adopted a suitable RGP analysis strategy;
- analysed the reference design against RGP;
- undertaken a compliance / gap analysis;
- identified areas where RGP is not met; and
- implemented appropriate measures to secure RGP compliance for GDA.

4.4.1.2 Application of RGP

535. During my assessment of RO-UKHPR1000-0012 closure:

- I assessed the adequacy of the RP's ALARP assessments (Ref. 107) to (Ref. 112). This is discussed in sub-section 4.7 of my assessment report.
- I sampled the following SSCs in more detail to judge the adequacy of the RP's application of specific RGP.

Reactor Coolant System (RCP) [RCS] Severe Accident Dedicated Valves

536. The SADVs:

- have a safety function to depressurise the Reactor Coolant System (RCP) [RCS], by opening in severe accident conditions (Category C / Class 3);
- have a safety function to maintain the pressure boundary in normal operations (Category A / Class 1) (Ref. 55); and
- fulfil an important role protecting the primary circuit from over-pressurisation during severe accidents. ERC.1 (Design and operation of reactors) is relevant.

537. The SADVs fulfil an important role during normal operation and severe accident conditions. This is because over-pressurisation of the containment can progress to core melt.

538. RGP for the SADVs include ONR SAPs:

- EDR.1 (Failure to safety)
- EDR.2 (Redundancy, diversity and segregation)
- EKP.2 (Fault tolerance)
- ERL.2 (Measures to achieve reliability)
- EMC.25 (Leakage)
- EMT.1 (Identification of requirements)

539. The SADV design incorporates a cold water 'plug', which whilst in standby limits the operational inlet temperature to approximately 60 °C. The 'plug' protects the valves from long-term exposure to elevated primary circuit temperatures.

540. ONR SAP ERL.2 (Measures to achieve reliability) states that appropriate measures should be taken to ensure that the onset of failures will be detected. However, given it was not clear how loss of the 'plug' is detected or mitigated, RQ-UKHPR1000-1228 was raised to seek clarification (Ref. 6).

541. The RP responded that, in the case of loss of the ‘plug’, an alarm triggers an alert to operators. This prompts a leakage rate test of the primary circuit to be conducted. If the leakage rate is within an acceptable range, normal operation continues, and the leaking valve is repaired at the next planned shutdown. The RP claims that the short-term loss of the water plug alone does not detrimentally impact the SADV’s safety function.

542. Given the short exposure time and subject to appropriate EQ to validate this, I consider this response acceptable.

543. The SADV design uses an electric actuator for remote operation and a handwheel for manual operation. ONR SAP EKP.2 (Fault tolerance) states that failures or maloperation should change a plant state towards a safer condition or produce no significant response. However, I perceived a risk that the valve could remain in manual mode when remote actuation is required. RQ-UKHPR1000-1349 and RQ-UKHPR1000-1543 were raised to seek clarification (Ref. 6).

544. The RP responded with a description of the clutch design (used to switch between manual and electric operation) and the operation sequences, which is summarised as follows:

- The clutch design uses a manual-electric ‘half-clutch’ (jaw or dog clutch type) with automatic return to the electric actuation position.
- The handwheel is for use only during maintenance activities with the plant in the cold state.
- SADV actuation, in an accident scenario, is undertaken remotely via the Digital Control System.

545. I note the design features an automatic return to electric actuation, which reverts the system to a safe state following manual actuation. I consider this acceptable.

546. Two parallel trains of SADVs aim to reduce the probability of failure on demand (pfd) for the pressure relief system. ONR SAP EDR.2 (Redundancy, diversity and segregation) requires demonstration that the required level of reliability for the SSC’s intended safety function has been achieved. However, for the SADVs, I judge that redundancy could increase the risk of spurious opening. RQ-UKHPR1000-1348 was raised to seek clarification (Ref. 6).

547. The RP confirmed that for either train to relieve pressure, both valves in a single train must open. Adequate diversity provisions were claimed to be in place in the form of:

- valve types (globe and gate);
- electrical divisions (A or B); and
- power supplies (normal, emergency diesel generators, station black-out generators, batteries).

548. I consider the response acceptable because diversity has been shown on several levels, reducing the risk of Common Cause Failure (CCF).

549. ONR SAP EMC.25 (Leakage) addresses the means of detection, location, monitoring and management of leakages. The RP claims that bellow seals should be provided when the conveyed fluid is radioactive. However, no evidence was provided for the SADVs. RQ-UKHPR1000-1349 was raised to seek clarification (Ref. 6).

550. The RP responded that the SADVs were equipped with live-loaded packing only. 'Live loading' is the application of a spring load (applied via Belleville type spring washers) to the gland follower of a packed valve. This is considered effective at reducing the loss of packing stress, and hence valve leakage. SADV seal leakage would be recovered by the Nuclear Island Vent and Drain System RPE [VDS]. I consider this response acceptable.

551. The SADV design includes a 'backseat'. This is a temporary stem-sealing arrangement, commonly used in industry, for 'on-line' replacement of valve-stem packing. ONR SAP EMT.1 (Identification of requirements) addresses the safety requirements for EIMT procedures. However, no evidence was provided for how the use and maintenance of the 'backseat' is managed to reduce risk to operators and ensure reliable sealing. RQ-UKHPR1000-1349 was raised to seek clarification (Ref. 6).

552. The RP responded that the 'back-seat' is only used in 'special circumstances' as a back-up / redundant function, i.e. EIMT of the valve whilst still installed on the pipework. I consider this response acceptable. This should align with the ongoing activities during the site-specific stages. This should demonstrate compliance with guidance on safe isolation of plant and equipment (HSG253) (Ref. 126) for the wider plant (see sub-section 4.5 of this report for further information).

553. I am satisfied that the RP has addressed RGP for the RCP [RCS] severe accident dedicated valves. It has satisfied my expectations regarding ONR SAPs:

- EDR.1(Failure to safety)
- EDR.2 (Redundancy, diversity and segregation)
- EKP.2 (Fault tolerance)
- ERL.2 (Measures to achieve reliability)
- EMC.25 (Leakage)
- EMT.1 (Identification of requirements)

554. It has also shown diversity and 'failure to safety' within the design together with the use of appropriate procedural measure and controls.

Reactor Coolant System (RCP [RCS]) Control Rod Drive Mechanism

555. The Control Rod Drive Mechanisms (CRDMs):

- have a safety function which contributes to reactivity control during normal, fault and accident conditions (Category A / Class 1);
- following a PIE, release the Rod Control Cluster Assembly (RCCA) to facilitate and maintain sub-critical reactor core conditions;
- support confinement of radioactive material as part of the primary circuit pressure boundary; and
- fulfil an important role controlling reactivity and confining radioactive material. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

556. RGP for the CRDMs includes:

- ONR SAPs:
    - SC.2 (Safety case process outputs) relates to clarity and structure of the safety case;

- MS.4 (Learning) relates to lessons learned from internal and external sources to improve safety performance; and
- EMC.3 (Evidence) relates to metallic component integrity. It states that evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations identified in the safety case.

■ OPEX:

- IAEA – Nuclear Power Plant Operating Experience from the IAEA/NEA International Reporting System for Operating Experience 2005 to 2008 (specifically page 23) (https://www-ns.iaea.org/downloads/ni/irs/npp-op-ex-05-08.pdf#page=23)
- AP1000 – ONR Generic Design Assessment – New Civil Reactor Build, Step 4 Mechanical Engineering Assessment of the Westinghouse AP1000® Reactor (specifically page 53) (https://www.onr.org.uk/new-reactors/reports/step-four/technical-assessment/ap1000-me-onr-gda-ar-11-010-r-rev-0.pdf#page=51)

557. Operational Experience from the International Atomic Energy Agency (IAEA) (Ref. 127) indicates there is a history of CRDMs sticking.

558. OPEX from Westinghouse's AP1000 design shows that the stainless steel shims intended to address the sticking (Ref. 128) have cracked during endurance testing.

559. However, for the CRDMs, I found no evidence that this OPEX had been adequately considered or addressed e.g. to mitigate the risk of shims fracturing in service. RQ-UKHPR1000-1624 sought further clarification (Ref. 6).

560. The RP responded that the CRDM design reduces the tendency to 'stick' due to residual magnetic attraction. This is achieved by reducing the magnetic forces between the operating components. I consider this response acceptable.

561. In relation to the shim cracking (Ref. 128), the RP responded that the cracking seen during the endurance testing of AP1000 has been taken into consideration in the UK HPR1000 CRDM design. The UK HPR1000 shims are made of nickel-based alloy instead of austenitic stainless steel which is used in the AP1000 (and CPR1000).

562. The nickel-based alloy has better impact, fatigue and corrosion resistance than the austenitic stainless steel. The RP responded that a CRDM prototype, using the nickel-based alloy shims, has been endurance tested. Subsequent inspection revealed them to be in a good condition. I consider this response acceptable, subject to a suitable endurance test.

563. I applied ONR SAPs SC.2 (Safety case process outputs) and EMC.3 (Evidence) against the RP's "Technical Specification for Control Rod Drive Mechanism" (Ref. 82). I noted it did not contain sufficient detail. For example, it makes statements such as "…serious cold hardening are not allowed…", "…except instantaneously or locally heating…" and "…plating shall be performed… …to increase their wear resistance…" yet it does not define 'serious', 'instantaneous', 'local' or quantify the level of wear resistance.

564. I am satisfied that the RP has adequately addressed RGP for the CRDMs. It has satisfied my expectations regarding ONR SAP MS.4 (Learning) by demonstrating how

the design is resilient to specific weaknesses in similar designs, in particular the IAEA (Ref. 127) and AP1000 OPEX (Ref. 128).

565. I judge that the CRDM Technical Specification requires more manufacturing information. I judge this to be a Minor Shortfall against ONR SAPs SC.2 (Safety case process outputs) and EMC.3 (Evidence). The licensee can address this during the detailed design and site-specific stages.

Safety Injection System (RIS) [SIS] In-Containment Refuelling Water Storage Tank Strainer

566. The RIS [SIS] strainers:

- have a safety function (Category A / Class 1) to filter the:
  - MHSI pump supply;
  - LHSI pump supply; and
  - supply to the containment heat removal (EHR [CHRS]) strainer for back-flushing.
- fulfil an important role preventing debris challenging heat removal safety functions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

567. RGP for the RIS [SIS] IRWST strainers includes:

- ONR SAPs:
  - EQU.1 (Qualification Procedures) considers suitability of qualification procedures.
  - EMT.3 (Type-testing) considers type testing conditions, which should be equal to, at least the most onerous design condition
  - EMT.4 (Validity of equipment qualification) considers that the validity or equipment qualification should not be degraded by EIMT activities.

568. I reviewed the “Technical Specification for IRWST Sump Strainers” (Ref. 129) and noted that:

- the RIS [SIS] strainer testing assumes an equal distribution of debris loading;
- the strainer performance testing was undertaken with lower water temperature compared with accident conditions; and
- two grades of mechanical fasteners (bolts) are specified.

569. I raised RQ-UKHPR1000-1555 (Ref. 6) to clarify:

- How an equal debris loading distribution across the RIS [SIS] strainers is a conservative approach given they are not equally spaced around the reactor building. ONR SAP EMT.4 (Validity of equipment qualification) is relevant here.
- How qualification (testing or analysis) shows the RIS [SIS] strainers can perform their safety functions for accident conditions. ONR SAPs EMT.3 (Type-testing) and EQU.1 (Qualification Procedures) apply.
- How the material selection for the strainer fasteners is proposed and how it reduces risk during operations such as EIMT to ALARP.

570. The RP responses, along with my judgements are:

Debris distribution

- It acknowledges that the equal debris loading may not be conservative. It also noted that the strainers used in the reference design (FCG3) are designed so that each strainer can bear 100% of the assumed debris. As this is based on fibrous insulation used within containment, the design change for the generic UK HPR1000 design to reflective metallic insulation (see sub-section 4.8 of this report) reduces the debris loading significantly as the fibres are the major source of blockages.
- I consider this to be appropriate. However, the licensee should review its assumption of equal debris across strainers as part of normal business.

Qualification tests

- Test conditions are selected by manufacturers. These consider both their relevance to operating and accident conditions and the safety of personnel.
- The conditions consider a correction formula. This is derived from a NUREG study of the Potential for Boiling Water Reactor (BWR) Emergency Core Cooling System (ECCS) Strainer Blockage Due to Loss of Cooling Accident (LOCA) Generated Debris (see report at https://doi.org/10.2172/184044). Evaluation of the test results is carried out based on the RCC-M standard and incorporates finite element analysis.
- This does not align with ONR SAP EMT.3 (Type testing), which states that "structures, systems and components should be type tested before they are installed to conditions equal to, at least, the most onerous for which they are designed".
- Whilst the RP argues that conditions are modified in accordance with industry practice, I judge this to be a Minor Shortfall. I expect the licensee to review the EQ and type testing methods during detailed design and site-specific stages, to determine if more appropriate tests can be undertaken.

Grading of fasteners

- The specification identified two possible grades. It is normal for the supplier to choose one single grade for fasteners. As a result, the concern over misuse of fasteners during EIMT is eliminated.
- The RP's response resolves the concern relating to mixing of fasteners. It aligns with ONR SAP EMT.4 (Validity of equipment qualification). However, this is dependent on the supplier or manufacturer acting as the RP assumes. I expect the licensee to manage this appropriately during detailed design and site-specific stages as normal business. This should meet ONR's expectations in TAG NS-TAST-GD-077 concerning Supply Chain Management (Ref. 4).

571. I am content that the RP has addressed RGP for the RIS [SIS] IRWST strainers. It has satisfied my expectations regarding appropriate qualification procedures against ONR SAPs EQU.1 (Qualification procedures) and EMT.4 (Validity of equipment qualification). Whilst I have identified a Minor Shortfall against EMT.3 (Type testing), this does not impact my overall judgement that the RIS [SIS] IRWST strainers address RGP.

Safety Injection System (RIS) [SIS] Residual Heat Removal Heat Exchanger

572. The RIS [SIS] RHR heat exchangers:

- have a safety function to remove residual heat from the core in normal and accident conditions (Category A / Class 1); and
- fulfil an important role in core heat removal. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

573. RGP for the RIS[SIS] RHR heat exchangers include:

  - ONR SAP ECS.3 (Codes and standards) states that "SSCs that are important to safety should be designed, manufactured, constructed…to the appropriate codes and standards"
  - Standards of the Tubular Exchanger Manufacturers Association (TEMA) (see http://kbcdco.tema.org). These are an important source of RGP for the design and manufacture of industrial shell-and-tube heat exchangers. The TEMA standards should be used alongside key design codes such as RCC-M.

574. When applying the above RGP to the RHR heat exchangers, the sole reference to TEMA was as specified by RCC-M for calculation of the tube-sheet thickness. I expect TEMA to be applied for other aspects of the heat exchanger design, which are not accounted for in RCC-M. RQ-UKHPR1000-1190 was raised to seek clarification and evidence for the wider application of TEMA (Ref. 6).

575. The RP responded with examples of where TEMA is applied for aspects of the heat exchanger other than the tube-sheet thickness, which included:

  - tube to baffle clearances (TEMA Section RCB-4.2);
  - baffle to shell clearance (TEMA Section RCB-4.3);
  - baffle / support plate thickness (TEMA Section RCB-4.4);
  - tube-sheet hole diameters (TEMA section RCB-7.21);
  - baffle spacing (TEMA Section RCB-4.52); and
  - implement tube bundle protection from impinging fluid for high shell side entrance velocities (TEMA Section RCB-4.61).

576. The RP also provided an excerpt of the thermal design calculations. These were performed using software known to be capable of realising designs that are TEMA-compliant.

577. The RP's response showed that TEMA standards are applied for certain aspects of the RHR heat exchanger design not explicitly covered by RCC-M. I consider this response acceptable for GDA. This should be followed up during detailed design and site-specific stages as normal business to ensure that TEMA is applied as required.

578. I am satisfied that the RP has addressed RGP for the RIS [SIS] heat exchanger. It has satisfied my expectations regarding SAP ECS.3 (Codes and standards) and compliance with TEMA standards by providing examples of the standards' application.

Component Cooling Water System (RRI) [CCWS] Containment Isolation Valve

579. The RRI [CCWS] containment isolation valves:

  - have safety functions to:

  - close and maintain pressure under accident conditions and providing confinement of radioactivity (Category A / Class 1) (Ref. 130); and
  - allow flow through the containment boundary to fulfil a range of cooling functions during normal operation (range of categories and classifications).

- fulfil an important role, in both normal and accident conditions, as failure could lead to inadequate cooling of the wider plant. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

580. RRI [CCWS] containment isolation valves RGP includes ONR SAPs:

- ECS.3 (Codes and standards) considers the application of appropriate codes and standards;
- ESS.21 (Reliability) considers that the design of safety systems should avoid complexity and apply a failsafe approach; and
- EMC.3 (Evidence) considers that evidence should be provided to show that the necessary level of integrity has been achieved for the most demanding situations identified in the safety case.

581. At each of the RRI [CCWS] containment penetrations, the containment isolation valves consist of a pair of valves arranged in series. One inside and one outside containment. Different valve arrangements are utilised for upstream valve pairs (where the flow is entering the containment boundary) compared to the downstream valve pairs (where the flow is leaving the containment boundary).

582. When applying ONR SAP ESS.21 (Reliability) to the rationale and function of some supporting valves, I noted this was not clearly presented. RQ-UKHPR1000-1181 was raised to seek clarification (Ref. 6).

583. The RP responded with an explanation of the supporting valves, which exist to provide a pressure balance system on a section of pipe between two closed gate valves. The intent of this is to avoid a dangerous pressure rise in a closed length of pipe in the event of a rise in temperature. Check valves are selected to avoid additional complexity in the system and to automatically provide this pressure balancing function.

584. I judge that the RP has justified the presence and function of the additional balance valves. It confirmed that the safety category and classification are commensurate with the containment isolation valves. This is essential as failure of these valves could lead to a failure of containment isolation. I consider this response acceptable.

585. I applied ONR SAP EMC.3 (Evidence) to the list of valves provided in the RP's "Requisition and List for Nuclear Island Isolation Valves" (Ref. 65). I noted that it did not contain information for all the containment isolation valves for the RRI [CCWS] system. Given inconsistencies in the documentation, I was unable to determine how the valves were classified and controlled. RQ-UKHPR1000-1181 also covered this matter (Ref. 6).

586. The RP responded that, due to the large number of valves in the system, only a selection was included in the documentation. It stated that it had provided technical information for the valves that had the harshest design requirements and qualification parameters. The RP was able to provide the additional information requested. This confirmed the safety category and class of the missing valves to be in line with the rest of the system.

587. I consider this response acceptable. Consistent information should be presented in its "Requisition and List for Nuclear Island Isolation Valves". I consider this to be normal business. This can be done during detailed design and site-specific stages.

588. Section 6.2 of the "Gate Valve Specification for Nuclear Island" (Ref. 78) referred to several forbidden materials. These forbidden materials were limited to stainless steel valve components. RQ-UKHPR1000-1769 was raised to seek clarification (Ref. 6).

589. The RP responded that the following forbidden material sources of information are considered for the generic UK HPR1000 design:

- RGP
- OPEX
- The Advanced Light Water Reactor Utility Requirements Document (URD) (Ref. 131)
- European Utility Requirements (EUR) (Ref. 132)

590. The RP also confirmed that it will consider existing sources of RGP related to prohibited materials.

591. I am content that the RP has addressed RGP for the RRI [CCWS] containment isolation valve. I judge it has:

- satisfied my expectations regarding ONR SAPs ESS.21 (Reliability), EMC.3 (Evidence) and ECS.3 (Codes and standards);
- clarified the function and justification of the system layout, demonstrating the required technical information for the valves; and
- suitably considered forbidden materials.

592. The above is subject to consistent information being presented in the "Requisition and List for Nuclear Island Isolation Valves" (Ref. 65) and the "Gate Valve Specification for Nuclear Island" (Ref. 78). I consider this to be normal business.

Essential Service Water System (SEC) [ESWS] Centrifugal Pump

593. The SEC [ESWS] centrifugal pump:

- has a safety function to provide cooling water for the Component Cooling Water System (RRI [CCWS]) in both normal and accident conditions (Category A / Class 1); and
- fulfils an important role in supporting reactor core heat removal during normal and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

594. The SEC [ESWS] pump fulfils an important role during normal and accident conditions. A failure to force flow through the SEC [ESWS] or RRI [CWCS] heat exchanger could prevent cooling of components and inhibit plant safety measures.

595. RGP for the SEC [ESWS] centrifugal pump includes:

- ONR SAPs:
    - EMC.11 (Failure modes) considers that failure modes should be gradual and predictable; and

- ESS.21 (Reliability) considers that where faults are not easily detected (revealed) at the time of occurrence, in-service testing or inspection should be specified to support reliability claims.

596. I applied the above SAPs considering resilience to detrimental mechanisms, such as dead-leg phenomena and water-hammer. I consider these vital to controlling the risks of unpredictable failures. However, no such evidence was provided for the SEC [ESWS]. RQ-UKHPR1000-0245 and RQ-UKHPR1000-1384 were raised to seek clarification (Ref. 6).

597. The RP responded to RQ-UKHPR1000-0245 providing examples of RGP used to ensure all systems are resilient to water hammer. This included IAEA Safety Standards, European Utility Requirements (EUR) and EPRI reports. Optimisation measures will initially be applied at the system level. This should reduce the risks prior to refining component performance following the results of more detailed transient analysis. This includes:

- Piping system layout design, such as removing the elbow sited close to a quick-open valve (for example, a safety valve) to eliminate the hydraulic load induced by the valve opening.
- Operating scheme, such as avoiding starting the second pump in the parallel trains when shutting down the first pump simultaneously to eliminate the hydraulic load induced by the pump operation.
- Equipment sizes, such as extend the closing time of a check valve to reduce the hydraulic load during valve closing.

598. In its response to RQ-UKHPR1000-1384, the RP stated that the potential for water-hammer is mitigated. This is achieved by regulating the closure time of the check valve at the outlet to the pump, with ‘two-stage closing’. Regarding seawater accelerated corrosion risks, the RP confirmed that the different trains within the SEC [ESWS] are routinely cycled. Furthermore, a robust inspection schedule will be implemented. This includes vent and drain pipes and appropriate material selection implemented throughout the pipework design.

599. The extension of the check valve closure time should reduce the size of sudden pressure surges within the SEC [ESWS]. Routine cycling of the different trains should also reduce the periods of local stagnation within the system pipework. This can reduce the likelihood of severe corrosion. I consider this response acceptable. This is subject to more detailed transient analysis at the system level and a complimentary in-service inspection plan being produced during detailed design and site-specific stages. I consider this to be normal business for the licensee.

600. I am satisfied the RP addressed RGP for the SEC [ESWS] centrifugal pump. It has satisfied my expectations regarding ONR SAPs EMC.11 (Failure modes) and ESS.21 (Reliability). The RP considered the detrimental hydraulic phenomena, implementing operational and surveillance measures. These measures protect against water hammer and accelerated corrosion in ‘dead legs’.

Liquid Waste Treatment System (TEU [LWTS]) Process Drains Storage Tank

601. The TEU [LWTS] process drains storage tanks:

- have a safety function to safely store various liquid wastes in normal operation conditions (Category C / Class 3) (Ref. 133);
- failure could result in loss of liquid waste containment;

- fulfil an important role during normal operation.

602. In the event of a tank rupture, failure to adequately size the tank bunds (retention pits) could result in non-confinement of liquid waste.

603. RGP for the TEU [LWTS] process drains storage tanks includes:

- ONR SAP ERL.4 (Margins of conservatism) considers that the safety case should include a margin of conservatism to allow for uncertainties.
- HSE Technical Measures guidance relating to Control of Major Accident Hazards (COMAH 2015) Regulations - secondary containment bunds www.hse.gov.uk/comah/sragtech/techmeascontain.htm. This addresses several related topics. These include secondary containment and states, under 'bunds', that they should be sized to hold 110% of the maximum capacity of the largest tank. This provides some margin for the addition of foam during response to the emergency.

604. I applied the above RGP to the TEU [LWTS] system. I noted the capacity of the retention pits (bunds) for all liquid radwaste storage tanks did not appear to be conservative. RQ-UKHPR1000-1050, RQ-UKHPR1000-1191 and RQ-HPR1000-1710 were raised to seek further clarification (Ref. 6).

605. The RP responded that all bund designs were sized to at least 110% of the tanks standard design useable volume of 50 m^3 thus complying with the HSE guidance relating to COMAH. It clarified that the maximum nominal volume was calculated from the fill level being at the same height as the overflow nozzles. I noted that the L-shaped overflow pipe is approximately 0.5 m above the indicated 50 m^3 volume 'high level', which may require the margin to be increased slightly.

606. I consider this response acceptable. This is subject to the geometry of the overflow pipe being considered and corresponding margins provided during detailed design and site-specific stages. I judge this to be normal business associated with tank and bunding design.

607. For the TEU [LWTS] system, the tank capacities related to the following were unclear:

- how the numbers of storage tanks for the sub-systems are decided;
- what liquid waste production OPEX data exists; and
- what levels of conservatism exists for the waste collection.

608. RQ-UKHPR1000-1423 was raised to seek further justification (Ref. 6).

609. The RP confirmed the different numbers of sub-system storage tanks across both the TEU [LWTS] and Nuclear Vent and Drain System (RPE) [NVDS] systems that were required for adequate liquid waste collection. The response also provided the relevant OPEX data. This was from the RP's operating fleet with liquid radwaste production rates from similar systems, used to size the sub-systems storage capacities. The RP's response confirmed that the range of margin for waste storage tanks was between 11% and 32% for those sampled. I consider this response acceptable.

610. I am satisfied that the RP has addressed RGP for the TEU [LWTS] process drains storage tanks. It has satisfied my expectations regarding ONR SAP ERL.4 (Margins of conservatism) and HSE guidance on compliance with COMAH Regulations. It has shown capability to store liquid waste by using reasonable assumptions for the volumes produced and providing measures to accommodate this, with suitable margins.

Safe Isolation of Plant and Equipment (HSG253)

611. Although HSG253 (Ref. 126) is RGP related to the safe isolation of plant and equipment, I have specifically considered this as part of Theme 5. Theme 5 considers the adequacy of the RP's EIMT arrangements. HSG253 implementation allows EIMT activities to be undertaken on safely isolated systems.

Control of Diesel Engine Exhaust Emissions in the Workplace (HSG187)

612. When there is a potential for gaseous diesel emissions into a building, there is a risk of asphyxiation. Therefore, I consider HSE's guidance on Control of Diesel Engine Exhaust Emissions in the Workplace, HSG187 (Ref. 134) to be relevant.

613. RQ-UKHPR1000-0367 queried whether the Diesel Generator Building HVAC system meets the requirements of HSG187. The RP's "HVAC Systems Analysis Report – Site Adaptability Modification in UK HPR1000" (Ref. 135) stated "…there is no specific standard for the design of the ventilation systems for diesel buildings in the UK".

614. The RP confirmed its HVAC design can meet the HSG187 guidance as the diesel generators have designated exhausts. The air intake is approximately 20 metres lower than the diesel exhaust outlet. The diesel hall air quality can be maintained at a sufficient level. I consider this response acceptable.

4.4.2 Strengths

615. The RP had performed a limited consideration of the generic UK HPR1000 design's alignment with RGP. The RP's engagement with me during my assessment has strengthened its alignment with RGP, which provides improvement in reducing risk to ALARP.

4.4.3 Outcomes

616. As a result of my assessment, the RP made the following changes:

- It acknowledged that its assessment of RGP required improvement and implemented improvements, in line with my expectations.
- It acknowledged TEMA as RGP. This has provided assurance that the standard will be applied in the UK HPR1000 heat exchanger design, citing evidential calculations from the reference design.

617. I judge that the RP has adequately addressed my concerns raised within RO-UKHPR1000-0012 and that the RO is closed (Ref. 136).

618. I have not raised any Assessment Findings related to Theme 4.

619. I have identified two Minor Shortfall in paragraphs 565 and 0 above, which I am content can be addressed during the detailed design and/or site-specific stages phase.

4.4.4 Conclusion

620. I judge the RP has:

- implemented an appropriate strategy for the analysis of Mechanical Engineering RGP;
- analysed the reference design against RGP;
- completed a suitable gap analysis identifying areas that did not meet RGP; and

- implemented appropriate measures to secure compliance for GDA.

621. I am satisfied, for the purpose of GDA, that the RP has addressed my concerns regarding its analysis of RGP gaps from GDA Step 3. It has:

- assessed RGP and implemented design modifications where necessary; and
- addressed my concerns raised within RO-UKHPR1000-0012.

622. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's consideration of relevant good practice is sufficient from a Mechanical Engineering perspective.

4.5 Theme 5: Adequacy of Examination, Inspection, Maintenance and Testing Arrangements

623. My Step 3 assessment (Ref. 22) identified EIMT as an area for improvement. It concluded:

- During Step 4, further evidence is required to demonstrate the UK HPR1000 asset management arrangements are adequate.

624. ONR raised RO-UKHPR1000-0021 (Ref. 137). It sought EIMT evidence for SSCs including:

- how EIMT links to the safety case;
- how UK EIMT specific legal requirements will be identified and addressed;
- the UK HPR1000 EIMT plan; and
- how operating rules inform EIMT requirements.

625. The RO Actions (ROA) were:

ROA.1 Examination, Maintenance, Inspection and Testing (EMIT) Strategy

- Provide a strategy which explains how EMIT will be derived, justified and included within the safety case for the generic UK HPR1000 design. This should adequately describe the scope of the EMIT aspects of the safety case to be produced during GDA, and what is proposed to be carried over to site specific stages.

ROA.2 Demonstration that the UK HPR1000 design and safety case is compatible with the EMIT Strategy

- Provide sufficient information to demonstrate that the UK HPR1000 generic safety case is consistent with the EMIT strategy produced in response to Action 1.

626. EIMT related RGP includes:

- ONR SAPs (Ref. 2):
  - EMT.1 (Identification of requirements)
  - EMT.2 (Frequency)
  - EMT.3 (Type-testing)
  - EMT.4 (Validity of equipment qualification)
  - EMT.5 (Procedures)
  - EMT.6 (Reliability claims)
  - EMT.7 (Functional testing)
  - EMT.8 (Continuing reliability following events)
  - EAD.1 (Safe working life)
  - EAD.2 (Lifetime margins)
  - EAD.3 (Periodic measurement of material properties)
  - EAD.4 (Periodic measurement of parameters)

- EAD.5 (Obsolescence)
- ELO.1 (Access)
- ERC.1 (Design and operation of reactors)
- EPS.3 (Pressure relief)
- ECS.3 (Codes and standards)
- EDR.1 (Failure to safety)

■ ONR TAGs (Ref. 4):

- NS-TAST-GD-009 Examination, Inspection, Maintenance and Testing of Items Important to Safety; and
- NS-TAST-GD-098 Asset Management.

■ Industry guidance:

- Health and Safety Executive (HSE) HSG253, The safe isolation of plant and equipment (Ref. 126);
- WENRA Safety Reference Level Issue K: Maintenance, In-Service Inspection and Functional Testing (Ref. 26); and
- IAEA Safety of Nuclear Power Plant; Design, Specific Safety Requirements SSR-2/1 (Ref. 11).

627. My EIMT assessment considered the following systems given their nuclear safety importance:

■ Safety Injection System (RIS [SIS]);
■ Containment Leak Rate Testing and Monitoring System (EPP [CLRTMS]);
■ Main Control Room Air Conditioning System (DCL [MCRACS]);
■ Liquid Waste Treatment System (TEU [LWTS]);
■ Main Steam System (VVP [MSS]); and
■ Reactor Building Handling Equipment System (DMR [RBHES]).

628. Given the EIMT gaps identified by RO-UKHPR1000-0021 (Ref. 137), my assessment considered the RP's:

■ EIMT strategy – what EIMT is required;
■ EIMT plan – when is EIMT undertaken; and
■ safe isolation arrangements – how safe EIMT is achieved.

4.5.1 Assessment

4.5.1.1 Closure of RO-UKHPR1000-0021

ROA.1 EIMT Strategy

629. RO-UKHPR1000-0021.A1 required the RP to consider its "Examination, Maintenance, Inspection and Testing Strategy" (Ref. 138). I consider the EIMT strategy to be adequate as it:

■ provides a UK HPR1000 EIMT scope;
■ distinguishes between planned and preventative EIMT;
■ provides a periodic testing regime;

- includes a compliance matrix against regulatory expectations / requirements for GDA; and
- identifies EIMT activities for safety Class 1 and 2 SSCs. Note: I also considered a safety Class 3 SSC within the scope of the Mechanical Engineering assessment.

630. I am satisfied that the RP has addressed EIMT RGP. It has satisfied my expectations regarding ONR SAP EMT.1 (Identification of requirements).

ROA.2 EIMT Plan

631. RO-UKHPR1000-0021.A2 required the RP to demonstrate its design and safety case is compatible with its EIMT Strategy. In response, the RP submitted:

- The “EMIT Windows” reports (Ref. 139) and (Ref. 140).
  These reports identified when EIMT can be undertaken
- The “EMIT Consistency Analysis” (Ref. 141).
  This report identified inconsistencies against legal requirements

632. ONR SAPs EMT.1-8 expect EIMT activities to be undertaken safely. The safety case identified that RIS [SIS] (Safety Class 1 system) periodic testing included unplanned intrusive EIMT during reactor operations. It was unclear how these EIMT activities could be undertaken safely. I considered this to be a shortfall.

633. RQ-UKHPR1000-1352,1599 and 1749 (Ref. 6) were raised to seek clarification.

634. To address EIMT shortfalls, the RP concluded:

- un-planned intrusive EIMT conditions should be the same as planned EIMT conditions i.e. safe isolation arrangements must be shown;
- this applies to primary and secondary circuit systems; and
- intrusive EIMT should be forbidden during power operations, unless safe isolation arrangements are proven.

635. This commitment is recorded in Revision C of its RIS [SIS] HSG253 Compliance Analysis (Ref. 142).

636. I am satisfied that the RP has shown that EIMT can be undertaken safely in accordance with its strategy. It has satisfied my expectations regarding:

- ONR SAPs EMT.1-8 series (Maintenance, inspection and testing), and
- NS-TAST-GD-009 Examination, Inspection, Maintenance and Testing of Items Important to Safety (Ref. 4).

637. I consider the RO-UKHPR1000-0021 submissions have shown:

- an adequate EIMT strategy; and
- the safety case is compatible with its EIMT strategy.

638. Further detail of the RO-UKHPR1000-0021 submissions is provided in the Fault Studies closure note (Ref. 143).

4.5.1.2 Adequacy of HSG253 Isolation Arrangements

Safe isolation arrangements

639. Safe isolations RGP includes HSG253 (Ref. 126), which provides guidance on safe isolation. This is to mitigate the worker risks while undertaking live maintenance. It recommends an isolation scheme, based on:

- assessment of plant failures occurring during an isolated activity;
- the likelihood of failure; and
- consequences.

640. It is important to note that the first step before undertaking intrusive maintenance is to consider the reasonable practicability of shutting down (i.e. reduce or remove hazard).

641. HSG253 considers process isolation safety e.g. intrusive maintenance on live plant. This considers:

- safe isolation;
- drainage; and
- pressure monitoring.

642. HSG253 excludes:

- Emergency situations where loss of containment has occurred, and immediate isolation of inventory is required.
- Non-process plant and equipment (e.g. powered access equipment used during isolation activities).

643. HSG253 considers carcinogenic substances but excludes a radiological exposure substance category. To allow radiological hazards to be considered, the RP developed a new category. This was included in its HSG253 scheme and was accepted by ONR's Radiological Protection inspector (Ref. 144).

644. Figure 5 in HSG253 shows the flow chart for selection of an ALARP isolation methodology.

645. Other sources of RGP concerning safe isolation arrangements include ONR SAPs:

- EMT.1 (Identification of requirements) considers that safety requirements for EIMT should be identified in the safety case;
- ECS.3 (Codes and standards) identifies the importance of applying appropriate codes and standards; and
- ERC.1 (Design and operation of reactors) relates to fundamental safety functions associated with reactor design and operations including:
  - control of reactivity;
  - removal of heat; and
  - confinement of radioactive material.

646. Given the significance of HSG253, I assisted the RP with its understanding. The RP then undertook a compliance analyses of the following fluid systems:

No.	System Code	System Name	No.	System Code	System Name
1	ADG [FDTGSS]	Feedwater Deaerating Tank and Gas Stripper System	21	LHV	NI 10kV SBO Power Supply System (Train B)
2	APG [SGBS]	Steam Generator Blowdown System	22	PTR [FPCTS]	Fuel Pool Cooling and Treatment System
3	ARE [MFFCS]	Main Feedwater Flow Control System	23	RBS [EBS]	Emergency Boration System
4	ASG [EFWS]	Emergency Feedwater System	24	RCP [RCS]	Reactor Coolant System
5	ASP [SPHRS]	Secondary Passive Heat Removal System	25	RCV [CVCS]	Chemical and Volume Control System
6	ATE [CPS]	Condensate Polishing System	26	REA [RBWMS]	Reactor Boron and Water Makeup System
7	CRF [CWS]	Circulating Water System	27	REN [NSS]	Nuclear Sampling System
8	DEL [SCWS]	Safety Chilled Water System	28	RIS [SIS]	Safety Injection System
9	ECS [ECS]	Extra Cooling System	29	RPE [VDS]	Nuclear Island Vent and Drain System
10	EHR [CHRS]	Containment Heat Removal System	30	RRI [CCWS]	Component Cooling Water System
11	EPP [CLRTMS]	Containment Leak Rate Testing and Monitoring System	31	SEC [ESWS]	Essential Service Water System
12	EUF [CFES]	Containment Filtration and Exhaust System	32	SEL [LWDS (CI)]	Conventional Island Liquid Waste Discharge System
13	GCT [TBS]	Turbine Bypass System	33	SRE [SRS]	Sewage Recovery System
14	JAC [FWPS]	Fire-fighting Water Production System	34	TEG [GWTS]	Gaseous Waste Treatment System
15	JPI [FWSNI]	Fire-fighting Water System for Nuclear Island	35	TEP [CSTS]	Coolant Storage and Treatment System
16	JPV [FSDB]	Fire Extinguishing System for Nuclear Island Diesel Generator Building	36	TER [NLWDS]	Nuclear Island Liquid Waste Discharge System
17	LHP	NI 10kV Emergency Power Supply System (Train A)	37	TEU [LWTS]	Liquid Waste Treatment System
18	LHQ	NI 10kV Emergency Power Supply System (Train B)	38	VDA [ASDS]	Atmospheric Steam Dump System
19	LHR	NI 10kV Emergency Power Supply System (Train C)	39	VVP [MSS]	Main Steam System
20	LHU	NI 10kV SBO Power Supply System (Train A)			

Figure 17: Requesting Party's HSG253 fluid system sample

647. The RP's analyses concentrated on whether gaps existed in the following areas:

- Isolation (using Figure 4 in HSG253 for final isolation method examples)
- Drainage (excluded from my assessment given its immature design)
- Pressure monitoring (e.g. pressure gauges)

648. Following the RPs analysis, I identified several compliance gaps against HSG253. Examples include:

- incorrect substance hazard;
- underestimated hazard release;
- number of personnel at risk; and
- inadequate isolation arrangements.

649. These compliance gaps may result in significant hazards being realised during EIMT operations.

650. In response to the above gaps, the RP reconsidered its safe isolation arrangements. To seek assurance of suitable application, I sampled the following HSG253 compliance assessment reports:

- Liquid Waste Treatment System (TEU) [LWTS], Rev B (Ref. 145)
- Safety Injection System (RIS) [SIS], Rev A (Ref. 142)
- Emergency Feed Water System (ASG) [EFWS], Rev A (Ref. 146)
- Main Steam System (VVP) [MSS], Rev A (Ref. 147)

651. This sample was chosen given their contributions to nuclear safety.

652. The following RQs (Ref. 6) were raised seeking clarification on the RP's analysis reports:

- RQ-UKHPR1000-1243 against TEU [LWTS]
- RQ-UKHPR1000-1258 against VVP [MSS]
- RQ-UKHPR1000-1259 against ASG [EFWS]
- RQ-UKHPR1000-1351 against RIS [SIS]
- RQ-UKHPR1000-1388 against RIS [SIS]
- RQ-UKHPR1000-1402 against RIS [SIS]
- RQ-UKHPR1000-1403 against TEU [LWTS]
- RQ-UKHPR1000-1404 against ASG [EFWS]

653. The RP subsequently applied the learning from the above four systems (TEU [LWTS], RIS [SIS], ASG [EFWS] and VVP [MSS]) to applicable fluid systems. This led to the following fluid systems design improvements (see Figure 18):

- Isolation – 146 design modifications identified
- Drainage – 135 design modifications identified
- Pressure monitoring (e.g. pressure gauges) – 138 design modifications identified

System	Isolation	Drainage	Sensor
ADG [FDTGSS]	5	3	4
APG [SGBS]	3	0	0
ASG [EFWS]	0	1	2
ASP [SPHRS]	0	1	1
ATE [CPS]	0	5	7
ECS [ECS]	0	0	4
EHR [CHRS]	3	0	0
PTR [FPCTS]	9	15	20
RCV [CVCS]	7	11	6
REA [RBWMS]	10	18	21
REN [NSS]	23	2	2
RIS [SIS]	9	0	0
RPE [VDS]	23	24	24
RRI [CCWS]	16	4	10
TEG [GWTS]	16	6	5
TEP [CSTS]	20	41	28
TEU [LWTS]	2	4	4
Total	**146**	**135**	**138**

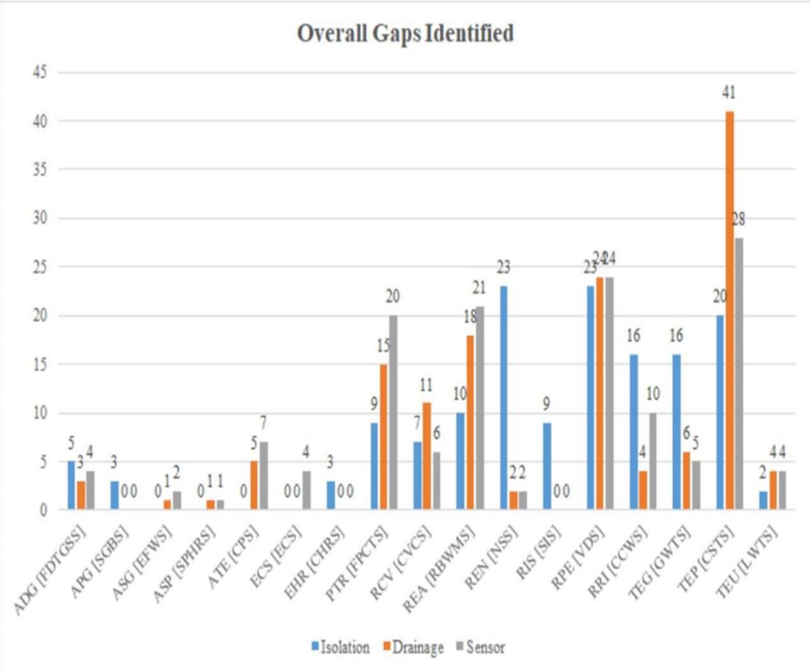

Figure 18: HSG253 sample, system modifications

654. Design modification M62 (Ref. 148) considers the above fluid system changes.

655. I consider the RP's HSG253 compliance analysis, against the four sampled fluid systems (RIS [SIS], ASG [EFWS], VVP [MSS] and TEU [LWTS]) to be appropriate for GDA.

656. The RP has recognised that an HSG253 assessment of applicable systems needs to be undertaken during site-specific stages. It has captured this as a post-GDA

commitment (see (Ref. 39), CM-SUPP-1557 to 1563 and CM-SUPP-1565 to 1577). I judge that further regulatory engagement during site-specific stages is appropriate.

657. For safe isolations, I consider the RP has not:

- Sufficiently identified EIMT safety requirements. This is a gap against ONR SAP EMT.1 (Identification of requirements).
- Shown its ability to confine radioactive material. This is a gap against ONR SAP ERC.1 (Design and operation of reactors).

658. Given HSG253 has not been fully considered for all applicable systems, I judge it significant enough to track to completion. Although the RP has made a post-GDA commitment, it does not incorporate all applicable systems. I have therefore raised the following Assessment Finding:

AF-UKHPR1000-0137: The licensee shall, during detailed design, produce a strategy and plan to justify its process isolations align with 'HSG253 The Safe Isolation of Plant and Equipment'. From this, isolation and drainage information shall be provided for an agreed Mechanical Engineering sample of systems and components.

659. By implementing HSG253, the RP has, for my sampled systems, reduced risks to ALARP.

660. For safe isolations I consider the RP has identified appropriate EIMT codes and standards (HSG253). This satisfies ONR SAP ECS.3 (Codes and standards).

4.5.1.3 Adequacy of Ageing and Degradation Arrangements

661. ONR SAPs EAD.1-5 (Ageing and degradation) consider effective SSC ageing and degradation management arrangements.

662. The RP's EQ methodology (Ref. 80) considers ageing and degradation management. This requires an EQ schedule (Ref. 95), identifying SSCs:

- important to safety that require qualification;
- performance requirements;
- operating environments; and
- EIMT requirements for through-life functional performance.

Note: SSC obsolescence should be considered in the EQ preservation phase.

663. Ageing and degradation arrangements should be applied through-life. I consider this to be normal business.

664. For GDA, I am content that SSC ageing and degradation management has been shown through the RP's EQ arrangements (Ref. 80). This satisfies the ONR SAP EAD (Ageing and degradation) series.

4.5.1.4 Mechanical Engineering EIMT Adequacy for Sample SSCs

665. I sampled EIMT arrangements for five components based on their importance to nuclear safety and when EIMT was allowed. These related to the systems identified in paragraph 627. My assessment of each of these is described below.

EPP [CLRTMS] Equipment Access Hatch

666. The EAH:

- provides reactor building access for outage work equipment during shutdown;
- during all other operational and accident scenarios, the hatch's safety function is to remain closed to maintain the containment building pressure boundary (Category A / Class 1); and
- fulfils an important confinement role during all normal and accident conditions. ONR SAP ERC.1 (Design and operation of reactors) is relevant here as it:
    - maintains external leak tightness; and
    - limits radionuclide release to the environment.

667. The EAH EIMT RGP includes ONR SAPs:

- EMT.1 (Identification of requirements) considers the identification of EIMT requirements;
- EMT.2 (Frequency) considers how often EIMT should be undertaken; and
- ERC.1 (Design and operation of reactors) considers the confinement of radioactive material.

668. When applying the above SAPs, I noted that the EAH design includes:

- pressure-retaining components (e.g. the cover and flanges);
- bearing components (e.g. lifting device); and
- ancillaries (e.g. ladders and leak-tightness test device).

669. The EAH service life is 60 years excluding vulnerable components. Vulnerable components, or the frequency of their replacement, were not identified. RQ-UKHPR1000-1069 (Ref. 6) was raised to seek clarification.

670. The RP responded that the EAH:

- seals are vulnerable components and are replaced at the end of their service life, or sooner if the air-tightness leakage rate is too high during tests;
- fasteners are checked during operation and replaced if defects are found; and
- is 'real-time' leak monitored with provision for interspace leaks to be managed.

671. For the EAH, I consider:

- It is appropriate for seals to be replaced as part of EIMT. For GDA, this satisfies ONR SAPs:
    - EMT.1 (Identification of requirements); and
    - EMT.2 (Frequency).
- The RP has shown its ability to satisfy the confinement function. This satisfies ONR SAP ERC.1 (Design and operation of reactors) for GDA.

Pressure Relief Valves

672. Pressure relief valves are used to relieve excess pressure within a system in a safe manner. Within the generic design, the pressure relief valves range from Class 3 to Class 1 components.

673. Pressure relief valve EIMT RGP includes:

- ONR SAPs:
  - EMT.1 (Identification of requirements) and ONR SAP EMT.2 (Frequency) identify what EIMT is required and when.
  - EPS.3 (Pressure relief) identifies requirement for pressure relief systems and their testing.
  - ECS.3 (Codes and standards) identifies the importance of applying appropriate codes and standards.
  - ERC.1 (Design and operation of reactors) relates to fundamental safety functions associated with confinement of radioactive materials.
- ONR TAGs:
  - NS-TAST-GD-067 (Pressure Systems Safety) (Ref. 4) does not prescribe the type or frequency of maintenance tasks.
- Codes and standards
  - AFCEN RSE-M, Rules for In-service Inspection of Nuclear Power Plant Components (Ref. 149). This states that interval between most frequent 'partial in-service inspections (ISIs)' should not exceed two years for the main primary system (B 3320). It also includes the following (C 3510):
    - Conformity checks
    - External visual checks
    - Internal checks
    - Manoeuvrability tests
    - Set pressure checks

674. I applied ONR SAPs EMT.1 (Identification of requirements), EMT.2 (Frequency), EPS.3 (Pressure relief) and ECS.3 (Codes and standards) to the design of the pressure relief valves. I noted that the basis for the pressure relief valve testing was unclear. RQ-UKHPR1000-0272 was raised to seek clarification.

675. The RP responded that periodic tests are performed on pressure relief valves at every fuel cycle (circa 18 months). Typical tests are:

- Set pressure checks
- Sprung and solenoid pilot operation

676. I noted AFCEN RSE-M (Ref. 149) states a maximum two-year window between:

- two partial in-service inspections; or
- a complete in-service inspection and a partial in-service inspection.

677. I consider pressure relief valve testing aligns with those defined in AFCEN RSE-M. However, this standard is not identified as the basis for in-service testing or inspection activities. This does not satisfy ONR SAP ECS.3 (Codes and standards). I consider this gap should be addressed during detailed design and site-specific stages as part of normal business.

678. For pressure relief valves I consider the RP has:

- Identified what EIMT is required and its frequency. This satisfies ONR SAPs:
  - EMT.1 (Identification of requirements); and
  - EMT.2 (Frequency).
- Provided valves and made provision for periodic testing. This satisfies ONR SAP EPS.3 (Pressure relief).
- Shown its ability to satisfy the confinement function. This satisfies ONR SAP ERC.1 (Design and operation of reactors).

Safety Injection System (RIS) [SIS] Residual Heat Removal Heat Exchanger

679. The RIS [SIS] RHR heat exchangers:

- have a safety function to remove residual heat from the core in normal and accident conditions (Category A / Class 1); and
- fulfil an important role in core heat removal. ONR SAP ERC.1 (Design and operation of reactors) is relevant.

680. RHR heat exchanger EIMT RGP includes:

- ONR SAPs:
  - EKP.5 (Safety measures) considers the hierarchy of safety measure characteristics, with passive measures preferred;
  - EMT.2 (Frequency) and EMT.7 (Functional testing) relate to when and how EIMT is achieved in service;
  - ECS.3 (Codes and standards) identifies the importance of applying appropriate codes and standards;
  - EDR.1 (Failure to safety) recognises the need for SSCs to fail in a safe manner;
  - ERC.1 (Design and operation of reactors) relates to fundamental safety functions associated with heat removal from the core; and
  - ECV.3 (Means of confinement) considers means of confinement by intrinsically safe features.
- Codes and standards:
  - AFCEN RSE-M, Rules for In-service Inspection of Nuclear Power Plant Components (Ref. 149). Section A3300 of AFCEN RSE-M (Ref. 149) defines periodic inspection for heat exchangers during both normal operation and outages.
  - Tubular Exchanger Manufacturers Association (TEMA) (Ref. 150). Section E-4 of TEMA (Ref. 150) states "At regular intervals and as

frequently as experience indicates, an examination should be made of the interior and exterior condition of the unit".

681. When considering the above RGP, I noted that the RP's RHR heat exchanger EIMT requirements were unclear. Conflicting information existed regarding what EIMT is undertaken and when it is required (see Appendix D of the RP's "EMIT Windows" report (Ref. 139)). RQ-UKHPR1000-RQ1350 (Ref. 6) was raised to seek clarification.

682. The RP's response against the RHR heat exchanger stated:

- Periodic testing is not required given their use during normal shutdown.
- Their performance (and therefore degradation) can be tested during operations and commissioning.
- No maintenance activities can be performed during normal operation (only in Reactor Complete Discharge (RCD) plant state).
- Visual external inspection is possible during normal operation, e.g. checking for leaks.
- EIMT will be undertaken according to AFCEN RSE-M and their operating and maintenance manual.

683. I consider it acceptable for each RHR heat exchanger's performance to be validated during commissioning and normal shutdown. I consider this reduces risks to ALARP as:

- The heat exchangers are passive equipment presenting a low risk of malfunction.
- Subject to HSG253 compliance, it is currently not reasonably practicable to evaluate the thermal performance when the reactor is at power or during outages.
- The performance requirement during normal shutdown bounds severe accident thermal performance.
- Performance degradation (e.g. from fouling) is observable and likely to be gradual.
- The heat exchangers can be visually inspected, subject to a suitable environment, during:
  - normal operation; and
  - RCD plant state.

684. The RP's RHR heat exchanger includes a 'hatch' in the hemispherical head pass-partition plate. The pass-partition plate design allows a volume of primary coolant to remain behind the access cover after draining. I considered this to be a gap against ONR SAP EMT.7 (Functional testing). RQ-UKHPR1000-RQ1425 (Ref. 6) was raised to seek clarification.

685. The RP responded stating:

- the pass partition plate design enabled inspection via a hatch (Figure 19);
- the hatch is appropriately secured and sealed; and
- a 6 mm through hole (Figure 20) drains primary circuit fluid retained by the pass partition plate.

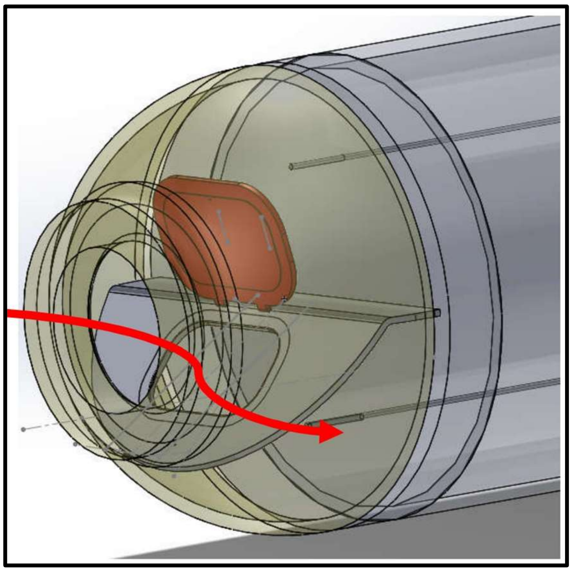

Figure 19: Inspection access to RHR via pass partition plate

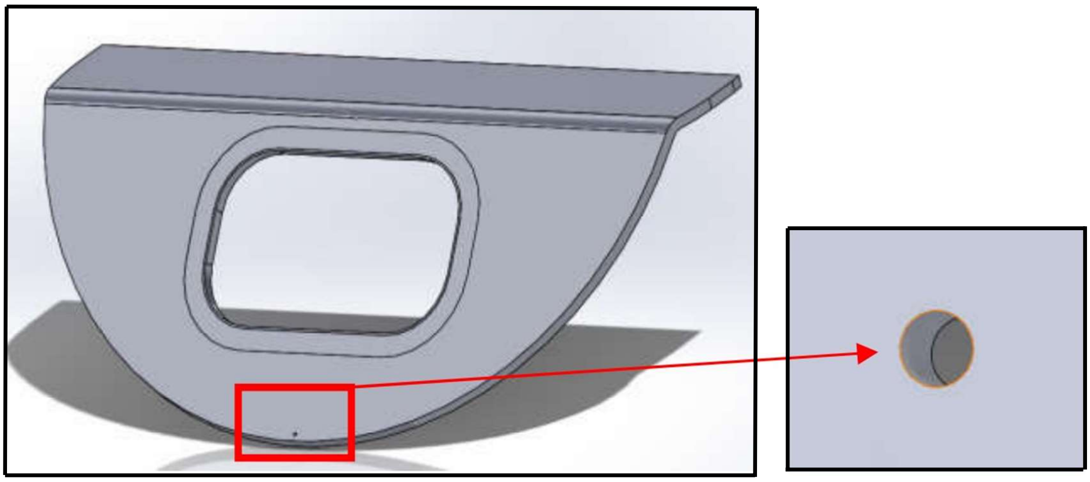

Figure 20: 6 mm diameter through hole to facilitate drainage

686. I am satisfied the measures for securing and sealing the hatch are proportionate. This is subject to seal leakage qualification during site-specific stages, which I consider to be normal business.

687. I consider the 6 mm through hole, in the pass partition plate, is an inadequate means of draining primary circuit fluid. This is because an unrevealed hole blockage may result in retention of primary circuit fluid. Before opening the hatch, a blockage cannot be seen. This could lead to an unacceptable risk to the operator and/or a leakage of contamination, which I judge can reasonably be mitigated by an improved design.

688. For the RIS [SIS] RHR heat exchangers I consider the RP has not shown:

- How confinement of radioactive material is assured.
  This does not satisfy ONR SAPs ERC.1 (Design and operations of reactors), EKP.5 (Safety measures) and ECV.3 (Means of confinement).
- How the design is fail-safe.
  This does not satisfy ONR SAP EDR.1 (Failure to safety).

689. Given the final design choice rests with the licensee during detailed design, I have raised the following Assessment Finding:

AF-UKHPR1000-0138: The licensee shall demonstrate, during detailed design of the residual heat removal heat exchanger, that the risk from primary circuit fluid retention is as low as reasonably practicable. This risk relates to intrusive maintenance operations.

690. I noted the RP refers to the 2010 Edition of the RSE-M code, rather than more recent editions (the 2020 Edition is not yet available in English at the time of writing this report). I have reviewed sections in both the 2010 and 2018 Edition and identified that some changes have occurred.

691. In addition, during my Step 4 assessment, the TEMA Standards have been revised from the Ninth Edition to the Tenth Edition.

692. I consider these to be a Minor Shortfall that the licensee may wish to resolve by undertaking its own gap analysis of revised codes and standards during site-specific stages.

693. For the RIS [SIS] RHR heat exchangers I consider that the RP has:

- Identified when EIMT is required and how it is achieved. This satisfies ONR SAPs:
  - EMT.2 (Frequency); and
  - EMT.7 (Functional testing).
- Identified appropriate codes and standards. This satisfies ONR SAP ECS.3 (Codes and standards).

Liquid Waste Treatment System (TEU [LWTS]) Process Drains Storage Tank

694. The TEU [LWTS] process drains storage tanks:

- have a safety function to safely store various liquid wastes in normal operation conditions (Category C / Class 3) (Ref. 133);
- failure could result in loss of liquid waste containment; and
- fulfil an important role during normal operation.

695. I sampled this Class 3 SSC as EIMT could be undertaken at any time. All other SSCs sampled had dedicated periods for EIMT. Hence, as the status of the plant may not always be consistent, there could be an increased radiological risk to personnel.

696. TEU [LWTS] EIMT RGP includes ONR SAPs EMT.1 (Identification of requirements) and EMT.7 (Functional testing), which relate to what and how EIMT is achieved in-service.

697. The RP's "EMIT Windows" report (Ref. 139), states TEU [LWTS] preventative maintenance may be undertaken during all reactor operation modes. However:

- I could not identify specific EIMT requirements in the safety case, and
- the RP claimed, in Revision C of its System Design Manual for the TEU (Ref. 151) that periodic testing of the TEU [LWTS] was not required.

698. RQ-UKHPR1000-1065 (Ref. 6) was raised to seek clarification.

699. In response to my query regarding the TEU [LWTS] EIMT requirements, the RP's response stated:

- A preventative maintenance programme will be developed during site-specific stages.
- This programme will utilise supplier operation and maintenance manuals.
- Pre-service inspection arrangements will comply with RSE-M (Ref. 149) and be informed by OPEX.

700. I consider this reasonable given:

- EIMT details are immature; and
- low system novelty.

701. I am satisfied TEU [LWTS] EIMT arrangements can be fully defined during site-specific stages. ONR SAP EMT.1 (Identification of requirements).

702. In response to my query regarding the TEU [LWTS] periodic testing, the RP explained the TEU [LWTS] is:

- not a safety system (i.e. it does not respond to a fault); and
- periodically tested through appropriate routine checks and/or preventative maintenance.

703. TEU [LWTS] in-service inspections, including bunds (i.e. confirming no leakage into them), should be considered during site-specific stages as normal business.

704. I am satisfied, given the TEU [LWTS] safety classification (Class 3), that its in-service inspection arrangements are proportionate. ONR SAP EMT.7 (Functional testing).

705. For the TEU [LWTS] I consider the RP has both identified what EIMT is required and how it is achieved. This satisfies ONR SAPs EMT.1 (Identification of requirements) and EMT.7 (Functional testing).

Polar Crane (Reactor Building)

706. The Reactor Building Handling Equipment System (DMR) [RBHES] polar crane:

- has a safety function (Category A / Class 1) to provide mechanical handling for SSCs within the reactor building during:
    - construction;
    - outages; and
    - decommissioning.

707. Polar crane EIMT RGP includes:

- ONR SAPs (Ref. 2):
    - EMT.1 (Identification of requirements) and EMT.2 (Frequency), which relate to what EIMT is required and when; and
    - EMT.5 (Procedures) and EMT.6 (Reliability claims), which relate to the need for adequate procedures to ensure continued quality and reliability and the tests required to achieve this.

- ONR Technical Assessment Guide, NS-TAST-GD-056 concerning Nuclear Lifting Operations (Ref. 4).
- Codes and standards:
  - Lifting Operations and Lifting Equipment Regulations 1998 (LOLER) (Ref. 152);
  - Safe use of lifting equipment. Lifting Operations and Lifting Equipment Regulations 1998. Approved Code of Practice and guidance (Ref. 153);
  - The Provision and Use of Work Equipment Regulations 1998 (PUWER) (Ref. 154); and
  - Safe use of work equipment. Provision and Use of Work Equipment Regulations 1998. Approved Code of Practice and guidance (Ref. 155).

708. The polar crane is positioned within the Reactor Building (BRX). As such it will require a risk based EIMT regime. During power generation, the BRX is sealed and is inaccessible for circa 18 months. At the start of a refuelling outage, the crane must be brought back into service so that it can undertake several, safety critical lifts. For example, the Reactor Pressure Vessel (RPV) head removal.

709. The polar crane's EIMT regime should:

- address its operating conditions;
- ensure it can deliver its safety function requirements throughout its lifetime; and
- comply with the Lifting Operations and Lifting Equipment Regulations 1998 (LOLER) statutory examination requirements (Ref. 152) and (Ref. 153).

710. To inform my assessment, I undertook several lifting interactions (Ref. 7). These concerned the lifting systems and their EIMT.

711. My assessment focussed on the RP's submission, "EMIT Requirements for the Polar Crane" (Ref. 156).

712. The document considers the statutory requirements of LOLER for a 12-monthly inspection (thorough examination) interval. To address the time when the crane is inaccessible the RP identifies that a Written Scheme of Examination (WSE) is required. I am satisfied that the RP understands how it needs to comply with this aspect of UK legislation. I consider this aligns with ONR SAPs EMT.1 (Identification of requirements) and EMT.2 (Frequency).

713. To address the 'out of use' period, the RP identifies additional activities, prior to the 'out of use' period and prior to bringing it back into use. I consider this aligns with ONR SAP EMT.5 (Procedures). Examples from (Ref. 156) include:

- Prior to 'out of use' (Section 4.6.1)
  - Management of protective coatings and use of desiccants
  - Removal and storage of components
  - Potential seizing of components (e.g. brakes)
  - Seismic qualification conditions
- Prior to 'bringing back into use' (Section 4.6.2)
  - Reinstatement of features and removal of protective measures

    - Adjustment of equipment setting and calibration

- Defining a datum (Section 4.6.3)

    - Monitoring to identify any through-life changes (i.e. deterioration) in equipment performance

714. My assessment identified a gap in the “EIMT Requirements for the Polar Crane” document (Ref. 156). It did not include the polar crane’s operational phases before reactor operations.

715. EIMT of the polar crane should start immediately after the crane has satisfactorily completed works testing. For example, deterioration can occur during:

- storage;
- transport;
- construction; and
- when it is being used to install other equipment (e.g. steam generators).

716. In addition, the RP’s report states that a ‘design confirmation’ will be undertaken “to confirm that the selected interval is appropriate both for the overall crane and for all key components”.

717. I am satisfied that these areas can be addressed during the site-specific stages. At that time the pre-operational use and conditions will be mature. Hence, I judge this to be a Minor Shortfall as it relates to matters necessary for the licensee to comply with relevant legal requirements.

718. I am satisfied that the RP understands and has addressed both the unusual and specific EIMT requirements. These relate to the extended duration between use and the work required to prepare the polar crane for this period and before bringing it back into service. This satisfies ONR SAP EMT.5 (Procedures) and EMT.6 (Reliability claims).

719. For the DMR [RBHES]) polar crane I consider the RP has identified:

- What EIMT is required and when it is required. This satisfies ONR SAPs:

    - EMT.1 (Identification of requirements); and
    - EMT.2 (Frequency).

- Appropriate in-service inspection. This satisfies ONR SAPs:

    - EMT.5 (Procedures); and
    - EMT.6 (Reliability claims).

4.5.2 Strengths

720. The RP has shown considerable knowledge of EIMT within its existing plants.

4.5.3 Outcomes

721. As a result of my assessment, the RP has:

- improved its isolation arrangements;

- prevented unsafe EIMT activities during power operations; and
- improved its understanding of EIMT requirements.

722. I am content the RP has addressed my Mechanical Engineering concerns raised within the Fault Studies RO-UKHPR1000-0021 (Ref. 143).

723. I have raised two Assessment Findings, identified in sub-section 4.5.1 above, for the licensee to:

- Ensure that the generic UK HPR1000 design satisfies HSG253 (safe isolation of plant and equipment) guidance
- Ensure the generic UK HPR1000 RHR heat exchanger design reduces retention of primary circuit fluid ALARP to allow safe EIMT

724. I have identified one Minor Shortfall in paragraph 717. This relates to EIMT during the pre-operational use of the polar crane.

725. The Assessment Findings are listed in Annex 3.

4.5.4 Conclusion

726. I judge, for the purposes of GDA, the RP has:

- understood EIMT requirements; and
- improved its understanding of and application of HSG253 to achieve safe isolations.

727. Overall, for the purpose of GDA, I conclude that the RP’s submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP’s examination, inspection, maintenance and testing arrangements are sufficient from a Mechanical Engineering perspective.

728. I have identified several matters that the licensee will need to address during the detailed design. I have captured these in two Assessment Findings.

4.6 Theme 6: Adequacy and Application of Design Assurance Arrangements

729. My UK HPR1000 Step 3 Mechanical Engineering assessment (Ref. 22) concluded that:

- "The design assurance arrangements, relating to ME equipment, require more substantive evidence. Suitable evidence will be obtained from a planned manufacturing facility visit during GDA Step 4.
- "Also, during Step 4, the RP's approach to design analysis requires further justification." See Theme 1 (sub-section 4.1 of this report), which covers this aspect.

4.6.1 Assessment

730. My Step 4 assessment aimed to consider the adequacy and application of the RP's design assurance arrangements.

731. The generic UK HPR1000 design consists of a large collection of mechanical components designed and procured from numerous sources. Adequate management of the design of these mechanical components is critical to delivering safe, reliable mechanical plant, capable of long-term operation.

732. The RP's design assurance arrangements are an important element to ensuring safety is integrated into its design production process. These arrangements integrate with:

- Procurement
- Site construction / installation
- Commissioning
- Operations and associated EIMT
- Safety case development

733. To assist my assessment, I identified the following sources of RGP for design assurance (Ref. 2, Ref. 4):

- ONR SAP EKP.3 (Defence in depth) considers conservative design of engineering components.
- ONR TAGs:
    - NS-TAST-GD-057 Design Safety Assurance.
    - NS-TAST-GD-077 Supply Chain Management Arrangements for the Procurement of Nuclear Safety Related Items or Services.
    - NS-TAST-GD-079 Licensee Design Authority Capability. Note – this provides guidance to existing and prospective licensees.

734. My assessment of the RP's safety case during Step 3, identified that:

- Within the RP, CGN is the principal designer[§§§§]. It is responsible for the concept and detail design for some UK HPR1000 mechanical SSCs. Examples include:

[§§§§] The Construction Design and Management Regulations 2015 (CDM 2015) defines the principal designer as the designer with control over the pre-construction phase of the project.

- Control Rod Drive Mechanism
- Residual Heat Removal Heat Exchanger

■ CGN also maintains responsibility for the concept design for other UK HPR1000 mechanical SSCs. Whilst not uncommon, it relies on third parties to undertake the detailed design. Examples include:

- Containment Isolation Valve within the Emergency Feedwater System (ASG) [EFWS]
- Secondary Passive Heat Removal System Heat Exchanger (ASP) [SPHRS]
- HVAC Refrigerating Units within the Main Control Room Air Conditioning System (DCL) [MCRACS]
- Containment Heat Removal Pump (EHR) [CHRS]
- Containment Leak Rate Testing and Monitoring System serving the Personnel Airlock / Equipment Hatch (EPP) [CLRTMS]

735. The above satisfies ONR SAP EKP.3 (Defence in depth).

736. To understand the adequacy of the RP's design processes, I had raised 15 RQs during GDA Step 3 (Ref. 6, Ref. 22).

737. A simplified view of the RP's design process controls (Ref. 157) is highlighted below:

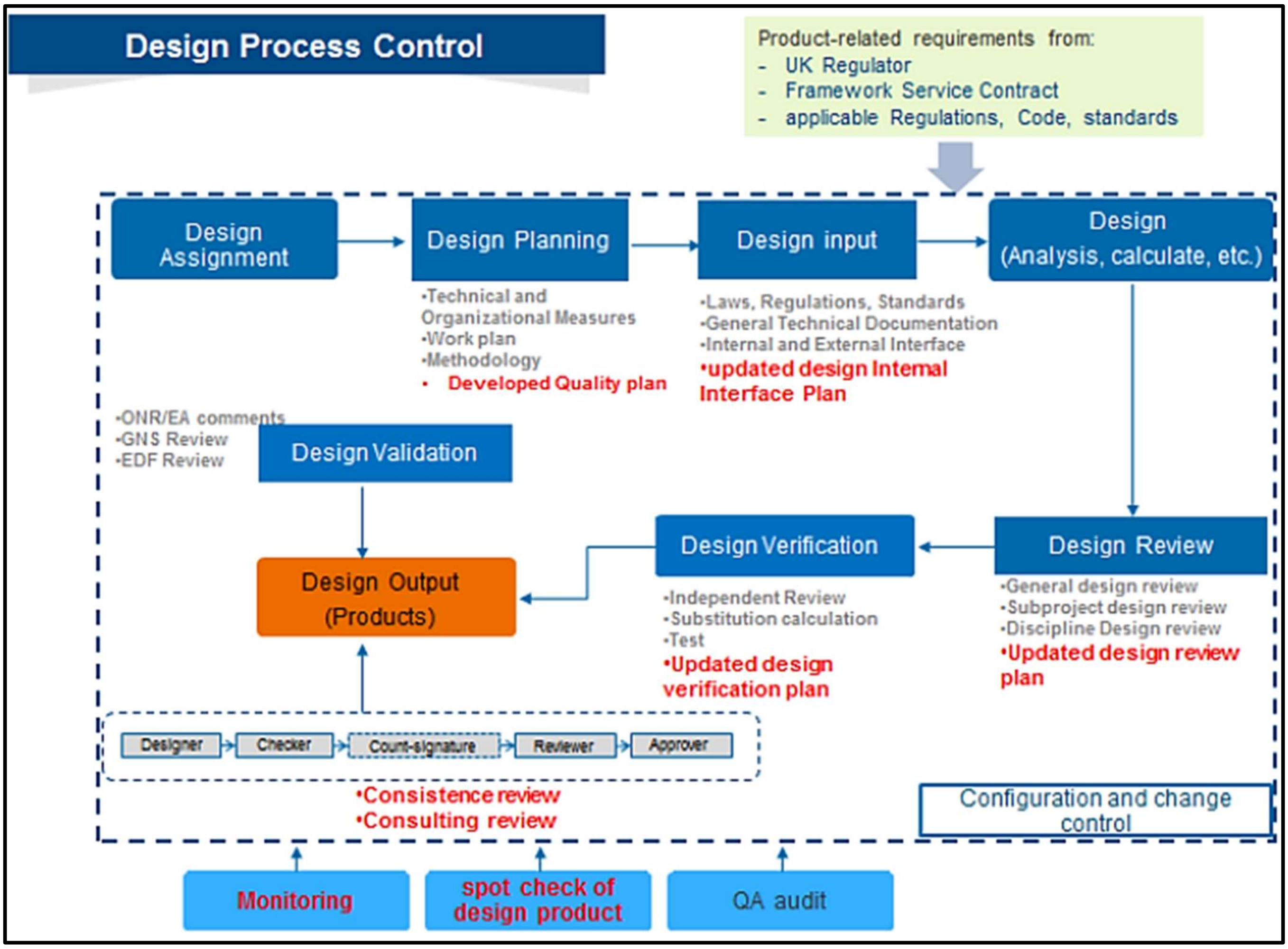

Figure 21: Simplified view of the RP's design process control

738. The above shows that a design assurance process exists (Ref. 157), which is sufficient for GDA purposes. However, assessment of its implementation was not possible during GDA Step 4 (see outcomes).

739. Regulatory Queries, ROs and CRs, which detail my regulatory interactions relevant to this assessment theme are recorded in (Ref. 6) and (Ref. 7).

4.6.2 Strengths

740. Not applicable for this assessment Theme, see sub-section 4.6.3 below.

4.6.3 Outcomes

741. Unforeseeably, due to the coronavirus (SARS-CoV-2) pandemic throughout 2020 and 2021, international travel restrictions did not allow manufacturing visits to be undertaken to China. Hence, the RP has been unable to provide substantive evidence that its design assurance arrangements satisfy my expectations.

742. I have confirmed that the RP has in place, design assurance arrangements and am content that these are adequate for GDA. I was, though, unable to assess the adequacy of their implementation, particularly within the supply chain.

743. My inability to undertake an assessment of design assurance implementation does not invalidate my judgement. I am content that suitable opportunities will exist during detailed design and site-specific stages to gain the necessary assurances. I consider this to be normal regulatory business.

4.6.4 Conclusion

744. I judge that:

- the RP's design assurance arrangements are adequate; and
- the licensee can demonstrate implementation of its design assurance arrangements during site-specific stages.

745. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's design assurance arrangements are sufficient from a Mechanical Engineering perspective.

4.7 Theme 7: Application of the ALARP Principle when Considering Design Changes

746. My Step 3 assessment report (Ref. 22) concluded that:

- the RP had not considered all sources of Mechanical Engineering related RGP;
- application of the ALARP principle in design changes required follow up; and
- further assessment of relevant design changes and ALARP improvements is required during Step 4.

4.7.1 Assessment

747. ONR's ALARP guidance (Annex 2 of NS-TAST-GD-005 (Ref. 4)) expects the following four main areas to be addressed during ALARP considerations:

- RGP is applied such that the standards and codes adopted by the RP must be shown to have been met.
- Optioneering is undertaken to show how options are both selected and deselected, and how the selected option reduces risks ALARP.
- A risk assessment is undertaken to identify potential engineering or operational improvements.
- A clear conclusion is reached that no further reasonably practicable improvements can be implemented.

748. RGP for ALARP also includes:

- ONR SAPs (Ref. 2):
  - SC.4 (Safety case characteristics) requires a safety case to demonstrate designs meet RGP and sound safety principles to reduce risks ALARP;
  - ECS.3 (Codes and standards) considers the use of appropriate codes and standards;
  - ECV.1 (Prevention of leakage) considers prevention of spread of contamination by leakage; and
  - RP.7 (Hierarchy of control measures) considers establishing a hierarchy of control measures in accordance with IRR17.
- HSE guidance on ALARP (see www.hse.gov.uk/managing/theory/index.htm)

749. I advised the RP of these expectations at a technical meeting in early 2020 (Ref. 7).

750. To assess the RP's consideration of ALARP I considered the following areas:

- ALARP process - methodology development
- ALARP assessment of reactor systems and components considering:
  - Examination, inspection, maintenance and testing
  - Diversity and redundancy of auxiliary components
  - Lifting operations
  - Insulation material used in containment
  - Categorisation and classification of SSCs
  - Modification procedure

    - HVAC design
    - Codes and standards

- ALARP application including:
    - Strategy
    - RGP analysis
    - Compliance analysis
    - Optioneering

- Demonstrating modifications reduce risks ALARP

4.7.1.1 ALARP Process – Methodology Development

751. The RP developed an “ALARP Methodology” (Ref. 158) to allow it to consistently apply a set of standards to all ALARP assessments.

752. Following its ALARP methodology, the RP produced six ALARP assessment reports (Ref. 107) to (Ref. 112). The assessment of these reports associated with RGP, is discussed in sub-section 4.4.1.1 of this report.

753. For Theme 7, I assessed a sample of these reports. This assessment confirmed if the RP had applied its ALARP methodology when making design changes (modifications). This was achieved by sampling documentation from the RP’s optioneering process relating to design modifications.

754. For the purposes of GDA I consider the RP’s ALARP methodology (Ref. 158) to be suitable.

4.7.1.2 ALARP Assessment of Reactor Systems and Components

755. During Step 2 of GDA, I identified several gaps against RGP. RQ-UKHPR1000-0001 (Ref. 6) was raised to seek clarification.

756. The RP responded stating that:

- using Chinese domestic codes and standards is considered a gap; and
- gaps exist against several Mechanical Engineering areas.

757. I had further interactions with the RP related to RGP and ALARP. The relevant RQs, ROs and technical meetings are recorded in (Ref. 6) and (Ref. 7). The following areas were sampled to assess the RP’s application of RGP to reduce risks ALARP.

Examination, Inspection, Maintenance and Testing

758. My assessment considered the RP’s application of RGP associated with EIMT.

759. I sampled several systems and components important to nuclear safety, which I discuss further in sub-section 4.5 of this report.

760. Theme 5 concluded (see sub-section 4.5 of this report) that the RP’s submissions sufficiently align with relevant SAPs, TAGs and RGP. Several matters were identified for the licensee to address during the detailed design. These were captured in Assessment Findings.

761. The above confirms the RP’s application of EIMT RGP to reduce risks ALARP.

Diversity and Redundancy of Auxiliary Components

762. My assessment considered the RP's application of RGP associated with diversity and redundancy of auxiliary components.

763. As a result of RO-UKHPR1000-0023, captured in the Fault Studies Assessment Report (Ref. 70), the following Mechanical Engineering modifications were made (Ref. 148):

- M34 Mechanical Diversification on Isolation Valves at the suction of the Fuel Pool Cooling and Treatment System (PTR) [FPCTS] Cooling Trains
- M35 HVAC systems diversity modification
- M44 Mechanical Diversification on Containment Isolation Valves
- M69 Mechanical Diversification on Isolation Valves of ASP and RCV

764. The above modifications confirm the RP's application of RGP to reduce risks ALARP.

Lifting Operations

765. My assessment considered the RP's application of RGP associated with lifting operations. This is discussed further in sub-sections 4.9 and 4.10 of this report.

766. Themes 9 and 10 concluded (see sub-sections 4.9 and 4.10 of this report) that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. A matter was identified for the licensee to address during the detailed design. This was captured in an Assessment Finding.

767. The above confirms the RP's application of lifting operation RGP to reduce risks ALARP.

Insulation Material Used in Containment.

768. My assessment considered the RP's application of RGP to reduce hazards associated with its choice of containment insulation material.

769. I considered the use of fibrous insulation material within the primary circuit did not meet the principles of prevention defined in MHSWR (Ref. 45). See sub-section 4.8 of this report further details of my assessment.

770. Theme 8 concluded (see sub-section 4.8 of this report) that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

771. The above confirms the RP's consideration of RGP in its choice of containment insulation material to reduce risks ALARP.

Categorisation and Classification of SSCs

772. My assessment considered the RP's application of RGP to its categorisation of safety functions and classification of systems and components. This is discussed further in sub-section 4.2 of this report.

773. Theme 2 concluded (see sub-section 4.2 of this report) that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Several matters were identified for the licensee to address during the detailed design. These were captured in Assessment Findings.

774. The above confirms the RP's consideration of RGP in its categorisation and classification arrangements. Suitable categorisation and classification arrangements contribute to reducing risks ALARP.

Modifications Procedure

775. My assessment considered the RP's application of RGP relative to its modification procedure.

776. I considered the output of the RP's modification procedure did not satisfy regulatory expectations. For example, ONR's ALARP guidance (Ref. 4). This is discussed further in this Theme in sub-section 4.7.1.4 below.

HVAC Design

777. My assessment considered the RP's application of RGP relative to the HVAC design.

778. I considered the HVAC system's ability to function in extreme environmental conditions. See sub-section 4.1 of this report for further details of my assessment.

779. Theme 1 concluded (see sub-section 4.1 of this report) that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Several matters were identified for the licensee to address during the detailed design. These were captured in Assessment Findings.

780. The above confirms the RP's consideration of RGP in its HVAC design to reduce risks ALARP.

Codes and Standards

781. My assessment considered the RP's application codes and standards in accordance with ONR SAP ECS.3 (Codes and standards). It also considered the RP's consideration of applicable GB regulations.

782. This is discussed further in this Theme in sub-section 4.7.1.3 below.

4.7.1.3 ALARP Application

783. RO-UKHPR1000-0012 (Ref. 105) was raised to address shortfalls in the RP's application of RGP. This includes its understanding and application of codes and standards and relevant GB regulations. It required the RP to:

- Prepare a strategy for identifying RGP
- Analyse whether RGP is applicable to the design
- Undertake an RGP compliance analysis for its reactor design

784. In accordance with ONR's Guidance on the Demonstration of ALARP (Ref. 4), I considered the RP's optioneering process. I also sampled its application for design modifications.

Strategy

785. The RP's strategy to identify applicable RGP was contained within its "ALARP Methodology" (Ref. 158). This methodology:

- Defined what was required and how it would be achieved
- Identified legal requirements and RGP including:

  - Acts of Parliament
  - Regulations
  - Approved Codes of Practice
  - Codes and standards
  - Guidance documents
  - Operational experience
- Provided RGP suitability analyses
- Established the relative importance of RGP collected
- Screened RGP to produce an applicable list
- Provided a compliance analysis against RGP
- Undertook gap identification against the generic design and safety case

786. I judge the RP's ALARP methodology suitably captures the principles set out in Annex 2 of ONR's ALARP TAG NS-TAST-GD-005 (Ref. 4) for GDA.

RGP Analysis

787. To analyse whether the RGP was applicable to the design, the RP produced:

- A general principles report (Ref. 159), which:
  - described general principles, process and selection criteria; and
  - presented a hierarchy of applicable laws, regulations and codes and standards.
- Suitability analysis reports for:
  - HVAC systems (Ref. 160)
  - Mechanical systems (Ref. 161)
  - Static SSCs (Ref. 162)
  - Dynamic SSCs (Ref. 163)
- Each report:
  - Described the suitability analysis process
  - Collected the related RGP
  - Screened the related RGP
  - Assessed the selected RGP
  - Listed the applicable RGP
- A "List of Gaps for Mechanical Engineering against RGP" report (Ref. 113). This collated the results of the suitability analysis reports (Ref. 160) to (Ref. 163).

Compliance Analysis

788. The RP undertook an RGP compliance analysis for its reactor design. These reports considered the following system or component types:

- HVAC systems (Ref. 164)

- Mechanical systems (Ref. 165)
- Static SSCs (Ref. 166)
- Dynamic SSCs (Ref. 167)

789. These reports:

- Outlined the analysis process
- Provided the results
- Identified closure plans for any gaps
- Recorded the justification for the conclusions reached

790. The RP's analysis shows that safety related SSCs are designed and manufactured to appropriate codes and standards. The RP has also confirmed RGP applicability for GDA. I consider this meets ONR SAP ECS.3 (Codes and standards).

791. During site-specific stages, I expect the licensee to develop its standards for safety related SSCs. These should include areas such as:

- Construction
- Installation
- Commissioning
- Quality assurance
- EIMT

792. I consider this to be normal business.

793. Through the resolution of RO-UKHPR1000-0012, the RP has undertaken significant work to understand Mechanical Engineering RGP (Ref. 136).

Optioneering

794. I applied ONR SAP SC.4 (Safety case characteristics) and ONR's Guidance on the Demonstration of ALARP (Ref. 4) to consider the RP's approach to optioneering.

795. Early in Step 4, I judged that the RP's optioneering proposals to support ALARP demonstration were not suitable (see (Ref. 7)). To address this gap, the RP submitted optioneering study reports. These reports considered RGP gaps in:

- HVAC Systems (Ref. 114)
- Mechanical Systems (Ref. 115)
- Static SSCs (Ref. 116)
- Dynamic SSCs (Ref. 117)

796. These optioneering reports:

- identified RGP gaps;
- proposed options to close the gaps; and
- presented the 'pros and cons' of each option.

797. Through the RP's application of its optioneering process and ALARP methodology, it has suitably assessed the hazards posed by its design and identified measures to control risks. This satisfies ONR SAPs SC.4 (Safety case characteristics).

4.7.1.4 Demonstrating Modifications Reduce Risks ALARP

798. Through its improved “ALARP Methodology” (Ref. 158), the RP implemented several improvements (Ref. 148). These covered the following areas:

- EIMT and Maintenance Strategy
- Diversity and redundancy of auxiliary components
- Design of cranes
- Insulation material used in containment
- Categorisation and classification
- Codes and standards
- HVAC Design
- Sample Assessment of Mechanical Engineering Related Design Modifications

799. I sampled eight modifications across the seven areas. This was to gain assurance that the RP had appropriately and consistently applied the ALARP principle when considering improvements. I identified these from the RP’s ALARP demonstration reports (Ref. 108, Ref. 109, Ref. 112, Ref. 168).

800. For the following modifications, I consider that the RP’s ALARP methodology was appropriately applied:

- M23 Modification of Resisting the Extremely Low Air Temperature of the UK on the Secondary Passive Heat Removal System (ASP) [SPHRS]. This changed the ASP [SPHRS] design to improve its resilience to low air temperatures.
- M57 Insulation material replacement in containment. This changed the reactor’s primary circuit insulation design to align with RGP.
- M62 Modification of UK HPR1000 HSG253 about the isolation design and drainage design. This changed the UK HPR1000 fluid systems to align with RGP (HSG 253).
- M66 Design Modification of Spent Fuel Delivery Process. This changed the spent fuel delivery process to align with RGP.
- M76 Design Modification of Fuel Handling Equipment in Fuel Building. This changed the fuel handling equipment design to align with RGP.
- M77 Design Modification of operation envelope control of Auxiliary Crane. This reduced the hazards associated with the auxiliary crane.

801. For other modifications, I found that the RP had not applied its methodology appropriately:

- M68 Modification spurious dilution caused by the LHSI pump seal cooling heat exchanger break. This aimed to prevent dilution of primary circuit fluid. The modification did not present the optioneering process or the consequences of the modification.
- M78 Design Modification for Maintenance of Spent Fuel Cask Crane. This changed the spent fuel cask crane design to align with RGP. This modification did not contain the expected level of detail as laid out in the RP’s ALARP strategy. The ‘pros and cons’ of options were not clearly presented.

802. Modification M68 (Ref. 148) and its supporting information (Ref. 169), relates to increasing the pressure in the RIS [SIS] side of the LHSI pump seal cooling heat

exchanger. This was done to mitigate a fault identified in GDA. When applying ONR SAPs RP.7 (Hierarchy of control measures) and ECV.1 (Prevention of leakage), I identified concerns regarding the adequacy of the RP's:

- assessment of consequences of RRI [CCWS] non-boronated water in-leakage to the primary circuit;
- assessment of the consequences of primary circuit leakage to the RRI [CCWS] system; and
- optioneering undertaken to demonstrate that no further reasonably practicable improvements can be made.

803. I consider these to be a shortfall against ONR SAPs RP.7 (Hierarchy of control measures) and ECV.1 (Prevention of leakage). I have discussed the RRI [CCWS] with ONR's Chemistry inspector, who confirmed that there is monitoring in place to detect increased dose in the RRI [CCWS]. However, this identifies a leak once it has occurred. I consider preventing leakage of primary circuit fluid a more robust engineering solution.

804. Given the above shortfalls, I judge it appropriate for the licensee to consider whether the design choices within modification M68 reduce risks to ALARP. I have raised this as an Assessment Finding:

AF-UKHPR1000-0139: The licensee shall, during detailed design, demonstrate that the boron dilution modification to the Low Head Safety Injection pump, reduces risks to as low as reasonably practicable. The modification should consider the hierarchy of control measures for restricting exposure and prevention of leakage.

805. My assessment also identified that:

- The level of detail in the demonstration reports is inconsistent. Examples include:
    - a lack of variety of options for some proposed modifications;
    - the reason for rejecting some options was unclear due to lack of detail; and
    - inconsistencies within risk assessments regarding proposed modifications.
- The ALARP demonstrations are inconsistent at a component level, but appropriately applied at the system level.

806. I judge these inconsistencies to be a Minor Shortfall. The reason for this is that they do not:

- undermine my confidence in the safety of the generic design; or
- impair my ability to understand the key risks associated with the generic design.

807. Despite these findings I consider that, on balance, the RP has:

- demonstrated why risks are ALARP;
- identified relevant hazards using a thorough and systematic process;
- provided links to the information necessary to show that risks are ALARP; and

- shown the generic design complies with engineering RGP and sound safety principles.

808. At this GDA stage, I judge that this aligns with the guidance within SAP SC.4 (Safety case characteristics).

4.7.2 Strengths

809. The RP has improved its ALARP methodology and shown a good understanding of RGP.

4.7.3 Outcomes

810. The RP has improved its understanding of RGP and its understanding of the ALARP principle.

811. I have identified one Assessment Finding related to design modification M68.

812. I have identified one Minor Shortfall in paragraph 806. This relates to the inconsistent application of the RP's ALARP methodology at a component level, which the licensee may wish to improve.

813. I consider this Minor Shortfall does not undermine the overall ALARP position of the generic design.

4.7.4 Conclusion

814. I judge that the RP has:

- considered sources of RGP;
- developed a suitable ALARP strategy and methodology; and
- completed modifications following its ALARP methodology.

815. Whilst I have raised one Assessment Finding and identified one Minor Shortfall, it does not undermine the overall ALARP position.

816. This satisfies ONR SAPs:

- SC.4 (Safety case characteristics)
- ECS.3 (Codes and standards).

817. During site-specific stages, a review of modifications is necessary. This should show that the ALARP principle is consistently used.

818. The Step 4 Summary Report (Ref. 21) details ONR's assessment of ALARP.

819. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that RP's application of the ALARP principle, when considering design changes, is sufficient from a Mechanical Engineering perspective.

820. I have identified one matter that the licensee will need to address during the detailed design. I have captured this in an Assessment Finding.

4.8 Theme 8: Approach to Reducing the Hazards from Fibrous Material within the UK HPR1000 Loss of Coolant Accident Zone of Influence

821. My Step 3 assessment report (Ref. 22) concluded that the RP had not made an adequate ALARP justification for its choice of primary circuit insulation material. I judged that improvements could be made in the RP's:

- arguments and evidence supporting the change to Reflective Metal Insulation (RMI); and
- consideration of nuclear safety impacts on other systems (e.g. ventilation systems that remove heat).

822. During Step 3, I advised the RP that the principles of prevention (i.e. avoiding rather than controlling the hazard) applied to its choice of insulation material. Hence, the RP chose to use RMI for its primary circuit instead of fibrous material.

4.8.1 Assessment

823. I assessed whether the RP, in its design, had chosen a type of insulation material that reduces risks ALARP.

824. Important ALARP considerations included:

- justification for how potential insulation debris would not negatively impact the performance of emergency core cooling systems;
- reducing worker dose uptake during EIMT activities; and
- OPEX and other new civil reactor designs.

825. No specific regulatory requirements exist for the type of primary circuit insulation material. However, there are several sources of RGP including:

- MHSWR Schedule 1 General Principles of Prevention (Ref. 45); and
- ONR SAPs (Ref. 2):
  - MS.4 (Learning) considers learning from experience to make improvements;
  - EKP.2 (Fault tolerance) considers how faults should produce a change in plant state towards a safer condition;
  - EKP.3 (Defence in depth) considers prevention of faults and independent barriers to escalation of events;
  - EMT.1 (Identification of requirements) considers what EIMT is needed and how it can be delivered; and
  - RP.1 (Normal operation (Planned Exposure Situations)) considers how suitable protection from radiation can be provided.

826. I also considered OPEX from GB nuclear new build projects (UK EPR™) and internationally:

- The UK EPR™ design at Hinkley Point C was modified to utilise RMI within containment to mitigate risks (Ref. 170). I consider the UK EPR™ approach to be RGP.
- Hazards resulting from fibrous material are an internationally recognised means of degrading emergency cooling. See US Nuclear Regulatory Commission report (Ref. 171).

827. My assessment of the RP's safety case (Ref. 14, Ref. 15, Ref. 16) identified:

- Using fibrous material, within the "zone of influence" (ZOI)*****, to reduce primary circuit heat losses did not align with RGP. This did not satisfy ONR SAP MS.4 (Learning). I consider the use of RMI to be RGP.
- Debris from the fibrous insulation material had the potential to detrimentally impact the emergency core cooling systems (RIS [SIS] and EHR [CHRS]). This did not satisfy ONR SAPs EKP.2 (Fault tolerance) and EKP.3 (Defence in depth).
- Using fibrous insulation during EIMT may not reduce radiological risks ALARP. The reason for this is that it takes more time to remove fibrous insulation that it does to remove RMI. This did not satisfy ONR SAPs EMT.1 (Identification of requirements) and RP.1 (Normal operation (Planned Exposure Situations)).

828. In parallel, ONR Fault Studies raised RO-UKHPR1000-0027 (Ref. 172). This considered the:

- debris effects on the Safety Injection System and Containment Heat Removal System performance; and
- the primary circuit insulation material choice.

4.8.1.1 Closure of RO-UKHRP1000-0027

829. RO-UKHPR1000-0027 required the RP to:

- review RGP;
- identify relevant safety factors; and
- show that debris effects risks during accidents are reduced ALARP.

830. Further detail of RO-UKHPR1000-0027 is contained within a Fault Studies assessment note (Ref. 173). I supported RO-UKHPR1000-0027 closure by assessing whether the RPs insulation choice reduced risks ALARP.

831. Regulatory Queries and CRs, relevant to this assessment, are recorded in (Ref. 6) and (Ref. 7).

832. The RP provided:

- a debris effect investigation report (Ref. 174) which considered UK OPEX; and
- an ALARP demonstration report (Ref. 108) which gave a way forward for primary circuit insulation.

833. These reports concluded:

- that RMI is considered RGP for the primary circuit insulation material; and
- a more widespread use of RMI may result in changes to pipe layout due to space constraints, and HVAC systems due to heat loading.

834. These reports ((Ref. 174) and (Ref. 108)) also state that:

***** *The use of a 'zone of influence' allows the calculation of the amount of material dislodged by a high energy pipe break at a given location within the primary circuit. The size of the ZOI is material dependent, and for a given break the ZOI of one material may be larger than another.*
For the purposes of this assessment, the zone of influence is within the containment boundary.

- where RMI is not currently within containment, it will replace the fibrous insulation material; and
- modifications to the plant from this change (likely to include pipe layout and HVAC systems) will be considered in site-specific stages (post-GDA commitment CM-SUPP-1545 (Ref. 39)).

835. The RP's modification (M57) implements this change to primary circuit insulation (Ref. 148).

836. I am satisfied that the RP has considered learning from other new build projects. It has revised its use of insulation materials within containment, in line with ONR SAP MS.4 (Learning). I judge the adoption of this RGP reduces associated risks to ALARP.

837. The RP's ALARP submission (Ref. 108) also identified that:

- The debris effect from fibrous material can be reduced as the RMI does not pose the same risk.

  I am content that this improves the design's fault tolerance and defence in depth for safety related systems. This satisfies my expectations regarding ONR SAPs:

  - EKP.2 (Fault tolerance)
  - EKP.3 (Defence in depth)

- The potential for operators to be exposed to fibrous material during EIMT is reduced.
- The ageing effects of temperature on RMI are less than for fibrous material. This should reduce the amount of EIMT required over the plant lifetime.

  I am content that this reduces EIMT risks including radiological exposures to operators. This satisfies my expectations regarding ONR SAPs:

  - EMT.1 (Identification of requirements)
  - RP.1 (Normal operation (Planned Exposure Situations))

838. I therefore judge that using RMI in containment (Modification M57) aligns with RGP.

4.8.2 Strengths

839. The RP has undertaken a review of its use of fibrous material within containment and modified its design in line with RGP.

4.8.3 Outcomes

840. The RP reviewed its choice of insulation material within the LOCA ZOI. This resulted in design modification M57 (see (Ref. 148)). This changed the insulation type from fibrous material to RMI so far as is reasonably practicable.

841. I judge that this addresses concerns, from a Mechanical Engineering perspective, raised within RO-UKHPR1000-0027 (Ref. 173).

842. I have not raised any Assessment Findings or Minor Shortfalls in this Theme.

4.8.4 Conclusion

843. In response to implementing RMI in containment, I judge that:

- this reduces debris risks ALARP;
- the dose uptake during EIMT should be reduced; and
- this change is captured in design modification M57.

844. The RP has confirmed that further RMI analysis will be undertaken, once a supplier is confirmed, during site-specific stages.

845. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's approach to reducing hazards from fibrous material within the loss of coolant accident zone of influence is sufficient from a Mechanical Engineering perspective.

4.9 Theme 9: Approach to Demonstrating Nuclear Lifts Reduce Risks ALARP

846. During Step 3 of GDA, I assessed the following four areas relating to nuclear lifts:

- The lifting of the RPV head by the polar crane.
- The reactor fuelling and refuelling operations.
- The lifting / handling of new and spent fuel.
- The loading and export of spent fuel for interim storage.

847. The conclusion of my Step 3 assessment (Ref. 22) was that further assessment of the RPV head lift by the polar crane and the spent fuel handling operations were necessary to determine that risks had been reduced ALARP.

848. Theme 9 (this theme) focusses on the polar crane's handling of RPV head.

849. Theme 10 (sub-section 4.10 of this report) focusses on spent fuel handling operations.

4.9.1 Assessment

850. The RPV head is lifted by the polar crane. In one movement it is lifted high enough to transport it to its storage position via a direct route. The weight of the load lifted is approximately 160 tonnes. It is lifted to approximately 20 metres above the RPV flange.

851. Nuclear lifting RGP includes:

- ONR SAP ELO.4 (Minimisation of the effects of incidents) considers minimising interactions between failed SSCs and other plant; and
- ONR TAG NS-TAST-GD-056 Nuclear Lifting Operations provides guidance on the assessment of safety cases relating to lifting operations and lifting equipment.

4.9.1.1 Reducing RPV Lifting Risks ALARP

852. I applied the above RGP to the RP's:

- "RPV Head Drop Analysis Report" (Ref. 175); and
- "Lifting Schedule of Reactor Pressure Vessel Head Assembly" (Ref. 176).

RPV Head Drop Analysis

853. The RP's "RPV Head Drop Analysis Report" (Ref. 175) concluded that a drop from 20 metres was unacceptable. The RP identified two other lifting routes which require RPV head to be lifted to:

- 12.51 metres (Lifting Path 2); and
- 5.51 metres (Lifting Path 3).

854. Given both these lifting routes pass over the RPV flange, drop loads have potential nuclear consequences.

855. For Lifting Path 3 (Ref. 175), the analysis report states that overall, the structural integrity under a dropped load can be guaranteed for the:

- RPV;
- main pipeline; and

- RPV support.

856. I consider ONR SAP ELO.4 (Minimisation of the effects of incidents) to be relevant.

RPV Head Lifting Schedule

857. The RP's "Lifting Schedule of Reactor Pressure Vessel Head Assembly" report (Ref. 176), considered lifting operations associated with lifting operating associated with reactor fuelling operations.

858. The RP evaluated the three lifting paths (see paragraph 853 of this report). Lifting Path 3 was identified as the preferred option. This was based on the RP implementing low-level lifting philosophy. I consider this to be RGP.

859. The RP also recognises the potential for higher risk. These lifting risks relate to the:

- duration of the lift;
- associated radiation dose; and
- complexity of operating procedures.

860. I am content that these risks have been identified. Suitable risk reduction measures should be made and applied by the licensee as part of normal business. This is an area that will be considered by Mechanical Engineering and/or other inspectors during site-specific stages.

4.9.2 Strengths

861. The RP has identified a suitable lifting path that reduces the risk of the RPV head being dropped. This minimises the risk of causing unacceptable damage to the RPV and coolant system.

4.9.3 Outcomes

862. The RP has changed the lifting path for the RPV head. This reduces risk to ALARP.

863. I have not identified any Assessment Findings or Minor Shortfalls.

864. I am satisfied that the safety case for the RPV head lifting and other loads can be developed during site-specific stages as part of normal business.

4.9.4 Conclusion

865. To conclude, I am content that the RP has suitably considered RGP by:

- accepting that the RPV head can be dropped; and
- adopting a low-level lifting strategy.

866. I consider the RP has reduced the risk of dropping the RPV head onto vulnerable components. This satisfies:

- ONR SAP ELO.4 (Minimisation of the effects of incidents); and
- ONR TAG NS-TAST-GD-056 Nuclear Lifting Operations

867. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's approach to demonstrating nuclear lifts reduce risks ALARP is sufficient from a Mechanical Engineering perspective.

4.10 Theme 10: Lifting Operations within the Fuel Building

868. Based upon the RP's submissions, my GDA Step 3 assessment (Ref. 22), judged there to be potential regulatory shortfalls associated with the lifting operations conducted within the Fuel Building. For example:

- The import and export of the spent fuel cask is a complex lift. This requires the movement of the crane and cask transport vehicle to be coordinated as it is rotated from horizontal to vertical on import and vice versa on export.
- Two cranes are used for spent fuel cask loading; this introduces a risk of collision unless their operation is adequately controlled.
- Conventional health and safety risks associated with the lifting operations also need to be addressed by the RP.

869. I assessed the RP's "PCSR Chapter 28 Fuel Route and Storage" (Ref. 19). I considered the Fuel Handling and Storage System (PMC) [FHSS] related documents (Ref. 177, Ref. 178, Ref. 179, Ref. 180) and drawings (Ref. 181, Ref. 182, Ref. 183, Ref. 184, Ref. 185). I used these to understand how the spent fuel cask will be imported, prepared, loaded and exported.

870. From this review, I judged that there are features of the Fuel Handling and Storage System that may expose operators to conventional health and safety, and radiological hazards / risks that may be avoidable. As such I judged these to have not been reduced to ALARP.

871. As a result, I raised RO-UKHPR1000-0014 (Ref. 186) to address the issues associated with nuclear lifting and handling operations in the Fuel Building.

872. The RO identified the following Actions (ROA):

ROA.1 Fuel Building handling operations and hazard identification

- Generate detailed flow diagrams that adequately describe the new and spent fuel handling operations.
- Review the design of the Spent Fuel Building and identify the nuclear, radiological and conventional health and safety hazards that are present.

ROA.2 Fuel Building consequence analysis

- Undertake a proportionate consequence analysis/assessment to determine the worst-case scenarios (e.g. at the fully raised position) that could result from the hazards identified.

ROA.3 Fuel Building optioneering and demonstration relevant risks are reduced SFAIRP

- Demonstrate compliance with the statutory requirements of UK legislation;
- Demonstrate for new fuel handling, spent fuel storage and handling, and spent fuel export operations, the chosen option(s) which reduces risks so far as is reasonably practicable (SFAIRP) has been selected; and
- Demonstrate a process of optimisation has been followed in a robust, transparent manner, which forms part of the UK HRP1000 generic safety case.

873. My assessment is based upon the resolution of Actions ROA.1 to 3 in this RO, which the RP outlined in its Resolution Plan (Ref. 186).

874. The basis of my Mechanical Engineering assessment for RO-UKHPR1000-0014 has been the generic fuel route safety case and design at DR2.1.

4.10.1 Assessment

875. RGP for lifting operations within the Fuel Building includes:

- ONR SAPs:
  - FP.4 (Safety assessment) considers effective understanding and control of hazards through safety assessment;
  - EKP.3 (Defence in depth) considers defence in depth in the prevention of significant faults and their progression;
  - EMT.6 (Reliability claims) considers the provision for EIMT throughout the plant’s lifetime;
  - EHF.6 (Workspace design) considers the design of workspaces to ensure tasks can be undertaken safely and reliably;
  - ELO.1 (Access) considers the design and layout of facilities to minimise adverse interactions; and
  - ELO.4 (Minimisation of the effects of incidents) considers the layout and design of facilities to minimise the effects of faults and accidents.
- ONR TAGs:
  - NS-TAST-GD-005 ONR Guidance on the Demonstration of ALARP
  - NS-TAST-GD-056 Nuclear Lifting Operations

4.10.1.1 Fuel Building Handling Operations and Hazard Identification (ROA.1)

876. The RP produced two documents:

- “Fuel Handling Process and Operations” (Ref. 187)
- “Hazards Identification and Consequence Assessment of Fuel Handling Operations” (Ref. 188).

877. These documents provided more clarity on how operations in the Fuel Building would be undertaken and what hazards were present during them.

878. Through the above two documents, the RP confirmed there were significant conventional and radiological hazards to be addressed. I raised several RQs to gain clarity on the RP’s design in respect to the conventional and nuclear safety related hazards (Ref. 6):

Conventional Safety Hazards

- RQ-UKHPR1000-0185 Prevention of falls into pond, pits and hoist wells
- RQ-UKHPR1000-0220 Design of Lifting Systems for Maintenance
- RQ-UKHPR1000-0221 Crane Interactions
- RQ-UKHPR1000-0993 Loading Pit to Cleaning Pit Operations

Nuclear Safety Hazards

- RQ-UKHPR1000-0404 Fuel Handling and Storage Safety Functions
- RQ-UKHPR1000-0994 Auxiliary Crane Recovery
- RQ-UKHPR1000-0993 Loading Pit to Cleaning Pit Operations
- RQ-UKHPR1000-1090 Protection Against Restrained/Snagged Fault Leading to Dropped Load
- RQ-UKHPR1000-1091 EIMT of Lifting Systems (Use of Auxiliary Lifting Equipment)

879. The above RQs supported closure of RO-UKHPR1000-0014. The RP's responses are discussed further in sub-section 4.10.1.3 of this report. The RP presented its progress on RO-UKHPR1000-0014 closure at a technical meeting in January 2020 (Ref. 189). At this stage, the RP was not intending to include consideration of the spent fuel cask and storage cylinder designs within the GDA scope.

880. I considered this position unacceptable. I also confirmed that the feasibility of the equipment design is within GDA scope (Ref. 190). In my opinion, the RP must be able to demonstrate, during GDA, that the fuel handling equipment design can meet the requirements placed upon it by the safety case. However, such designs should not foreclose any options for the cask design, which is outside the scope of GDA and will be decided by the licensee. The RP accepted this approach (Ref. 7).

881. The RP submitted its hazard identification document at Revision B (Ref. 188) in June 2020. I provided feedback to the RP (Ref. 191) to support the RP's alignment with RGP. For example, the RP's assessment did not:

- consider un-mitigated faults (see sub-section 4.2.1.3 of this report); or
- align with guidance in ONR's Nuclear Lifting TAG, NS-TAST-GD-056 (Ref. 4), which considers safety measures to protect against relevant faults, e.g. overload, restrained load and over speed conditions.

882. ONR received Revision C in September 2020 and Revision D in November 2020. I assessed Revision D (Ref. 188) and concluded that, from a Mechanical Engineering perspective:

- processes are suitably identified and presented; and
- the identified hazards are sufficiently detailed for the purposes of GDA.

883. My concerns regarding the Fuel Building hazard identification are covered by Action ROA.2 below.

4.10.1.2 Fuel Building Consequence Analysis (ROA.2)

884. I assessed Revision D of the RP's "Hazards Identification and Consequences Assessment of Fuel Handling Operations" report (Ref. 188). I concluded it suitable, as radiological consequences are identified for each of the hazards. The assessment of the calculated doses is outside the scope of my Mechanical Engineering assessment.

885. My conclusion noted that the design of the spent fuel cask and its inner cannister are outside of the scope of GDA. These will be further developed within the site-specific stages. I consider this acceptable for GDA.

886. Those hazards and consequences from (Ref. 188), identified as conventional health and safety related, are captured in the RP's design risk register (Ref. 192). This allows

these to be separately managed by the RP's conventional health and safety team. I confirmed with ONR's Conventional Health and Safety inspector that this is appropriate for managing these risks.

887. The RP's analysis aligned with a hazard and operability (HAZOP) process (Ref. 193). It assessed:

- hazards;
- initiating events;
- consequences to workers and the public;
- categorisation of safety functions; and
- the classification and substantiation of safety measures.

888. In each case, the RP assessed the unmitigated faults and consequences. I considered that, from a Mechanical Engineering perspective and based on the design and safety case assessed, the RP's approach was reasonable.

889. The RP's analysis showed where the consequences of an initiating event (fault) were ALARP or otherwise. It identified a plan to develop ALARP assessments and identify reasonably practicable improvements that could be made. These were submitted and are assessed within ROA.3 below.

890. The faults considered in my assessment were taken from the RP's own fault analysis. The adequacy of the fault analysis itself is assessed by ONR's Fault Studies discipline (Ref. 70) and addressed through the resolution of RO-UKHPR1000-0056, Fuel Route Safety Case (Ref. 194).

4.10.1.3 Fuel Building Optioneering and Demonstration Relevant Risks are Reduced SFAIRP (ROA.3)

891. Initially, the RP attempted to demonstrate that conventional, nuclear and radiological risks were ALARP without changing the building layout or handling equipment design (Ref. 7). I did not consider this appropriate, as options for reducing risks were being foreclosed.

892. Unable to demonstrate risks were ALARP, the RP accepted that design changes would be required to the Fuel Building (Ref. 6). Importantly, as part of its optioneering, the RP agreed that options would no longer be space constrained. The RP established a Fuel Building Working Group (Ref. 195) to assess, in detail, the options being considered. This involved using multi-disciplined reviews of options to ensure a holistic view of these was considered.

893. The outcome of this review was that the RP enlarged the Fuel Building envelope. This was achieved by increasing its width and height and by lengthening the floor area of the +18.3 metre level operating floor. The benefits of this are summarised below:

- The Spent Fuel Cask is imported and exported in a vertical orientation, thereby eliminating the need to rotate the cask.
- Full-length walkways are provided on both sides of the building, thereby allowing safe access for breakdown recovery of the Fuel Building cranes at any point.
- The handling and process equipment for spent fuel loading and export could be stored on the +18.3 metre level operating floor. This would reduce the number of lifting or handling operations and the need for equipment to be removed from the building and brought back in.

- Auxiliary Crane travel was restricted to prevent heavy loads being carried over the Spent Fuel Pool, thereby reducing the risk of damaging fuel assemblies.
- A heat exchanger was repositioned so that it was no longer underneath the Hoisting Pit. Therefore, it could not be damaged by a dropped load, eliminating the risk of a significant pool leak. This aligns with my expectations against ONR SAP ELO.4 (Minimisation of the effects of incidents) for GDA.
- Building headroom was increased to provide suitable lifting facilities for Fuel Building crane maintenance through-life. This aligns with my expectations against ONR SAP EMT.6 (Reliability claims) for GDA.

894. Although these were notable improvements, several issues remained that required resolution within GDA. These were principally:

- The Spent Fuel Pool Crane (SFPC) pensile[†††††] walkway was raised to clear the handrails around the pool but did not provide sufficient headroom for operators on the +18.3 metre level floor. This did not align with the requirements of LOLER Regulation 6 (Positioning and installation), which requires the employer to ensure that the risk of striking a person from either the lifting equipment or load is reduced ALARP.
- An intermediate level platform was introduced into the Loading Pit. The spent fuel cask would be placed on it to lid, seal and prepare the spent fuel cask for export. However, it was not evident how these operations could be undertaken safely or how safe operator access would be achieved around the full perimeter of the cask. This did not align with my expectations against ONR SAP EHF.6 (Workspace design).

895. Several technical meetings took place in which my concerns were discussed (Ref. 7). The RP then identified further options to reduce risk ALARP. For example:

- Repositioning the SFPC pensile walkway to the other crane bridge girder meant that the walkway could be kept within the confines of the Fuel Pool handrailing, i.e. not raised above it. This had advantages in that the operator’s view of the fuel handling operations is not compromised and it avoided the need to raise the SFPC gantry rail height and therefore the overall Fuel Building height.
- Introduction of a hinged lifting beam meant that it could remain attached to the spent fuel cask during fuel loading operations. This eliminated the need to reconnect the flask underwater (with poor visibility) thereby reducing the risk of a dropped cask. Additionally, this should avoid the need to adjust water levels within the Loading Pit during fuel loading operations. The RP shows the beam to rest against a fitting or area of the pool wall when not in use and attached to the Spent Fuel Cask Crane (SFCC). There is potential for this to cause wear or damage to the wall, however I judge that this is not a significant risk and should be considered during detailed design as the design of this is not sufficiently advanced within GDA. I consider this to be normal business for the licensee.
- The RP introduced access platforms that provided full operator access to undertake the processes and operations needed to prepare the spent fuel cask for export. The RP improved its alignment with my expectations against ONR SAP ELO.1 (Access) and EHF.6 (Workspace design).

896. To conclude the optioneering, the RP produced three ALARP reports (Ref. 168, Ref. 112, Ref. 196).

[†††††] *A pensile walkway is one that hangs (is suspended) from the structure. In this case, the spent fuel pool crane structure.*

897. I assessed these using ONR's guidance on ALARP (Ref. 4) and concluded that the RP had:

- suitably assessed its design;
- considered RGP;
- defined reasonable options, considering risk;
- suitably assessed whether options could be implemented; and
- considered the benefit of combining options to achieve an ALARP position.

898. Following its own processes (Ref. 158, Ref. 148), I consider that the RP made suitable design modifications during GDA.

899. However, I identified an additional matter during my assessment of the reports related to the fault frequency associated with a dropped load from the SFPC. In its "Safety Assessment Report for the PMC [FHSS] Related Operations" (Ref. 197), the RP defines the frequency of this drop as between 1×10^{-3} and 1×10^{-5} pa. I noted from Revision D of its "Classification of Typical Cranes" (Ref. 58) the hoist load path, which would need to fail for the drop to occur, is Class 2.

900. ONR's guidance on Categorisation and Classification of SSCs, NS-TAST-GD-094 (Ref. 4), defines a Class 2 SSC as having a failure frequency of between 1×10^{-2} and 1×10^{-3} pa. Hence, the classification and reliability of the crane's load path does not align with the claimed dropped load (load path failure) fault frequency. In accordance with ONR guidance I consider that a Class 1 load path may be more appropriate as this provides greater reliability (failure frequency of between 1×10^{-4} and 1×10^{-5} pa).

901. I considered that the RP could address this matter through its work responding to RO-UKHPR1000-0056. This RO considered the adequacy of the fuel route safety case. Increasing the classification of the load path from Class 2 to Class 1 should not significantly impact the mechanical engineering aspects of the design. Hence, I judge that it does not detrimentally impact the conclusions of my assessment of RO-UKHPR1000-0014. See sub-section 4.11 in this report for further information on RO-UKHPR1000-0056.

902. The RP also undertook additional work to redesign the lifting and handling equipment for cask operations within the Loading and Cleaning Pits. During my assessment, I reviewed the lifting arrangements for moving the loaded cask from the Loading Pit to the Cleaning Pit.

903. I noted that when the filled cask is lifted from the Loading Pit to the Cleaning Pit, the inner cover is not secured to the cannister and the outer cover and cask lid are not fitted (see Figure 22).

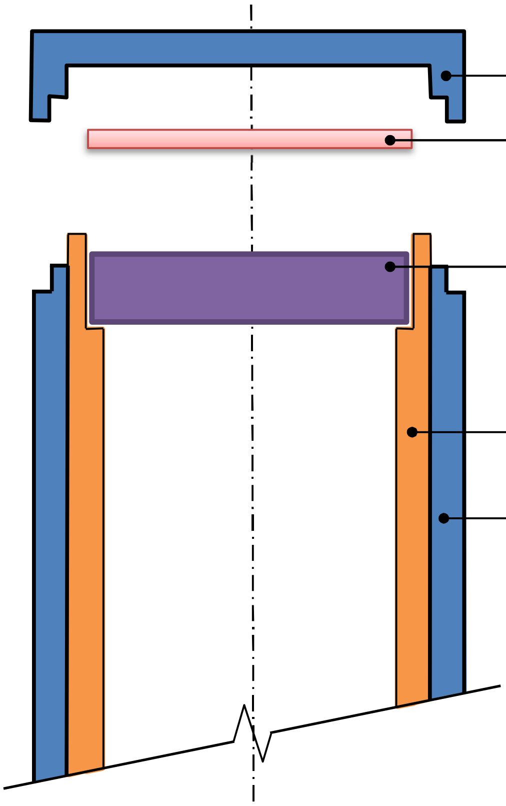

Figure 22: Diagram of spent fuel cask and inner cannister

904. I raised RQ-UKHPR1000-1583 (Ref. 6) to address queries relating to the cannister lid operations.

905. The RP submitted "Radiological Consequences Analysis of Dropping a Spent Fuel Cask" (Ref. 198). This document shows that if a full spent fuel cask is dropped in the Loading Pit, the radiological consequences are above the Target 4 basic safety level (BSL) within ONR SAP NT.1 (Assessment against targets). This would occur if:

- the drop height is 7.64 metres;
- the cask lands and topples over; and
- all the fuel elements are spilled from the cask into the Loading Pit (conservative assumption).

906. The SFCC is designated a Class 1 load path (defined in (Ref. 58)).

907. In its response to my RQ, the RP provided an explanation, with diagrams, of how the inner cover is held in place during lifts within its other operating plants. However, the method shown does not 'secure' the inner cover to the cannister, nor mitigate the risk of fuel assemblies falling from the cask if it toppled i.e. the fault the RP has identified in (Ref. 198).

908. Consequently, I judge there to be a shortfall regarding adequate mitigation of an identified fault within the GDA design. Currently, if the fault occurs, then there is no engineered barrier to prevent, or reduce the risk of fuel spillage within the Loading Pit. This results in a potentially significant operator dose, which I consider to be a shortfall against ONR SAP EKP.3 (Defence in depth). The licensee should address this during

detailed design as further design decisions are required. Consequently, I have raised an Assessment Finding:

AF-UKHPR1000-0140: The licensee shall demonstrate, during detail design, that the spent fuel cask design, including handling operations, reduces risks as low as reasonably practicable. This shall include prevention or mitigation of spent fuel assemblies falling from the cask should it topple within the Loading Pit.

909. The design of the spent fuel cask is outside the scope of GDA. Hence, I judge that the current design of the SFPC, SFCC and associated lifting equipment, does not foreclose the licensee from addressing this fault.

4.10.2 Strengths

910. In response to ONR's concerns, the RP undertook a broad ranging study of options (Ref. 187). This resulted in several design changes to the Fuel Building and lifting operations within it.

4.10.3 Outcomes

911. The RP has produced a suite of ALARP assessments (Ref. 168) to (Ref. 196) to support its decision making.

912. As a result of its response to RO-UKHPR1000-0014, the RP has identified several improvements to its generic design. These are implemented via four, key design modifications during Step 4 (Ref. 148):

- M66 Design Modification of Spent Fuel Delivery Process
- M76 Design Modification of Fuel Handling Equipment in Fuel Building
- M77 Design modification of Operation envelop control of Auxiliary Crane
- M78 Design Modification for Maintenance of Spent Fuel Cask Crane

913. I consider that the RP has provided sufficient evidence to allow RO-UKHPR1000-0014 (Ref. 199) to be closed.

914. I have identified one Assessment Finding relating to the adequacy of the engineered measures to mitigate a dropped load fault during lifting of the spent fuel cask from the Loading Pit to the Cleaning Pit.

915. I have not identified any Minor Shortfalls.

916. The Assessment Finding is listed in Annex 3.

4.10.4 Conclusion

917. I judge that:

- The RP has clarified the scope of fuel handling operations.
- A sufficient assessment of the hazards and consequences has been presented.
- The RP has undertaken an appropriate assessment of options, OPEX and RGP. This enabled it to show that the generic design reduces the risks associated with fuel handling operations ALARP.
- Significant design modifications to the Fuel Building have been made. This has reduced risks in relation to conventional and nuclear safety-related concerns identified by RO-UKHPR1000-0014.

918. The RP has provided assurance that its design can meet relevant statutory requirements of UK legislation, through appropriate consideration of:

- the design;
- risks to workers and the public;
- optioneering; and
- relevant good practice.

919. The RP has provided arguments and evidence within its ALARP assessment submissions (Ref. 168) to (Ref. 196). These demonstrate that for new fuel handling, storage and handling of spent fuel, and spent fuel export operations the chosen option(s) reduce relevant risks to workers and the public ALARP.

920. I judge that the RP has shown that a process of optimisation has been followed in an appropriate and transparent manner. I was therefore able to judge that the concerns identified RO-UKHPR1000-0014 have been adequately resolved.

921. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's lifting operations within the Fuel Building are sufficient from a Mechanical Engineering perspective.

922. I have identified one matter that the licensee will need to address during the detailed design. I have captured this in an Assessment Finding.

4.11 RO-UKHPR1000-0056 Fuel Route Safety Case

923. As described in sub-section 4.10, I raised RO-UKHPR1000-0014 (Ref. 186). This required the RP to provide further justification for lifting operations within the Fuel Building, with an emphasis on the engineering design. The RP resolved the RO-UKHPR1000-0014 related gaps (see sub-section 4.10 of this report).

924. However, assessment of the overall fuel route safety case, led by Fault Studies, identified additional shortfalls. RO-UKHPR1000-0056 (Ref. 194) was raised to address these. When considered together, the RP's response to both ROs should provide:

- the holistic safety case; and
- the engineering substantiation that underpins it.

925. The assessment of the fault analysis aspects of RO-UKHPR1000-0056 is reported in the Fault Studies Assessment Report (Ref. 70).

926. RO-UKHPR1000-0056 identified the following actions (ROA):

ROA.1 Handling of Spent Nuclear Fuel

- In response to this Regulatory Observation Action, the RP should provide a suitable and sufficient safety case for the handling of spent fuel by the Spent Fuel Pool Crane (SFPC). This should demonstrate that the relevant risks from spent fuel handling have been reduced to ALARP.

ROA.2 Handling of Spent Fuel Casks

- In response to this Regulatory Observation Action, the RP should provide a suitable and sufficient safety case for the handling of spent fuel casks within the Fuel Building (BFX). This should demonstrate that the relevant risks from spent fuel cask handling have been reduced to ALARP.

927. Improvements to the safety case from RO-UKHPR1000-0056 resolution, could have resulted in engineering design changes. Hence, I considered it important that this was assessed by Mechanical Engineering given the link with RO-UKHRP1000-0014.

928. The main outcome of RO-UKHPR1000-0056, was design modification M94 “Modifications of the BFX to Adopt Gantry Crane for Fuel Handling” (Ref. 148). This changed the SFPC and Fuel Building design.

929. My assessment sampled the RO-UKHPR1000-0056 submissions relevant to Mechanical Engineering supporting RO closure, for each of the RO Actions.

4.11.1 Assessment

930. In response to RO-UKHPR1000-0056 the RP amended its fuel route safety case. This identified that several faults and hazards could be removed or reduced by engineering design changes to the SFPC. My RO-UKHR1000-0056 assessment targeted the Mechanical Engineering aspects of these. The adequacy of the fuel route safety case is assessed by other ONR disciplines (Ref. 70, Ref. 200, Ref. 201).

931. My assessment targeted the following areas:

- The adequacy of the RP's ALARP process. For example:

   - the optioneering undertaken and the consideration of alternative engineering solutions to address safety case related concerns;
   - its demonstration that options considered were adequately assessed
   - its consideration of risks eliminated, added, or controlled by the options; and
   - its demonstration that the chosen solution reduces risks to ALARP.

- The feasibility of the chosen option.
- Whether the classification of the SFPC hoist load path is appropriate. I identified this in my RO-UKHPR1000-0014 assessment (see sub-section 4.10 in this report).

932. Mechanical Engineering RGP in relation to RO-UKHPR1000-0056 includes:

- ONR SAPs:

   - FP.3 (Optimisation of protection), FP.5 (Limitation of risks to individuals) and FP.6 (Prevention of accidents) consider the optimisation of safety and preventing or mitigating radiation risks;
   - EKP.3 (Defence in depth) considers the provision of independent barriers. These should be aimed at preventing faults or limiting the consequences if they do occur;
   - EKP.5 (Safety measures) considers a hierarchy of safety measure characteristics;
   - ECS.1 (Safety categorisation) considers the identification and categorisation of safety functions, based on their safety significance;
   - ECS.2 (Safety classification of structures, systems and components) considers classification of SSCs based on their importance to nuclear safety;
   - ECS.3 (Codes and standards) considers appropriate codes and standards to be identified for safety related SSCs. These should reflect the reliability requirements based on the classification;
   - EDR.1 (Failure to safety) considers the need for inherently safe designs or that SSCs fail in a safe manner;
   - EMT.2 (Frequency) considers how often EIMT is required;
   - ELO.1 (Access) considers the design and layout of facilities to minimise adverse interactions;
   - EMC.7 (Loadings) considers design loadings and their frequency of occurrence for normal, fault and accident conditions;
   - ERL.3 (Engineered safety measures) considers that automatically initiated safety measures should be provided when reliable and rapid protection is needed;
   - NT.1 (Assessment against targets) Target 4 considers the effective dose objectives and limits for design basis faults; and
   - RP.7 (Hierarchy of control measures) considers establishing a hierarchy of control measures in accordance with IRR17.

- The Management of Health and Safety at Work Regulations 1999 (MHSWR) Regulation 4 and Schedule 1 (Ref. 45). This requires the application of general principles of prevention.
- The Lifting Operations and Lifting Equipment Regulations 1998 (LOLER) (Ref. 152). This sets out legal requirements associated with the design, manufacture and use of lifting equipment.

4.11.1.1 Handling of Spent Nuclear Fuel

933. My assessment of the RP's submissions considered on the following submissions:

- "Optioneering Report for Spent Fuel Pool Crane" (Ref. 202)
- "Classification of the Typical Cranes" (Ref. 58)
- "Technical Specification for Spent Fuel Pool Crane" (Ref. 203)
- "Impact Analysis Report of the Fuel Building Modification" (Ref. 204)
- "Summary of Fuel Route Safety Case in BFX" (Ref. 60)

934. Within the Optioneering Report (Ref. 202), the RP identifies four potential options for the SFPC and Fuel Building design. Options 2, 3 and 4 were very similar. There were variations of the building layout but using the same gantry crane proposed in Option 2. As my Mechanical Engineering assessment would not cover the building design, I focussed my assessment on Options 1 and 2:

- Option 1: Retain the current design and incorporate modifications to reduce or eliminate some of the hazards.
- Option 2: Modify the crane type from an overhead crane to a modified gantry crane for fuel handling operations.

935. During my assessment, I identified the following areas of concern:

- For Option 1:
    - The identified safety case gaps (new faults) are not sufficiently addressed by the proposed modifications.
    - Sufficient consideration of preventing a collision of a Spent Fuel Assembly (SFA) with the pond wall or over the pond wall has not been made.
- For Option 2:
    - EIMT (crane and lifting equipment) is not sufficiently considered. Examples include, access / egress, crush hazards, statutory examinations and inspections, and confined spaces.
    - Safe recovery from faults is not sufficiently considered.
    - The safety case did not adequately show that mechanical or C&I reliability claims offer sufficient levels of prevention / protection against the faults.
    - The safety functions for key components were not clear.
    - Evidence that principles of prevention (MHSWR) have been applied by the designer was not included.
    - The SFPC interactions with other cranes in the Fuel Building were not clear.

936. I consider that my concerns related to Option 1 would not change the RP's overall conclusion that Option 2 reduces risks to ALARP. However, the licensee may wish to address these during site-specific stages. I have therefore identified this as a Minor Shortfall.

937. A diagram of the BFX, which shows Option 2 is shown in Figure 23.

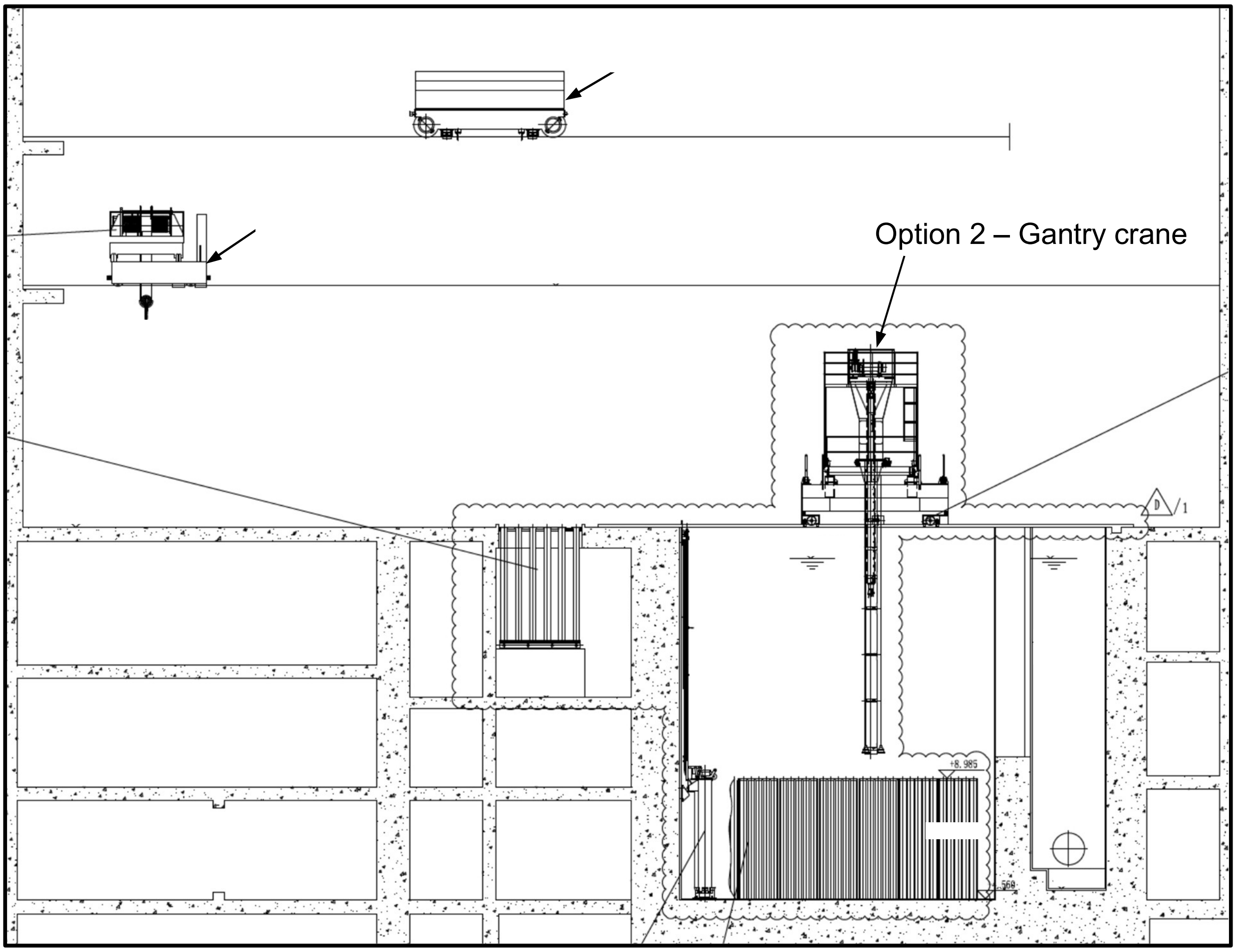

Figure 23: Layout of cranes in BFX following RO-UKHPR1000-0056

938. I held three technical meetings with the RP (Ref. 205, Ref. 206, Ref. 207) to discuss Option 2. The following paragraphs summarise the Mechanical Engineering related concerns I raised with the RP.

Mechanical Overtravel Protection

939. I applied the following ONR SAPs to my assessment of the SFPC overtravel protection:

- EKP.3 (Defence in depth).
- ECS.1 (Safety categorisation)
- ECS.2 (Safety classification of structures, systems and components) and
- ECS.3 (Codes and standards).
- ERL.3 (Engineered safety measures)
- RP.7 (Hierarchy of control measures)

940. Shortfalls identified against RGP include:

- I consider the mechanical overtravel protection against the SFPC fixed sleeve colliding with the pond walls (overtravel) to be insufficient against ONR SAPs EKP.3 (defence in depth), ECS.3 (Codes and standards) and ERL.3 (Engineered safety measures). This gap is relevant to 7 of the 12 SFP walls (see thick, dotted lines in Figure 24).

  Note: the RP's 'preference' is to claim C&I protection, which may be more difficult to substantiate over Mechanical Engineering means.

- Mechanical buffers protect against the overtravel fault on 5 of the 12 walls (see thick, dashed lines in Figure 24). The RP claims two, diverse means of mechanical protection exist (a buffer and torque limiter). Considering ONR SAP EKP.3 (defence in depth), the torque limiter does not prevent the fault. I acknowledge the torque limiter offers some protection against fault progression. Hence, when considering ONR SAP ECS.2 (Safety classification of structures, systems and components), for this fault the single Class 1 mechanical buffer does not adequately protect against overtravel.

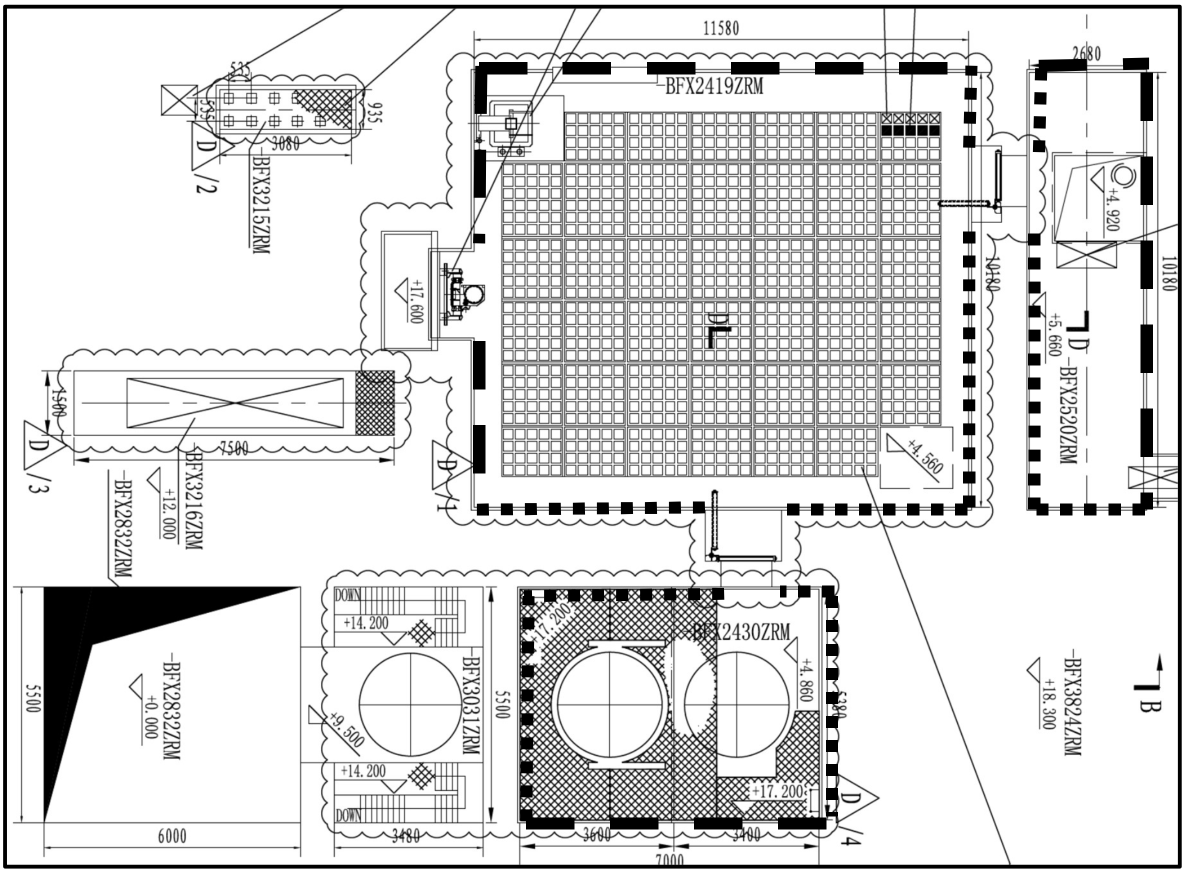

Figure 24: Spent Fuel Pool overtravel protection

- The SFPC fixed and telescopic sleeves are not currently claimed as safety measures to protect the fuel being damaged following a collision. However, I noted the RP's arguments do make claims on the integrity of the sleeves in its safety case (Ref. 60). The sleeves are neither classified nor substantiated. Hence, further consideration of the safety functions of the SFPC fixed and telescopic sleeves is required in line with ONR SAPs ECS.1 (Safety categorisation).

- Currently only a Class 3 C&I system is claimed, alongside administrative controls, to protect against the Auxiliary crane lifting any heavy items, removed from the SFPC during EIMT, over the Spent Fuel Pond[‡‡‡‡‡]. No mechanical safety measures are in place. I consider this insufficient against ONR SAP RP.7 (Hierarchy of control measures).

941. These shortfalls are captured within Assessment Finding AF-UKHPR1000-0141.

Spent Fuel Pool Crane Hoist Classification

942. I applied ONR SAPs ECS.2 (Safety classification of structures, systems and components) and NT.1 (Assessment against targets) Target 4 to my assessment of the SFPC hoist classification. I also used guidance within ONR's Categorisation and Classification TAG NS-TAST-GD-094.

943. SFPC hoist classification shortfalls against RGP include:

- The Class 2 SFPC hoist may be insufficient considering ECS.2 (Safety classification of structures, systems and components) given:
  - The hoist reliability for a Class 2 SSC is between 1 x10^{-2} and 1 x10^{-3} pa, identified in ONR's Categorisation and Classification guidance NS-TAST-GD-094 (Ref. 4).
  - The RP calculates the worker dose following a dropped load within the pond to be between 200 and 500 mSv from (Ref. 59).
  - To align with ONR SAP NT.1 (Assessment against targets) Target 4 BSL, the SFPC hoist reliability should be at least between 1 x10^{-4} and 1 x 10^{-5} pa.

944. A Class 1 SFPC hoist would appear to be more appropriate. However, I note that Revision E of (Ref. 59) states the dose as below 200 mSv. This does not change the key conclusions of my assessment. This shortfall is captured within Assessment Finding AF-UKHPR1000-0141.

Examination, Inspection, Maintenance and Testing Arrangements

945. I applied ONR SAPs ELO.1 (Access) and EMT.2 (Frequency) in my assessment of the EIMT arrangements. I also considered the requirements of LOLER (Ref. 152).

946. Shortfalls against EIMT arrangements RGP include:

- The hook clearance between the Auxiliary crane and SFPC may not allow the safe removal and replacement of heavy items. ONR SAP ELO.1 (Access) is relevant here. This also applies to the SFCC and Auxiliary crane clearance. This shortfall is captured within Assessment Finding AF-UKHPR1000-0142.
- The method by which heavy items are moved from and to the Auxiliary crane during EIMT also requires further consideration. This too should align with ONR SAP ELO.1 (Access). This shortfall is also captured within Assessment Finding AF-UKHPR1000-0142.
- The RP's design currently assumes that EIMT activities on the Telescopic Sleeve are infrequent. ONR advised that under LOLER (Ref. 152), thorough examination of the lifting equipment will be required at least every 12 months (6 months for lifting accessories and lifting equipment lifting persons). Safe access

[‡‡‡‡‡] *Dropping of a heavy load into the pond could lead to damaged fuel.*

for these activities also requires consideration. The current design is judged not to align with ONR SAP EMT.2 (Frequency) and ELO.1 (Access). I consider this to be a Minor Shortfall. It relates to the licensee addressing matters relating to compliance with relevant legal requirements.

Management of Crane Operations

947. I considered ONR SAP RP.7 (Hierarchy of control measures) in my assessment of the management of crane operations. This included how cranes may interact and how this is controlled.

948. The operational restrictions proposed for the Auxiliary crane and SFPC during new fuel operations require further development. The RP proposes to use a 'soft park' position, i.e. the crane is temporarily parked out of the way, with power still connected. This is reasonable for GDA, but greater assurance that sufficient control and management of crane operations will be required. I consider this appropriate for the site-specific stages. I consider that this sufficiently meets ONR SAPs RP.7 (Hierarchy of control measures) for GDA and can be taken forward as normal business.

Spent Fuel Pool Sluice Gates

949. I applied the following ONR SAPs to my assessment of the SFP sluice gates:

- RP.7 (Hierarchy of control measures)
- EKP.3 (Defence in depth)
- EKP.5 (Safety measures)
- EMC.7 (Loadings)
- EDR.1 (Failure to safety)

950. SFP sluice gates shortfalls against RGP include:

- The SFP sluice gates are opened and closed for normal operations and EIMT related tasks. Opening both gates at the same time, may result in the SFP water level falling below its minimum level for safe operation. This could lead to elevated operator doses. The RP stated that its reference design (FCG3) uses administrative controls to manage the opening and closing. There are currently no engineered measures to prevent simultaneous gate opening. I consider this a shortfall against ONR SAP RP.7 (Hierarchy of control measures). This SAP references IRR17 Regulation 9(2), which requires action to be taken to control doses by engineered means in the first instance. Only after these have been applied, should systems of work be considered.
- SFPC collision with the sluice gates is not currently considered within the generic design. I consider this a shortfall against ONR SAP EMC.7 (Loadings). Given a collision shortfall exists with the SFPC fixed and telescopic sleeves (discussed in the mechanical overtravel protection sub-heading), the integrity of the sluice gates and/or requirement for additional protective measures should be considered against ONR SAP EKP.3 (Defence in depth).
- The SFP sluice gates sealing arrangement appears overly complex. The current arrangement uses a pressurised gas seal. The gas pressure is monitored to identify any pressure loss i.e. loss of ability to sufficiently seal. When asked why it was not possible to use a simpler sealing arrangement, the RP was unable to adequately justify its choice. This was originally designed for the previous SFPC and EIMT operations, which were not undertaken in the Transfer Compartment. Given the revised EIMT arrangements for the SFPC,

the option of a simpler, passive sealing arrangement should be considered against the expectations of ONR SAPs EKP.5 (Safety measures) and EDR.1 (Failure to safety).

951. These shortfalls are captured within Assessment Finding AF-UKHPR1000-0143.

Confined Spaces

952. ONR's Conventional Health and Safety inspector attended the third technical meeting with the RP (Ref. 207). The RP's consideration of The Confined Spaces Regulations 1997 was discussed. An Assessment Finding has been raised in the Conventional Health and Safety Assessment Report (Ref. 208).

Safe Isolations

953. The revised SFPC design requires EIMT to be undertaken on the telescopic sleeve. The RP proposes to undertake this in the Transfer Compartment. To do this, the sluice gate must be closed, and the compartment drained.

954. Given the potential for confined spaces (see (Ref. 208)), I queried whether HSG253 "The safe isolation of plant and equipment" (Ref. 126) had been considered. The Fuel Pool Cooling and Treatment System (PTR) [FPCTS] is used to fill the compartments and should be suitably isolated during EIMT.

955. The RP claimed that the isolation and drainage arrangements for the PTR [FPCTS] have been assessed against HSG253. It also stated that this is discussed in the DRRs (Ref. 207).

956. I have not included the PTR [FPCTS] in my assessment sample for HSG253 (see sub-section 4.5 of this report). I consider that this will be addressed as part of AF-UKHPR1000-0137 (identified in sub-section 4.5.1), concerning HSG253 compliance.

Summary

957. The above Mechanical Engineering shortfalls are applicable to both the spent fuel pool operations and the safety case. I judge them significant enough that it is necessary to track them to completion.

958. The shortfalls will require site or operator specific design choices, and/or information that is currently not available. These should be made during detailed design and/or site-specific stages. I have therefore raised the following Assessment Findings:

AF-UKHPR1000-0141: The licensee shall, during detailed design, justify the design and safety case for the Spent Fuel Pool Crane. This should:

- identify diverse, engineered prevention and protection measures for all design basis faults;
- using the hierarchy of control measures, justify the choice of mechanical and/or control and instrumentation safety measures;
- justify the hoist load path classification; and
- substantiate claims made against the integrity of the fixed and telescopic sleeves.

AF-UKHPR1000-0142: The licensee shall, during detailed design:

- justify the means for handling 'heavy items' such as hoist drums or motors, during examination, inspection, maintenance and testing of Fuel Building cranes; and
- demonstrate that there is sufficient clearance between cranes to allow safe removal and replacement of such items.

AF-UKHPR1000-0143: The licensee shall demonstrate, during detailed design, how the Spent Fuel Pool sluice gate design arrangement aligns with the hierarchy of control measures in:

- preventing or protecting against inadvertent opening;
- preventing or withstanding a collision by the Spent Fuel Pool Crane whilst closed, stopping water entering either the Transfer Pit or Loading Pit; and
- reducing the risk of water ingress into the Transfer Pit and Loading Pit via a suitable sealing design.

959. The Fault Studies Assessment Report (Ref. 70) also raises an Assessment Finding concerning the Fuel Route Safety Case.

960. During the technical meetings (Ref. 205, Ref. 206, Ref. 207), the RP acknowledged the shortfalls I had identified. I consider that these can be addressed by a licensee during detailed design and/or site-specific stages.

4.11.1.2 Handling of Spent Fuel Casks

961. In closing RO-UKHPR1000-0014 (Ref. 199), I judged the Mechanical Engineering related Spent Fuel Cask Crane modifications to be ALARP for GDA.

962. The RP has made no changes to either its classification of mechanical SSCs, or the engineering design during its work to close RO-UKHPR1000-0056. Hence, my Mechanical Engineering judgement is unchanged (see sub-section 4.10 of this report).

963. The suitability of the safety analysis and safety case is judged within the Fault Studies (Ref. 70), Fuel and Core (Ref. 201), and Probabilistic Safety Assessment (Ref. 200) reports.

4.11.2 Strengths

964. In response to RO-UKHPR1000-0056, the RP has undertaken a considerable amount of work to develop its concept design and safety case.

965. The RP's revised crane design shows that it can safely manage some of the risks posed in the original design.

4.11.3 Outcomes

966. The RP has provided suitable and sufficient information to show that the concept design for its SFPC is feasible. I consider this sufficient for GDA and aligns with ONR's expectations. I also consider, that from a Mechanical Engineering perspective, the RP has provided adequate evidence to close RO-UKHPR1000-0056 (Ref. 209).

967. I have identified three Assessment Findings in sub-section 4.11.1 above, which relate to the suitability of:

- the SFPC design and safety case;

- safe removal of heavy items during EIMT of the cranes; and
- the design of the SFP sluice gates.

968. I identified two Minor Shortfalls in paragraphs 936 and 946. I judge these are matters for the licensee to consider further as part of its compliance with legal requirements, including the ONR SAPs.

969. The Assessment Findings are listed in Annex 3.

4.11.4 Conclusion

970. I judge that the RP has shown that its revised Spent Fuel Pool Crane concept design is feasible.

971. It references other operating nuclear power plants using a similar design of crane, for example the Taishan EPR. This has provided me with assurance of its concept design at this stage.

972. I have noted three Assessment Findings, which are largely due to the immaturity of the RP's engineering design. I do not consider these Assessment Findings significant enough to undermine the concept design, but they do require consideration during detailed design and site-specific stages.

973. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's fuel route safety case is sufficient from a Mechanical Engineering perspective.

974. I have identified several matters that the licensee will need to address during the detailed design. I have captured these in three Assessment Findings.

4.12 Consolidated Safety Case Review

975. My Mechanical Engineering assessment of the safety case is based on the PCSR and supporting references, submitted by the RP in January 2020 for Step 4 of GDA. Since then, the RP has updated the safety case due to:

- the design's development;
- completion of Forward Action Plans;
- resolution of ROs; and
- responding to RQs.

976. At the end of Step 4 (in October 2021) the RP submitted its updated and consolidated PCSR. This was Design Reference 3.0 (DR3.0). The RP claimed to have incorporated all the changes that had occurred during Step 4 into its safety case documentation.

977. I undertook a high-level review, sampling six PCSR chapters. The aim was to give me confidence that the RP had included the outcomes achieved during my Mechanical Engineering assessment. The sampled chapters were:

- Chapter 6 Reactor Coolant System (Ref. 210)
- Chapter 7 Safety Systems (Ref. 211)
- Chapter 10 Auxiliary Systems (Ref. 212)
- Chapter 11 Steam and Power Conversion (Ref. 213)
- Chapter 23 Radioactive Waste Management (Ref. 214)
- Chapter 28 Fuel Route and Storage (Ref. 215)

978. This was not a re-assessment of the RP's safety case. My assessment of the adequacy of the RP's safety case and the findings from that are presented in the preceding sub-sections of this report (sub-sections 4.1 to 4.11). Further Mechanical Engineering assessment will be conducted throughout the site-specific stages.

4.12.1 Review

979. The aim of my review was to provide me with sufficient confidence that the RP had indeed consolidated Mechanical Engineering related improvements it had made during Step 4 into its safety case. In addition to the above PCSR chapters, also sampled the following areas where they related to my Mechanical Engineering assessment:

- six Forward Action Plans across three PCSR chapters;
- six Modifications relating to five PCSR chapters and Level 2 safety case documentation;
- responses to the four Mechanical Engineering ROs; and
- responses to 19 RQs relating to the ROs sampled and the supporting Level 2 and Level 3 safety case documentation.

980. My review confirmed that the RP has made appropriate amendments to its safety case documentation (PCSR, Tier 2 and Tier 3 samples). I provided comments to the RP (Ref. 216). The RP did not address all my comments in its updated PCSR chapters. I have identified this as a Minor Shortfall, which the licensee may wish to address during site-specific stages. My comments largely concern the clarity and readability of the safety case.

981. During a technical meeting in May 2021 (Ref. 217), the RP showed a set of documents it was using to track the amendments to safety case documents resulting from each

RO, RQ and meeting action. This provided me with an increased level of confidence that adequate consolidation arrangements were in place.

982. At the meeting in May (Ref. 217) the RP stated that its documents had been updated where necessary. Through my sample review, I have confirmed that these align with my expectation for DR3.0.

4.12.2 Strengths

983. The RP has kept a record of its consolidation work during Step 4, providing me with assurance that it captured the necessary requirements throughout its safety case.

984. The RP's safety case aligns with my expectations following my review for GDA.

4.12.3 Outcomes

985. I judge that the RP's safety case aligns with its design at Design Reference 3.0.

986. I have not raised any Assessment Findings during my review.

987. I have identified one Minor Shortfall in paragraph 980, whereby the licensee may wish to review comments provided by me (Ref. 216).

4.12.4 Conclusion

988. Based on my sample review, the RP has sufficiently consolidated the changes made during Step 4 of GDA. I judge its safety case documentation aligns with Design Reference 3.0.

989. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP. Therefore, I judge that the RP's consolidated safety case is sufficient from a Mechanical Engineering perspective.

4.13 Comparison with Standards, Guidance and Relevant Good Practice

990. During Step 3 of GDA, I identified that the RP's understanding of UK RGP was limited (Ref. 22). Statements of compliance with UK RGP were not adequately supported by evidence. I therefore raised RO-UKHPR1000-0012 (Ref. 105) to seek improvements. Sub-section 4.4 of my report presents my assessment across a sample of systems and components.

991. The RP's compliance with RGP is also discussed within other assessment sub-sections of my report (sub-sections 4.1 to 4.11) for the specific themes covered.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

992. This report presents the findings of my Mechanical Engineering assessment of the generic UK HPR1000 design as part of the GDA process. My conclusions are summarised as follows.

5.1.1 Adequacy of the UK HPR1000 Heating, Ventilation and Air Conditioning Design Substantiation

993. The RP has closed the following ROs from a Mechanical Engineering perspective:

- RO-UKHPR1000-0036 concerning its choice of HEPA filters, led by the Environment Agency; and
- RO-UKHPR1000-0039 concerning the adequacy of its HVAC related design substantiation.

994. During my assessment I raised one Assessment Finding.

995. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

996. The RP has addressed my concerns raised within RO-UKHPR1000-0039. I judge, for the purpose of GDA, that the RP's substantiation of the HVAC system design is adequate from a Mechanical Engineering perspective.

5.1.2 Adequacy of the Mechanical Engineering Schedule, including the Implementation of Safety Functional Categorisation and Safety Classification

997. There were no Mechanical Engineering led ROs raised in this Theme. RO-UKHPR1000-0004 concerning development of a suitable and sufficient safety case is assessed in the ONR Cross-Cutting (Ref. 49) report.

998. During my assessment I raised four Assessment Findings.

999. The RP has produced a categorisation and classification methodology. This allows safety function traceability in the safety case. A complete list of Mechanical Engineering safety functional requirements will be needed in site-specific stages.

1000. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

5.1.3 Adequacy of Equipment Qualification Arrangements

1001. The RP has closed the following RO from a Mechanical Engineering perspective:

- RO-UKHPR1000-0048 concerning the equipment qualification of Mechanical Engineering based SSCs.

1002. During my assessment I raised four Assessment Findings.

1003. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1004. The RP has addressed my concerns raised within RO-UKHPR1000-0048. It has improved its understanding of EQ requirements and shown its EQ methodology can be implemented. I judge this to be suitable from a Mechanical Engineering perspective for the purposes of GDA.

5.1.4 Closure of Gaps Against Relevant Good Practice

1005. The RP has closed the following RO from a Mechanical Engineering perspective:

- RO-UKHPR1000-0012 concerning the identification and application of RGP applicable to Mechanical Engineering for the UK HPR1000 design.

1006. I raised no Assessment Findings during my assessment.

1007. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1008. The RP has addressed my concerns raised within RO-UKHPR1000-0012. It has implemented design modifications where necessary to align with RGP. I judge this to be suitable from a Mechanical Engineering perspective for the purposes of GDA.

5.1.5 Adequacy of Examination, Inspection, Maintenance and Testing Arrangements

1009. The RP has adequately resolved the following RO from a Mechanical Engineering perspective:

- RO-UKHPR1000-0021 raised by Fault Studies concerning demonstration of the adequacy of EIMT for items importance to safety.

1010. During my assessment I raised two Assessment Findings.

1011. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1012. The RP has addressed my concerns raised within RO-UKHPR1000-0021. It has shown that it understands the EIMT requirements placed on SSCs. It has also improved its understanding and application of HSG253 to achieve safe isolations within the generic design. I judge this to be suitable from a Mechanical Engineering perspective for the purposes of GDA.

5.1.6 Adequacy and Application of Design Assurance Arrangements

1013. I am satisfied that the RP's design assurance arrangements are suitable.

1014. I raised no Assessment Findings during my assessment.

1015. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1016. I judge that the RP's design assurance arrangements are suitable and sufficient for the purposes of GDA.

5.1.7 Application of the ALARP Principle when Considering Design Changes

1017. The RP has closed the following RO from a Mechanical Engineering perspective, which is also relevant to this Theme:

- RO-UKHPR1000-0012 concerning the identification and application of RGP applicable to Mechanical Engineering for the UK HPR1000 design.

1018. I raised one Assessment Finding during my assessment.

1019. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1020. The RP has addressed my concerns raised within RO-UKHPR1000-0012. It has implemented design modifications that align with the ALARP principle. I judge this to be adequate from a Mechanical Engineering perspective for the purposes of GDA.

5.1.8 Approach to Reducing the Hazards from Fibrous Material within the UK HPR1000 Loss of Coolant Accident Zone of Influence

1021. The RP has closed the following RO from a Mechanical Engineering perspective:

- RO-UKHPR1000-0027 concerning its consideration of gaps against the debris effects on Safety Injection System and Containment Heat Removal System performance, which was led by Fault Studies.

1022. I raised no Assessment Findings during my assessment.

1023. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1024. The RP has addressed my concerns relating to its choice of insulation material within containment. The RP has changed the insulation type from fibrous material to reflective metallic insulation. I judge this to be adequate from a Mechanical Engineering perspective for the purposes of GDA.

5.1.9 Approach to Demonstrating Nuclear Lifts Reduce Risks ALARP

1025. No ROs were raised in this Theme.

1026. I raised no Assessment Findings during my assessment.

1027. I am satisfied that the RP has identified a suitable lifting path for the RPV Head, that it has implemented appropriate RGP in this area and that risks are reduced ALARP.

1028. I am also content that the risk associated with lifting the RPV Head above the reactor pressure vessel can be reduced to an acceptable level as part of normal business during detailed design and site-specific stages. I judge this to be adequate from a Mechanical Engineering perspective for the purposes of GDA.

5.1.10 Lifting Operations within the Fuel Building

1029. The RP has closed the following RO from a Mechanical Engineering perspective:

- RO-UKHPR1000-0014 concerning nuclear lifting and handling operations in the Spent Fuel Building

1030. During my assessment I raised one Assessment Finding.

1031. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1032. I judge, for the purpose of GDA, the RP has suitably shown that its generic design reduces risk to workers and the public ALARP.

5.1.11 Fuel Route Safety Case

1033. The RP has closed the following RO from a Mechanical Engineering perspective:

- RO-UKHPR1000-0056 concerning the adequacy of the Fuel Route safety case.

1034. During my assessment I have raised three Assessment Findings.

1035. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1036. I judge the RP's Spent Fuel Pool Crane concept design shows improvement in the safety of workers. It also shows that the Mechanical Engineering related SSCs can be adequately designed to reduce risk ALARP during detailed design and site-specific stages.

5.1.12 Safety Case Consolidation

1037. No ROs were raised in this area.

1038. I raised no Assessment Findings during my assessment.

1039. Overall, for the purpose of GDA, I conclude that the RP's submissions sufficiently align with relevant SAPs, TAGs and RGP.

1040. I conclude that the RP has undertaken an appropriate consolidation of its work during Step 4 of GDA and its safety case documentation aligns with Design Reference 3.0.

5.1.13 Summary

1041. No GDA Issues were raised with respect to Mechanical Engineering. All Mechanical Engineering related ROs have been closed. Responses have been provided to all RQs raised during my Mechanical Engineering assessment.

1042. Overall, based on my sample assessment of the safety case for the generic UK HPR1000 design, I am satisfied that the case presented within the PCSR and supporting documentation is adequate.

1043. On this basis, I am content that a DAC should be granted from a Mechanical Engineering perspective.

1044. **Table 10** presents a summary of my conclusions.

Table 10: Mechanical Engineering assessment theme conclusions

Assessment Theme	Related ROs	Assessment Findings	Minor Shortfalls	Adequate for GDA
1. Adequacy of the UK HPR1000 HVAC design substantiation	RO-UKHPR1000-0039 Closed	1	1	Yes
2. Adequacy of the ME schedule	-	4	6	Yes
3. Adequacy of equipment qualification arrangements	RO-UKHPR1000-0048 Closed	4	3	Yes
4. Closure of gaps against RGP	RO-UKHPR1000-0012 Closed	0	2	Yes

Assessment Theme	Related ROs	Assessment Findings	Minor Shortfalls	Adequate for GDA
5. Adequacy of examination, inspection, maintenance and testing (EIMT) arrangements	RO-UKHPR1000-0021 Closed	2	1	Yes
6. Adequacy and application of the design assurance arrangements	-	0	0	Yes
7. Application of the ALARP principle when considering design changes	RO-UKHPR1000-0012 Closed	1	1	Yes
8. Approach to reducing the hazards from fibrous material within the UK HPR1000 loss of coolant accident zone of influence	RO-UKHPR1000-0027 Closed	0	0	Yes
9. Approach to demonstrating nuclear lifts reduce risks ALARP	-	0	0	Yes
10. Lifting Operations within the Fuel Building	RO-UKHPR1000-0014 Closed	1	0	Yes
11. Fuel Route Safety Case	RO-UKHPR1000-0056 Closed	3	2	Yes
12. Safety Case Consolidation	-	0	1	Yes
TOTALS		**16**	**17**	

5.2 Recommendations

1045. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1:** From a mechanical engineering perspective, ONR should grant a DAC for the generic UK HPR1000 design.
- **Recommendation 2:** The 16 Assessment Findings identified in this report should be resolved by the future licensee for a site-specific application of the generic UK HPR1000 design

6 REFERENCES

1. *New Nuclear Reactors: Generic Design Assessment, Guidance to Requesting Parties for the UK HPR1000,* ONR-GDA-GD-001, Revision 4, October 2019, Office for Nuclear Regulation. www.onr.org.uk

2. *Safety Assessment Principles for Nuclear Facilities.,* 2014 Edition Revision 1, January 2020, Office for Nuclear Regulation. www.onr.org.uk

3. *UK HPR1000 Pre-Construction Safety Report,* Revision B, March 2018, General Nculear System Ltd. [CM9 Ref. 2018/127683]

4. *Operational Inspection, Technical Inspection Guides,* , Office for Nuclear Regulation. www.onr.org.uk

5. *GDA Step 4 Assessment Plan of Mechanical Engineering Topic for the UK HPR1000 Reactor,* ONR-GDA-UKHPR1000-AP-10-012, Revision 0, February 2020, Office for Nuclear Regulation. [CM9 Ref. 2020/27133]

6. *UK HPR1000 - Mechanical Engineering Assessment Reference Document 2 - Regulatory Queries,* 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/23659]

7. *UK HPR1000 - Mechanical Engineering Assessment Reference Document 1 – Regulatory Observations and Contact Records,* 2021, Office for Nuclear Regulation. [CM9 Ref. 2020/291798]

8. *New Nuclear Power Plants: Generic Design Assessment Technical Guidance,* ONR-GDA-GD-007, Revision 0, May 2019, Office for Nuclear Regulation. www.onr.org.uk

9. *IAEA Safety Standards, Safety Classification of Structures, Systems and Components in Nuclear Power Plants. Specific Safety Guide.,* SSG-30, 2014, International Atomic Energy Agency. www.iaea.org

10. *IAEA Safety Standards, Design of Fuel Handling and Storage Systems for Nuclear Power Plants. Specific Safety Guide.,* SSG-63, 2020, International Atomic Energy Agency. www.iaea.org

11. *IAEA Safety Standards, Safety of Nuclear Power Plants: Design,* Specific Safety Requirements No. SSR-2/1, Revision 1, February 2016, International Atomic Energy Agency. www.iaea.org

12. *Document List and Master Document Submission List Arrangements,* HPR-GDA-PROC-0006, Revision 002, May 2019, General Nuclear System Ltd. [CM9 Ref. 2019/366792]

13. *UK HPR1000 Pre-Construction Safety Report Chapter 1 - Introduction,* HPR/GDA/PCSR/0001, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. Rev 000: 2017/401345 Rev 001: 2020/13610]

14. *UK HPR1000 Pre-Construction Safety Report Chapter 6 - Reactor Coolant System,* HRP/GDA/PCSR/0006, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. CM9 Ref. 2020/13625]

15. *UK HPR1000 Pre-Construction Safety Report Chapter 7 - Safety System,* HPR/GDA/PCSR/0007, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. 2020/13658]

16. *UK HPR1000 Pre-Construction Safety Report Chapter 10 - Auxiliary Systems,* HPR/GDA/PCSR/0010, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. CM9 Ref. 2020/13656]

17. *UK HPR1000 Pre-Construction Safety Report Chapter 11 - Steam and Power Conversion System,* HPR/GDA/PCSR/0011, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. CM9 Ref. 2020/13931]

18. *UK HPR1000 Pre-Construction Safety Report Chapter 23 - Radioactive Waste Management,* HPR/GDA/PCSR/0023, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. CM9 Ref. 2020/13969]

19. *UK HPR1000 Pre-Construction Safety Report Chapter 28 - Fuel Route and Storage,* HPR/GDA/PCSR/0028, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. CM9 Ref. 2020/13982]

20. *UK HPR1000 Pre-Construction Safety Report Chapter 33 - ALARP Evaluation,* HPR/GDA/PCSR/0033, Revision 001, January 2020, General Nuclear System Ltd. [CM9 Ref. 2020/14002]

21. *New Reactors Division - Generic Design Assessment, Summary of the Step 4 Assessment of the UK HPR1000 Reactor,* ONR-NR-PAR-21-001, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/37711]

22. *GDA Step 3 Assessment of Mechanical Engineering for the UK HPR1000 Reactor,* ONR-NR-AN-19-012, Revision 0, December 2019, Office for Nuclear Regulation. [CM9 Ref. 2019/340491]

23. *Identification and Management of GDA Issues, Assessment Findings and Minor Shortfalls for the GDA of UK HPR1000,* ONR-GEN-IN-021, Revision 0, May 2020, Office for Nuclear Regulation. www.onr.org.uk [CM9 Ref. 2019/218899]

24. *Ventilation Systems for Radiological Facilities, Design Guide,* EG_0_1738_1, Issue 1, December 2018, Sellafield Ltd. [CM9 Ref. 2019/138402]

25. *IAEA Safety Standards, Meteorological and Hydrological Hazards in Site Evaluation for Nuclear Installations. Specific Safety Guide,* SSG-18, 2011, International Atomic Energy Agency. www.iaea.org

26. *WENRA Safety Reference Levels for Existing Reactors 2020,* Issue K: Maintenance, In-Service Inspection and Functional Testing, February 2021, Western European Nuclear Regulators' Association. www.wenra.eu

27. *Nuclear Facilities – Criteria for the design and operation of ventilation systems for nuclear installations other than nuclear reactors,* ISO 17873:2004 , October 2004, International Organization for Standardization. www.bsigroup.com

28. *Nuclear Facilities. Criteria for the design and operation of containment and ventilation systems for nuclear reactors,* BS ISO 26802:2010, August 2010, International Organization for Standardization. www.bsigroup.com

29. *IAEA TECDOC SERIES, Treatment of Radioactive Gaseous Waste,* IAEA-TECDOC-1744, July 2014, International Atomic Energy Agency. www.iaea.org

30. *The Safety of the Nuclear Fuel Cycle,* Third Edition, 2005, OECD Nuclear Energy Agency. www.oedc-nea.org

31. *The Building Regulations 2010,* Statutory Instrument 2010 No. 2214, October 2010, Crown Copyright. www.legislation.gov.uk

32. *The Dangerous Substances and Explosive Atmospheres Regulations 2002 (DSEAR),* Statutory Instrument 2002 No. 2776, December 2002, Crown Copyright. www.legislation.gov.uk

33. *Regulatory Observation Resolution Plan - RO-UKHPR1000-0039 Performance Analysis of UK HPR1000 Heating, Ventilation and Air Conditioning Systems,* GDA-REC-GNSL-006684, Revision 0, July 2020, General Nuclear System Ltd. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2020/207868]

34. *Analysis Report of the HVAC Sample Systems,* GHX08000010DCNT03TR, Revision A to C, May 2021, CGN. [CM9 Ref. A: 2021/247 B: 2021/27294 C: 2021/43093]

35. *UK HPR1000 - Step 4 Electrical Engineering Assessment Report,* ONR-NR-AR-21-011, Revision 0, December 2021, Office for Nuclear Regulation. www.onr.gov.uk [CM9 Ref. 2021/51507]

36. *Design Guide for Filters and Filter Installations in Ventilation Systems,* EG_1_1702_1, Issue 1, December 2016, Sellafield Ltd. [CM9 Ref. 2021/54616]

37. *Assessment of the Response to RO-UKHPR1000-0036 - HEPA Filter Type,* ONR-NR-AN-21-018, Revision 0, May 2021, Office for Nuclear Regulation and Environment Agency. www.onr.org.uk [CM9 Ref. 2021/40388]

38. *Optioneering Report of the HEPA Filters Types,* GHX08000003DCNT03TR, Revision A to E, June 2021, CGN. [CM9 Ref. A: 2019/230162 C: 2020/198932 D: 2021/8873 E: 2021/50557]

39. *Post-GDA Commitment List,* GHX00100084KPGB03GN, Revision C, August 2021, CGN. [CM9 Ref. 2021/65125]

40. *DVL Electrical Divison of Safeguard Building Ventilation System, Design Manual Chapter 3, System Functions and Design Bases,* GHX17DVL003DCNT45GN, Revision E, December 2020, CGN. [CM9 Ref. 2021/310]

41. *UK HPR1000 - Step 4 Human Factors Assessment Report,* ONR-NR-AR-21-013, Revision 0, December 2021, Office for Nuclear Regulation. www.onr.org.uk [CM9 Ref. 2021/54151]

42. *Turbine Missiles Safety Assessment Report,* GHX84200032DOZJ03GN, Revision B, January 2021, CGN. [CM9 Ref. 2021/8889]

43. *UK HPR1000 - Step 4 Internal Hazards Assessment Report,* ONR-NR-AR-21-012, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/55302]

44. *Assessment of the Response to RO-UKHPR1000-0039 - Performance Analysis of UK HPR1000 Heating Ventilation and Air Conditioning Systems,* ONR-NR-AN-21-030, Revision 0, July 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/49521]

45. *The Management of Health and Safety at Work Regulations 1999,* Statutory Instrument 1999 No. 3242, December 1999, Crown Copyright. www.legislation.gov.uk

46. *IAEA TECDOC SERIES, Application of the Safety Classification of Structures, Systems and Components in Nuclear Power Plants,* IAEA-TECDOC-1787, April 2016, International Atomic Energy Agency. www.iaea.org

47. *Methodology of Safety Categorisation and Classification,* GHX00100062DOZJ03GN, Revision B, June 2018, CGN. [CM9 Ref. 2018/199731]

48. *Regulatory Observation Resolution Plan - RO-UKHPR1000-0004 - Development of a Suitable and Sufficient Safety Case,* GDA/REC/GNS/000786, Revision 0, December 2018, Office for Nuclear Regulation. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2018/396670]

49. *UK HPR1000 - Step 4 Assessment of Cross-cutting Topics for the UK HPR1000 Reactor,* ONR-NR-AR-21-007, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/47905]

50. *Extant Duty Schedule of RIS [SIS], ASG [EFWS] and DCL [MCRACS],* GHX11000003DOZJ45GN, Revision B, June 2021, CGN. [CM9 Ref. 2021/44502]

51. *Engineering Schedule for Mechanical Engineering,* GHX00100027DNHX03GN, Revision F, May 2021, CGN. [CM9 Ref. 2021/43585]

52. *Requirement Management Summary Report,* GHX00100127DOZJ03GN, Revision A, May 2020, CGN. [CM9 Ref. 2020/130900]

53. *UK HPR1000 Generic Design Assessment - Level 4 Mechanical Engineering - Traceability of performance requirements,* ONR-NR-CR-21-064, Revision 0, June 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/46461]

54. *The Ionising Radiations Regulations 2017,* Statutory Instrument 2017 No. 1075, November 2017, Crown Copyright. www.legislation.gov.uk

55. *RCP-Reactor Coolant System, Design Manual Chapter 3, System Functions and Design Bases,* GHX17RCP003DNHX45GN, Revision C, July 2021, CGN. [CM9 Ref. B: 2019/372785 C: 2021/53506]

56. *Reactor Coolant Pump Equipment Specification,* GHX44400001DNHX44DS, Revision F, July 2021, CGN. [CM9 Ref. 2021/52391]

57. *RCP-Reactor Coolant System, Design Manual Chapter 6, System Operation and Maintenance,* GHX17RCP006DNHX45GN, Revision D, December 2019, CGN. [CM9 Ref. 2019/373164]

58. *Classification of the Typical Cranes,* GHX45600013DPZS45GN, Revision E, May 2021, CGN. [CM9 Ref. D: 2021/8446 E: 2021/43567]

59. *On-site Radiological Consequence Evaluation for Fuel Route PIE,* GHX00530035DNFP02GN, Revision B, January 2021, CGN. [CM9 Ref. 2021/2105]

60. *Summary of Fuel Route Safety Case in BFX,* GHX30000001DNBZ00GN, Revision B, May 2021, CGN. [CM9 Ref. 2021/43562]

61. *ASG-Emergency Feedwater System, Design Manual Chapter 9 Flow Diagrams,* GHX17ASG009DNHX45GN, Revision C, September 2021, CGN. [CM9 Ref. 2021/67015]

62. *ASG-Emergency Feedwater System, Design Manual Chapter 4, System and Component Design,* GH X 17ASG 004 DNHX 45 GN, Revision A, October 2018, CGN. [CM9 Ref. 2018/318440]

63. *ASP-Secondary Passive Heat Removal System, Design Manual Chapter 4, System and Component Design,* GH X 17ASP 004 DNHX 45 GN, Revision A, October 2018, CGN. [CM9 Ref. 2018/318489]

64. *ASG-Emergency Feedwater System, Design Manual Chapter 6, System Operation and Maintenance,* GH X 17ASG 006 DNHX 45 GN, Revision B, October 2018, CGN. [CM9 Ref. 2018/318437]

65. *Requisition and List for Nuclear Isolation Valves,* GHX40000014DNHX44GN, Revision A, June 2020, CGN. [CM9 Ref. 2020/196000]

66. *Equipment Specification for Secondary Passive Heat Removal System Heat Exchanger,* GHX44400002DPZS44DS, Revision A, January 2020, CGN. [CM9 Ref. 2020/22050]

67. *EHR-Containment Heat Removal System, Design Manual Chapter 4, System and Component Design,* GH X 17EHR 004 DNHX 45 GN, Revision A, October 2018, CGN. [CM9 Ref. 2018/318482]

68. *EHR-Containment Heat Removal System Design Manual Chapter 9 Flow Diagrams,* GH X 17EHR 009 DNHX 45 GN, Revision B, October 2018, CGN. [CM9 Ref. 2018/318479]

69. *EHR-Containment Heat Removal System, Design Manual Chapter 6, System Operation and Maintenance,* GHX17EHR006DNHX45GN, Revision D, July 2021, CGN. [CM9 Ref. 2021/53522]

70. *UK HPR1000 - Step 4 Fault Studies Assessment Report,* ONR-NR-AR-21-014, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/44803]

71. *EPP-Containment Leak Rate Testing and Monitoring System Design Manual Chapter 4 System and Component Design,* GH X 17EPP 004 DNHX 45 GN, Revision C, December 2019, CGN. [CM9 Ref. A: 2018/318431 C: 2019/372789]

72. *Equipment Specification for Equipment Access Hatch,* GHX29100001DPZS44DS, Revision D, January 2021, CGN. [CM9 Ref. B: 2020/22065 C: 2020/286865 D: 2021/2060]

73. *DCL Main Control Room Air Conditioning System, Design Manual Chapter 3, System Functions and Design Basis,* GH X 17DCL 004 DCNT 45 GN, Revision B, October 2018, CGN. [CM9 Ref. 2018/317402]

74. *Confinement Schedule,* GHX00600379DRAF02GN, Revision A, November 2020, CGN. [CM9 Ref. 2020/309769]

75. *American National Standard for Rotodynamic Pumps - Guideling for NPSH Margin,* ANSI/HI 9.6.1-2017, January 2017, American National Standards Institute. webstore.ansi.org

76. *RCP-Reactor Coolant System, Design Manual Chapter 4, System and Component Design,* GHX17RCP004DNHX45GN, Revision C, December 2019, CGN. [CM9 Ref. 2019/372789]

77. *RPE-Nuclear Island Vent and Drain System, Design Manual Chapter 4, System and Component Design,* GHX17RPE004DNFF45GN, Revision F, October 2020, CGN. [CM9 Ref. 2020/305425]

78. *Gate Valve Specification for Nuclear Island,* GHX40000013DNHX44DS, Revision B, September 2020, CGN. [CM9 Ref. 2020/271000]

79. *Design and Construction Rules for Mechanical Components of PWR Nuclear Islands,* RCC-M 2007, 2007, AFCEN. www.afcen.com

80. *Equipment Qualification Methodology,* GHX80000003DOZJ03GN, Revision C, May 2021, CGN. [CM9 Ref. A: 2019/156180 B: 2020/315892 C: 2021/43099]

81. *Equipment Qualification for Mechanical Engineering Based Structures, Systems and Components,* RO-UKHPR1000-0048, Revision 0, October 2020, General Nuclear System Ltd. www.onr.org.uk [CM9 Ref. 2020/292120]

82. *Technical Specification for Control Rod Drive Mechanism,* GHX44600004DPFJ44DS, Revision D, April 2021, CGN. [CM9 Ref. A: 2020/21850 D: 2021/35897]

83. *RIS-Safety Injection System, Design Manual Chapter 4, System and Component Design,* GHX17RIS004DNHX45GN, Revision F, July 2021, CGN. [CM9 Ref. B: 2019/318842 F: 2021/52389]

84. *Technical Specification for Medium Head Safety Injection Pumps,* GHX45200006DNHX44DS, Revision E, July 2021, CGN. [CM9 Ref. C: 2020/322980 D: 2021/43602 E: 2021/52221]

85. *Technical Specification for EHR Spray Pumps,* GHX45200003DNHX44DS, Revision A, June 2020, CGN. [CM9 Ref. 2020/195950]

86. *Technical Specification of Essential Service Water Pumps,* GHX45200009DNHX44DS, Revision C, July 2021, CGN. [CM9 Ref. 2021/52377]

87. *Optioneering on VVP [MSS] related to the Loss of MSL Isolation induced by CCF under SGTR (one tube),* GHX00100070DNHX03GN, Revision B, August 2020, CGN. [CM9 Ref. 2020/233049]

88. *The Health and Safety at Work etc. Act 1974,* 1974, HM Stationary Office. www.legislation.gov.uk

89. *IAEA Safety Reports Series No. 3 - Equipment Qualification in Operational Power Plants: Upgrading, Preserving and Reviewing,* April 1998, International Atomic Energy Agency. www.iaea.org

90. *Qualification of Active Mechanical Equipment Used in Nuclear Facilities,* ASME QME-1, August 2017, The American Society of Mechanical Engineers (ASME). www.asme.org

91. *Plant Support Engineering: Equipment Qualification Reference Manual,* Revision 1, September 2010, Electrical Power Research Institute (EPRI). www.epri.com

92. *Equipment Qualification RGP Compliance Analysis Report,* GHX40300030DOZJ03GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/304237]

93. *Advanced Feedback on EQ Compliance Analysis,* Email, November 2020, Office for Nuclear Regulation. [CM9 Ref. 2021/51820]

94. *Environmental Requirements for Equipment Qualification,* GHX00100079DOZJ03GN, Revision B, January 2021, CGN. [CM9 Ref. 2021/7677]

95. *EQ Schedule for the 12 Samples Components of ME,* GHX00100100DNHX03GN, Revision C, April 2021, CGN. [CM9 Ref. A: 2020/315891 B: 2021/8891 C: 2021/37892]

96. *Test and Analysis Requirements for First-off Reactor Coolant Pump,* GHX45200013DNHX44DS, Revision B, January 2021, CGN. [CM9 Ref. 2021/7674]

97. *Email: UK HPR1000 - Mechanical Engineering Assessment Report - Clarification on the UK HPR1000 Reactor Coolant Pump (RCP) technical detail,* August 2021, General Nuclear System Ltd. [CM9 Ref. 2021/63118]

98. *Requisition and List for Dedicated PZR Gate Valves,* GH X 44801 013 DNHX 44 GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/303730]

99. *Requisition and List for Dedicated PZR Globe Valves,* GHX44801014DNHX44GN, Revision B, July 2021, CGN. [CM9 Ref. A: 2020/303731 B: 2021/52632]

100. *Equipment Classification List of Safety Injection System (RIS),* GHX99RIS001DNHX45GN, Revision A, October 2019, CGN. [CM9 Ref. 2019/318749]

101. *Technical Specification for the Emergency Diesel Generator,* GHX54100001DCCJ44DS, Revision C, May 2020, CGN. [CM9 Ref. 2020/159829]

102. *IAEA Safety Standards, Seismic Design and Qualification for Nuclear Power Plants,* Safety Guide No. NS-G-1.6, November 2013, International Atomic Energy Agency. www.iaea.org

103. *Generic Site Related Design Values,* GHX00100007DOZJ03GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/4287]

104. *Assessment of the Response to RO-UKHPR1000-0048 – Equipment Qualification for Mechanical Engineering Based Structures Systems and Components,* ONR-NR-AN-21-052, Revision 0, October 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/62076]

105. *Regulatory Observation Resolution Plan - RO-UKHPR1000-0012 Identification and Application of Relevant Good Practice Applicable to Mecahnical Engineering for the UK HPR1000,* GDA/REC/GNS/005250, Revision 0, November 2019, General Nuclear System Ltd. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2019/356762]

106. *UK HPR1000 Strategy for Analysis of RGP in Mechanical Engineering Design,* GHX00800009DNHX02GN, Revision B, March 2020, CGN. [CM9 Ref. A: 2020/266 B: 2020/92084]

107. *ALARP Demonstration for Reactor Coolant System,* GHX00100049KPGB03GN, Revision E, December 2020, CGN. [CM9 Ref. D: 2019/375582 E: 322675]

108. *ALARP Demonstration Report for Safety Systems,* GHX00100050KPGB03GN, Revision E, December 2020, CGN. [CM9 Ref. 2020/322688]

109. *ALARP Demonstration for Auxiliary Systems,* GHX00100053KPGB03GN, Revision G, July 2021, CGN. [CM9 Ref. B: 2018/316827 D: 2019/375598 E: 2020/322676 G:2021/52223]

110. *ALARP Demonstration Report for Steam and Power Conversion System,* GHX00100054KPGB03GN, Revision D, December 2020, CGN. [CM9 Ref. A: 2018/369035 B: 2019/181122 C: 2019/375550 D: 2020/322689]

111. *ALARP Demonstration Report for Radioactive Waste Management,* GHX00100072KPGB03GN, Revision H, May 2021, CGN. [CM9 Ref. C: 2019/281164 D: 2020/65755 E: 2020/130875 G: 2021/2807 H: 2021/39949]

112. *ALARP Demonstration Report of the PMC [FHSS] SSCs,* GHX00100065KPGB03GN, Revision E, December 2020, CGN. [CM9 Ref. 2020/314108]

113. *List of Gaps for Mechanical Engineering against RGP,* GHX00800013DNHX02GN, Revision C, July 2021, CGN. [CM9 Ref. B: 2020/322026 C: 2021/57050.]

114. *UKHPR1000 Optioneering Study for Identified Gaps of sample of HVAC Systems,* GHX08000011DCNT03TR, Revision B, March 2021, CGN. [CM9 Ref. 2021/27292]

115. *UKHPR1000 Optioneering Study for Identified Gaps of sample of Mechanical Systems,* GHX00800005DPZS02GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/309803]

116. *UKHPR1000 Optioneering Study for Identified Gaps of sample of Static SSCs,* GHX00800006DPZS02GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/304228]

117. *UKHPR1000 Optioneering Study for Identified Gaps of sample of Dynamic SSCs,* GHX00800014DNHX02GN, Revision A, October 2020, CGN. [CM9 Ref. 2020/304229]

118. *UKHPR1000 The List of SSCs Affected by the Optimal Options for sample of HVAC Systems,* GHX00800003DCNT02GN, Revision A, August 2020, CGN. [CM9 Ref. 2020/258852]

119. *UKHPR1000 The List of SSCs Affected by the Optimal Options for sample of Mechanical Systems,* GHX00800007DPZS02GN, Revision A, September 2020, CGN. [CM9 Ref. 2020/259799]

120. *UKHPR1000 The List of SSCs Affected by the Optimal Options for sample of Static SSCs,* GHX00800008DPZS02GN, Revision A, November 2020, CGN. [CM9 Ref. 2020/314111]

121. *UKHPR1000 The List of SSCs Affected by the Optimal Options for sample of Dynamic SSCs,* GHX00800007DPZS02GN, Revision A, November 2020, CGN. [CM9 Ref. 2020/315897]

122. *UKHPR1000 Compliance Analysis of RGP for sample of HVAC systems,* GHX00800001DCNT02GN, Revision A, June 2020, CGN. [CM9 Ref. 2020/163972]

123. *UKHPR1000 Compliance Analysis of RGP for sample of Mechanical Systems,* GHX00800002DPZS02GN, Revision C, October 2020, CGN. [CM9 Ref. 2020/305460]

124. *UKHPR1000 Compliance Analysis of RGP for sample of Static SSCs,* GHX00800001DPZS02GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/308592]

125. *UKHPR1000 Compliance Analysis of RGP for sample of Dynamic SSCs,* GHX00800008DNHX02GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/308593]

126. *The Safe Isolation of Plant and Equipment,* HSG 253, Second Edition, 2006, Health and Safety Executive. www.hse.gov.uk

127. *Nuclear Power Plant Operating Experience from the IAEA/NEA International Reporting System for Operating Experience 2005–2008,* June 2010, IAEA. www.iaea.org/publications

128. *Step 4 Mechanical Engineering Assessment of the Westinghouse AP1000® Reactor,* ONR-GDA-AR-11-010, Revision 0, November 2011, Office for Nuclear Regulation. www.onr.org.uk [CM9 Ref. 2011/620762]

129. *Technical Specification for IRWST Sump Strainers,* GHX45800001DPZS44DS, Revision C, July 2021, CGN. [CM9 Ref. A: 2020/131042 C: 2021/52623]

130. *RRI Component Cooling Water System, Design Manual Chapter 3, System Functions and Design Basis,* GHX17RRI003DNHX45GN, Revision C, December 2019, CGN. [CM9 Ref. 2019/373268]

131. *Advanced Light Water Reactor Utility Requirements Document, Volume II: Evolutionary Plant Requirements,* Revision 8, March 1999, Electric Power Research Institute (EPRI). www.epri.com

132. *European Utility Requirements for LWR Nuclear Power Plants, Volume 2 Chapter 6 Material-Related Requirements,* Revision E, December 2016, European Utility Requirements Organisation. www.europeanutilityrequirements.eu

133. *TEU-Liquid Waste Treatment System, Design Manual Chapter 3, System Functions and Design Bases,* GH917TEU003DNFF45GN, Revision D, November 2019, CGN. [CM9 Ref. 2019/359926]

134. *Control of diesel engine exhaust emmissions in the workplace,* HSG187, Third Edition, 2012, Health and Safety Executive. www.hse.gov.uk

135. *HVAC Systems Analysis Report - Site Adaptability Modification in UK HPR1000,* GHX08000001DCNT03TR, Revision D, March 2021, CGN. [CM9 Ref. C: 2020/99441 D: 2021/27278]

136. *Assessment of the Response to RO-UKHPR1000-0012 – Identification and Application of Relevant Good Practice Applicable to Mechanical Engineering for the UK HPR1000 Design,* ONR-NR-AN-21-038, Revision 4, August 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/54489]

137. *Regulatory Observation Resolution Plan - RO-UKHPR1000-0021 - Demonstration of the Adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of Structures, systems and Components Important to Safety,* GDA/REC/GNS/005378, Revision 0, November 2019, Office for Nuclear Regulation. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2019/347544]

138. *Examination, Maintenance, Inspection and Testing (EMIT) Strategy,* GHX42EMT001DOYX45GN, Revision D, March 2021, CGN. [CM9 Ref. 2021/28205]

139. *Examination, Maintenance, Inspection and Testing (EMIT) Windows,* GHX42EMT002DOYX45GN, Revision D, January 2021, CGN. [CM9 Ref. 2021/8441]

140. *EIMT Windows for Mechanical Engineering Sample Systems,* July 2021, CGN. [CM9 Ref. 2021/52820]

141. *EMIT Consistency Analysis,* GHX42EMT004DOYX45GN, Revision A, September 2020, CGN. [CM9 Ref. 2020/289528]

142. *HSG253 Compliance Analysis - RIS,* GHX00100094DNHX03GN, Revision C, June 2021, CGN. [CM9 Ref. A: 2020/278875 B: 2021/8890 C: 2021/51077]

143. *Assessment of the Response to RO-UKHPR1000-0021 - Demonstration of the Adequacy of Examination, Maintenance, Inspection and Testing (EMIT) of Structures, Systems and Components Important to Safety,* ONR-NR-AN-21-004, Revision 0, May 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/41436]

144. *GDA Step 4 - Review of Unmitigated Dose Assessment to Support HSG253 Compliance for the UK HPR100,* ONR-NR-AN-010, Revision 0, June 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/39201]

145. *HSG253 Compliance Analysis - TEU,* GHX00100110DNFF03GN, Revision C, January 2021, CGN. [CM9 Ref. B: 2020/278866 C: 2021/2062]

146. *HSG253 Compliance Analysis - ASG,* GHX00100082DNHX03GN, Revision B, January 2021, CGN. [CM9 Ref. A: 2020/278869 B: 2021/2061]

147. *HSG253 Compliance Analysis - VVP,* GHX00100098DNHX03GN, Revision B, December 2020, CGN. [CM9 Ref. A: 2020/278884 B: 2021/243]

148. *UK HPR1000 GDA – Step 4 Modifications Log,* CM9 Revision 63, December 2021, Office for Nuclear Regulation. [CM9 Ref. 2020/313979]

149. *In-service Inspection, Installation and Maintenance Rules for Mechanical Components of PWR,* 2018 Edition, December 2018, AFCEN. www.afcen.com

150. *Standards of the Tubular Exchanger Manufacturers Association,* Ninth Edition, November 2007, Tubular Exchanger Manufacturers Association. kbcdco.tema.org

151. *TEU - Liquid Waste Treatment System, Design Manual Chapter 6, System Operation and Maintenance,* GH917TEU006DNFF45GN, Revision D, November 2020, CGN. [CM9 Ref. C: 2019/359849 D: 2020/315811]

152. *The Lifting Operations and Lifting Equipment Regulations 1998 (LOLER),* Statutory Instrument 1998 No. 2307, December 1998, Crown Copyright. www.legislation.gov.uk

153. *Safe use of lifting equipment. Lifting Operations and Lifting Equipment Regulations 1998. Approved Code of Practice and guidance,* L113, Second Edition, December 2014, HSE Books. www.hse.gov.uk

154. *The Provision and Use of Work Equipment Regulations 1998 (PUWER),* Statutory Instrument 1998 No. 2306, December 1998, Crown Copyright. www.legislation.gov.uk

155. *Safe use of work equipment. Provision and Use of Work Equipment Regulations 1998. Approved Code of Practice and guidance,* L22, Fourth Edition, 2014, HSE Books. www.hse.gov.uk

156. *EMIT Requirements for the Polar Crane,* GHX45600014DPZS45GN, Revision B, October 2020, CGN. [CM9 Ref. 2020/304226]

157. *Design and Development control procedure,* PJ-30E-001, Revision H, February 2018, CGN. [CM9 Ref. 2018/109531]

158. *ALARP Methodology,* GHX00100051DOZJ03GN, Revision D, May 2020, CGN. [CM9 Ref. 2020/139106]

159. *General Principles for Application of Laws, Regulations, Codes and Standards,* GHX00100018DOZJ03GN, Revision G, March 2020, CGN. [CM9 Ref. 2020/73817]

160. *Suitability Analysis of RGP for sample of HVAC systems,* GHX00800005DCNT02GN, Revision B, April 2020, CGN. [CM9 Ref. 2020/116967]

161. *Suitability Analysis of RGP for sample of Mechanical Systems,* GHX0080000DPZS02GN, Revision B, April 2020, CGN. [CM9 Ref. 2020/116983]

162. *Suitability Analysis of RGP for sample of Static SSC's,* GHX00800004DPXZS02GN, Revision B, June 2020, CGN. [CM9 Ref. 2020/163981]

163. *Suitability Analysis of RGP for sample of Dynamic SSC's,* GHX008000010DNHX02GN, Revision B, June 2020, CGN. [CM9 Ref. 2020/163987]

164. *Compliance Analysis of RGP for sample of HVAC systems,* GHX00800001DCNT02GN, Revision A, June 2020, CGN. [CM9 Ref. 2020/163972]

165. *Compliance Analysis of RGP for sample of Mechanical Systems,* GHX00800002DPZS02GN, Revision C, October 2020, CGN. [CM9 Ref. 2020/305460]

166. *Compliance Analysis of RGP for sample of Static SSC's,* GHX00800001DPZS02GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/308592]

167. *Compliance Analysis of RGP for sample of Dynamic SSC's,* GHX00800008DNHX02GN, Revision B, November 2020, CGN. [CM9 Ref. 2020/308593]

168. *ALARP Assessment of the Spent Fuel Delivery Process,* GHX00100012DPFJ45GN, Revision B, December 2020, CGN. [CM9 Ref. 2020/319242]

169. *LHSI pump seal cooling heat exchanger modification introduction,* March 2021, CGN. [CM9 Ref. 2021/71674]

170. *Assessment of Reflective Metal Insulation (RMI) Replacements and Fibre Removal,* ONR-NR-AN-20-016, Revision 0, September 2020, Office for Nuclear Regulation. [CM9 Ref. 2020/262700]

171. *Resolution of Generic Safety Issues, Section 3 New Generic Issues. Issue 191: Assessment of Debris Accumulation on PWR Sump Performance,* NUREG-0933, Revision 2, December 2011, US Nuclear Regulatory Commission. www.nrc.gov/sr0933/Section%203.%20New%20Generic%20Issues/191r2.html#

172. *Regulatory Observation Resolution Plan - RO-UKHPR1000-0027 Debris effects on Safety Injection System and Containment Heat Removal System performance,* GDA-REC-GNSL-005959, Revision 0, March 2020, General Nuclear System Ltd. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2020/101966]

173. *Assessment of the Response to RO-UKHPR1000-0027 – Debris effects on Safety Injection System and Containment Heat Removal System performance,* ONR-NR-AN-20-029, Revision 0, March 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/22936]

174. *The Investigation Report on the Debris Effect,* GHX22400001DNHX00TR, Revision A, May 2020, CGN. [CM9 Ref. 2020/130999]

175. *RPV Head Drop Analysis Report,* GHX00100012DPLX44GN, Revision C, January 2020, CGN. [CM9 Ref. 2020/64816]

176. *Lifting Schedule of Reactor Pressure Vessel Head Assembly,* GHX44100002DPFJ44DS, Revision C, July 2020, CGN. [CM9 Ref. 2019/225816]

177. *Fuel Handling and Storage System Design Manual Chapter 9 Flow Diagrams,* GH/X/17PMC/009/DPFJ/45/GN, Revision A, Undated, CGN. [CM9 Ref. 2018/316124]

178. *Technical Specification for Spent Fuel Pool Crane,* GH/X/45600/007/DPFJ/44/DS, Revision A, July 2018, CGN. [CM9 Ref. 2019/91957]

179. *Technical Specification for Auxiliary Crane,* GH/X/45600/008/DPFJ/44/DS, Revision A, 2018 July, CGN. [CM9 Ref. 2019/91956]

180. *Technical Specification for New Fuel Elevator,* GH/X/45600/010/DPFJ/44/DS, Revision A, August 2018, CGN. [CM9 Ref. 2019/91957]

181. *General Layout Drawing (Top View) for Fuel Handling and Storage System,* GHX45600004DNSB44DD, Revision A, 2018 June, CGN. [CM9 Ref. 2019/25985]

182. *General Layout Drawing (Front View) for Fuel Handling and Storage System,* GHX45600005DNSB44DD, Revision A, June 2018, CGN. [CM9 Ref. 2019/25969]

183. *General Layout Drawing (A-A Section) for Fuel Handling and Storage System,* GHX45600006DNSB44DD, Revision B, June 2018, CGN. [CM9 Ref. 2019/25978]

184. *General Layout Drawing (B-B Section) for Fuel Handling and Storage System,* GHX45600007DNSB44DD, Revision B, June 2018, CGN. [CM9 Ref. 2019/25985]

185. *General Layout Drawing (C-C Section) for Fuel Handling and Storage System,* GHX45600008DNSB44DD, Revision B, June 2018, CGN. [CM9 Ref. 2019/25998]

186. *Regulatory Observation Resolution Plan – RO-UKHPR1000-0014 Spent Fuel Building – Design of Nuclear Lifting Operations to Demonstrate Relevant Risks are Reduced to ALARP,* GDA/REC/GNS/005251, Revision 0, November 2019, General Nuclear Service Ltd. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2019/339040]

187. *Fuel Handling Process and Operations,* GHX00100008DPFJ45GN, Revision A to D, January 2021, CGN. [CM9 Ref. A: 2020/10863 B: 2020/99304 C: 2020/200802 D: 2021/2103]

188. *Hazards Identification and Consequence Assessment of Fuel Handling Operations,* GHX00100009DPFJ45GN, Revision B to D, November 2020, CGN. [CM9 Ref. B: 2020/163923 C: 2020/286965 D: 2020/315907]

189. *UK HPR1000 Generic Design Assessment - Mechanical Engineering Level 4 Workshop in China,* ONR-NR-CR-19-474, Revision 0, January 2020, Office for Nuclear Regulation. [CM9 Ref. 2020/31964]

190. *UK HPR1000 GDA Scope for Spent Fuel Interim Storage (SFIS),* REG-GNS-0031N, October 2018, Office for Nuclear Regulation and Environment Agency. [CM9 Ref. 2018/329187]

191. *Email: UK HPR1000 - ONR Comments - Hazards Identification and Consequence Assessment of Fuel Handling Operations - GHC00100008DPFJ45GN (CM9 2020/163923),* June 2020, Office for Nuclear Regulation. [CM9 Ref. 2020/189304]

192. *BFX Conventional Health and Safety Design Risk Register,* GHX00100005DNBZ03GN, Revision E, May 2021, CGN. [CM9 Ref. 2021/41240]

193. *Hazard and operability studies (HAZOP studies) – Application guide,* BS EN 61882:2016, 2016, BSI Standards Publication. https://www.bsol.bsigroup.com [CM9 Ref. ISBN 978 0 580 87354 6]

194. *Regulatory Observation Resolution Plan – RO-UKHPR1000-0056 – Fuel Route Safety Case,* GDA-REC-GNSL-008099, Revision 0, December 2020, General Nuclear System Ltd. www.onr.org.uk/new-reactors/uk-hpr1000/ro-res-plan.htm [CM9 Ref. 2020/320723]

195. *UK HPR1000 Level 4 Fuel Route Meeting Information,* September 2020, CGN. [CM9 Ref. 2020/285651]

196. *ALARP Assessment of the BFX Cranes Arrangements,* GHX00100011DPFJ45GN, Revision B, January 2021, CGN. [CM9 Ref. 2021/5994]

197. *Safety Assessment Report for the PMC [FHSS] Related Operations,* GHX00100001DPFJ45GN, Revision C, November 2020, CGN. [CM9 Ref. 2020/315312]

198. *Radiological Consequence Analysis of Dropping of Spent Fuel Cask,* GHX00600384DRAF02GN, Revision A, January 2021, CGN. [CM9 Ref. 2021/8454]

199. *Assessment of the Response to RO-UKHPR1000-0014 – Spent Fuel Building – Design of Nuclear Lifting Operations to Demonstrate Relevant Risks are Reduced to ALARP,* ONR-NR-AN-21-001, Revision 0, April 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/30122]

200. *UK HPR1000 - Step 4 PSA Assessment Report,* ONR-NR-AR-21-020, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/49362]

201. *UK HPR1000 - Step 4 Fuel and Core Assessment Report,* ONR-NR-AR-21-021, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/23724]

202. *Optioneering Report for Spent Fuel Pool Crane,* GHX00100010DPFJ45GN, Revision B, May 2021, CGN. [CM9 Ref. 2021/43557]

203. *Technical Specification for Spent Fuel Pool Crane,* GHX45600007DPFJ44DS, Revision D, May 2021, CGN. [CM9 Ref. 2021/43565]

204. *Impact Analysis Report of the Fuel Building Modification,* GHX30000001DPFJ00GN, Revision A, May 2021, CGN. [CM9 Ref. 2021/43563]

205. *UK HPR1000 Engineering Level 4 Meeting - RO-UKHPR1000-0056,* ONR-NR-CR-21-235, Revision 0, July 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/58304]

206. *UK HPR1000 Engineering Level 4 Meeting - RO-UKHPR1000-0056,* ONR-NR-CR-21-272, Revision 0, August 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/62785]

207. *UK HPR1000 Engineering Level 4 Meeting - RO-UKHPR1000-0056,* ONR-NR-CR-21-287, Revision 0, September 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/67269]

208. *UK HPR1000 - Step 4 Conventional Health and Safety Assessment Report,* ONR-NR-AR-21-009, Revision 0, January 2022, Office for Nuclear Regulation. [CM9 Ref. 2021/50011]

209. *Assessment of the Response to RO-UKHPR1000-0056 - Fuel Route Safety Case,* ONR-NR-AN-21-054, Revision 0, September 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/70093]

210. *UK HPR1000 Pre-Construction Safety Report Chapter 6 - Reactor Coolant Systems,* HPR/GDA/PCSR/0006, Revision 002, October 2021, General Nuclear System Ltd.. [CM9 Ref. 2021/72678]

211. *UK HPR1000 Pre-Construction Safety Report Chapter 7 - Safety Systems,* HPR/GDA/PCSR/0007, Revision 002, October 2021, General Nuclear System Ltd.. [CM9 Ref. 2021/72677]

212. *UK HPR1000 Pre-Construction Safety Report Chapter 10 - Auxiliary Systems,* HPR/GDA/PCSR/0010, Revision 002, October 2021, General Nuclear System Ltd.. [CM9 Ref. 2021/72674]

213. *UK HPR1000 Pre-Construction Safety Report Chapter 11 - Steam and Power Conversion System,* HPR/GDA/PCSR/0011, Revision 002, October 2021, General Nuclear System Ltd.. [CM9 Ref. 2021/72673]

214. *UK HPR1000 Pre-Construction Safety Report Chapter 23 - Radioactive Waste Management,* HPR/GDA/PCSR/0023, Revision 002, October 2021, General Nuclear System Ltd.. [CM9 Ref. 2021/72657]

215. *UK HPR1000 Pre-Construction Safety Report Chapter 28 - Fuel Route and Storage,* HPR/GDA/PCSR/0028, Revision 002, October 2021, General Nuclear System Ltd.. [CM9 Ref. 2021/72624]

216. *ONR - UK HPR1000 GDA - PCSR Version 2 Draft 1 - Mechanical Engineering Comments,* Revision 1, July 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/53366]

217. *UK HPR1000 Mechanical Engineering Level 4 Meeting: Safety Case Consolidation,* ONR-NR-CR-21-115, Revision 0, May 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/43052]

218. *RIS-Safety Injection System, Design Manual Chapter 3, System Functions and Design Bases,* GHX17RIS003DNHX45GN, Revision F, May 2021, CGN. [CM9 Ref. B: 2018/318450 C: 2019/318827 E: 2020/315911 F: 2021/43575]

219. *The Confined Spaces Regulations 1997,* Statutory Instrument 1997 No. 1713, January 1998, Crown Copyright. www.legislation.gov.uk

220. *Safety Case Consolidation for Mechanical Engineering Topic Area - Scope of review and plan,* Revision 0, May 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/54007]

221. *Assessment of the Response to RO-UKHPR1000-0023 – Demonstration of Diverse Protection for frequent faults,* ONR-NR-AN-21-027, Revision 0, June 2021, Office for Nuclear Regulation. [CM9 Ref. 2021/48327]

222. *Safe work in confined spaces. Confined Spaces Regulations 1997. Approved Code of Practice, Regulations and guidance,* L101, Third Edition, December 2014, HSE Books. www.hse.gov.uk

Annex 1

Mechanical Engineering Assessment Scope

	Structure, System and Components																					
System	ASP [SPRHRS]	ASG [EFWS]	EHR [CHRS]	EPP [CLRTMS]	DCL [MCRACS]	DEL [SCWS]	DVL [EDSBVS]	RCP [RCS]														
PCSR Chapter No.	7	7	7	7	10	10	10	6			7			10	10	23	7	11	10	10	28	10
System Description	Secondary Passive Residual Heat Removal System	Emergency Feedwater System	Containment Heat Removal System	Containment Leak Rate Testing and Monitoring System	Main Control Room Air Conditioning System	Safety Chilled Water System	Electrical Division of Safeguard Building Ventilation System	Reactor Coolant System			Safety Injection System			Component Cooling Water System	Essential System	Liquid Waste Treatment System	Atmospheric Steam Dump System	Main Steam System	Fuel Building Handling Equipment System	Reactor Building Handling Equipment System	Fuel Handling and Storage System	Diesel Generator
THEME / **SSC DETAIL**	Condenser (Heat Exchanger)	Containment Isolation Valves	Containment Heat Removal Pump	Personal Airlock Equipment Hatch	HEPA Filter	Chiller Unit	Isolation Damper	Reactor Coolant Pump	Pressure Relief Valve / SADV	Control Rod Drive Mechanism	IRWST Strainer	Medium Head Safety Injection Pump	Residual Heat Removal Exchanger	Containment Isolation Valve	Centrifugal Pump	Process Drains Storage Tank	Silencer	Isolation Valve	Spent Fuel Cask Crane	Polar Crane	Spent Fuel Pool Crane	Emergency Diesel Generator
Mechanical Engineering Equipment's Functional Safety Classification / Design Provision Classification	F-SC3 / NC	F-SC1 / B-SC2	F-SC3 / B-SC2	F-SC1 / B-SC2	F-SC2 / NC	F-SC2 / NC	F-SC2 / NC	F-SC1 / B-SC1	F-SC1 / B-SC1	F-SC1 / B-SC1	F-SC1 / NC	F-SC1 / B-SC2	F-SC1 / B-SC2	F-SC1 / B-SC2	F-SC1 / NC	F-SC3 / B-SC3	F-SC1 / NC	F-SC1 / B-SC2	NC / B-SC2	NC / B-SC1	NC / B-SC2	F-SC1 / NC
THEME 1: Adequacy of the UK HPR1000 HVAC Design Substantiation																						
THEME 2: Adequacy of the ME Schedule - includes Categorisation and Classification of SSCs																						
THEME 3: Adequacy of Equipment Qualification Arrangements - relating to RO-UKHPR1000-0048																						
THEME 4: Closure of Gaps Against RGP - relating to RO-UKHPR1000-0012																						
THEME 5: Adequacy of EIMT Arrangements - relating to RO-UKHPR1000-0021																						
THEME 6: Adequacy and Application of the Design Assurance Arrangements																						
THEME 7: Application of the ALARP Principle when Considering Design Changes																						
THEME 8: Approach to Reducing the Hazards from Fibrous Material within the UK HPR1000 Loss of Coolant Accident Zone of Influence																						
THEME 9: Approach to Demonstrating Nuclear Lifts Reduce Risks ALARP																						
THEME 10: Lifting Operations within the Fuel Building - relating to RO-UKHPR1000-0014																						

Key:

= Heat exchangers

= Valves

= Pumps

= Lifting equipment

= HVAC components

= Others

Annex 2

Relevant Safety Assessment Principles Considered During the Assessment

SAP No	SAP Title	Description
FP.3	Optimisation of protection	Protection must be optimised to provide the highest level of safety that is reasonably practicable.
FP.4	Safety assessment	Dutyholders must demonstrate effective understanding and control of the hazards posed by a site or facility through a comprehensive and systematic process of safety assessment.
FP.5	Limitation of risks to individuals	Measures for controlling radiation risks must ensure that no individual bears an unacceptable risk of harm.
FP.6	Prevention of accidents	All reasonably practicable steps must be taken to prevent and mitigate nuclear or radiation accidents.
MS.4	Learning	Lessons should be learned from internal and external sources to continually improve leadership, organisational capability, the management system, safety decision making and safety performance.
SC.2	Safety case process outputs	The safety case process should produce safety cases that facilitate safe operation.
SC.4	Safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
SC.7	Safety case maintenance	A safety case should be actively maintained throughout each of the lifecycle stages and reviewed regularly.
EKP.1	Inherent safety	The underpinning safety aim for any nuclear facility should be an inherently safe design, consistent with the operational purposes of the facility.

SAP No	SAP Title	Description
EKP.2	Fault tolerance	The sensitivity of the facility to potential faults should be minimised.
EKP.3	Defence in depth	Nuclear facilities should be designed and operated so that defence in depth against potentially significant faults or failures is achieved by the provision of multiple independent barriers to fault progression.
EKP.4	Safety function	The safety function(s) to be delivered within the facility should be identified by a structured analysis.
EKP.5	Safety measures	Safety measures should be identified to deliver the required safety function(s).
ECS.1	Safety categorisation	The safety functions to be delivered within the facility, both during normal operation and in the event of a fault or accident, should be identified and then categorised based on their significance with regard to safety.
ECS.2	Safety classification of structures, systems and components	Structures, systems and components that have to deliver safety functions should be identified and classified on the basis of those functions and their significance to safety.
ECS.3	Codes and standards	Structures, systems and components that are important to safety should be designed, manufactured, constructed, installed, commissioned, quality assured, maintained, tested and inspected to the appropriate codes and standards.
ECS.5	Use of experience, tests or analysis	In the absence of applicable or relevant codes and standards, the results of experience, tests, analysis, or a combination thereof, should be applied to demonstrate that the structure, system or component will perform its safety function(s) to a level commensurate with its classification.
EQU.1	Qualification Procedures	Qualification procedures should be applied to confirm that structures, systems and components will perform their allocated safety function(s) in all normal operational, fault and accident conditions identified in the safety case and for the duration of their operational lives.

SAP No	SAP Title	Description
EDR.1	Failure to safety	Due account should be taken of the need for structures, systems and components to be designed to be inherently safe, or to fail in a safe manner, and potential failure modes should be identified, using a formal analysis where appropriate.
EDR.2	Redundancy, diversity and segregation	Redundancy, diversity and segregation should be incorporated as appropriate within the designs of structures, systems and components.
EDR.3	Common cause failure	Common cause failure (CCF) should be addressed explicitly where a structure, system or component employs redundant or diverse components, measurements or actions to provide high reliability.
ERL.1	Form of claims	The reliability claimed for any structure, system or component should take into account its novelty, experience relevant to its proposed environment, and uncertainties in operating and fault conditions, physical data and design methods.
ERL.2	Measures to achieve reliability	The measures whereby the claimed reliability of systems and components will be achieved in practice should be stated.
ERL.3	Engineered safety measures	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.
ERL.4	Margins of conservatism	Where safety-related systems and/or other means are claimed to reduce the frequency of a fault sequence, the safety case should include a margin of conservatism to allow for uncertainties.
ECM.1	Commission testing	Before operating any facility or process that may affect safety it should be subject to commissioning tests defined in the safety case.
EMT.1	Identification of requirements	Safety requirements for in-service testing, inspection and other maintenance procedures and frequencies should be identified in the safety case.

SAP No	SAP Title	Description
EMT.2	Frequency	Structures, systems and components should receive regular and systematic examination, inspection, maintenance and testing as defined in the safety case.
EMT.3	Type-testing	Structures, systems and components should be type tested before they are installed to conditions equal to, at least, the most onerous for which they are designed.
EMT.4	Validity of equipment qualification	The continuing validity of equipment qualification of structures, systems and components should not be unacceptably degraded by any modification or by the carrying out of any maintenance, inspection or testing activity.
EMT.5	Procedures	Commissioning and in-service inspection and test procedures should be adopted that ensure initial and continuing quality and reliability.
EMT.6	Reliability claims	Provision should be made for testing, maintaining, monitoring and inspecting structures, systems and components (including portable equipment) in service or at intervals throughout their life, commensurate with the reliability required of each item.
EMT.7	Functional testing	In-service functional testing of structures, systems and components should prove the complete system and the safety function of each functional group.
EMT.8	Continuing reliability following events	Structures, systems and components should be inspected and/or re-validated after any event that might have challenged their continuing reliability.
EAD.1	Safe working life	The safe working life of structures, systems and components that are important to safety should be evaluated and defined at the design stage.
EAD.2	Lifetime margins	Adequate margins should exist throughout the life of a facility to allow for the effects of materials ageing and degradation processes on structures, systems and components.

SAP No	SAP Title	Description
EAD.3	Periodic measurement of material properties	Where material properties could change with time and affect safety, provision should be made for periodic measurement of the properties.
EAD.4	Periodic measurement of parameters	Where parameters relevant to the design of plant could change with time and affect safety, provision should be made for their periodic measurement.
EAD.5	Obsolescence	A process for reviewing the obsolescence of structures, systems and components important to safety should be in place.
ELO.1	Access	The design and layout should facilitate access for necessary activities and minimise adverse interactions while not compromising security aspects.
ELO.4	Minimisation of the effects of incidents	The design and layout of the site, its facilities (including enclosed plant), support facilities and services should be such that the effects of faults and accidents are minimised.
EHA.5	Design basis event operating states	Analysis of design basis events should assume the event occurs simultaneously with the facility's most adverse permitted operating state (see ONR SAPs paragraph 631 c) and d)) (Ref. 2).
EHA.9	Earthquakes	The seismology and geology of the area around the site and the geology and hydrogeology of the site should be evaluated to derive a design basis earthquake (DBE).
EPS.3	Pressure relief	Adequate pressure relief systems should be provided for pressurised systems and provision should be made for periodic testing.
EMC.3	Evidence	Evidence should be provided to demonstrate that the necessary level of integrity has been achieved for the most demanding situations identified in the safety case.

SAP No	SAP Title	Description
EMC.7	Loadings	The schedule of design loadings (including combinations of loadings) for components and structures, together with conservative estimates of their frequency of occurrence should be used as the basis for design against normal operation, fault and accident conditions. This should include plant transients and tests together with internal and external hazards.
EMC.11	Failure modes	Failure modes should be gradual and predictable.
EMC.13	Materials	Materials employed in manufacture and installation should be shown to be suitable for the purpose of enabling an adequate design to be manufactured, operated, examined and maintained throughout the life of the facility.
EMC.22	Materials compatibility	Materials compatibility for components should be considered for any operational or maintenance activity.
EMC.25	Leakage	Means should be available to detect, locate, monitor and manage leakages that could indicate the potential for an unsafe condition to develop or give rise to significant radiological consequences.
ESS.21	Reliability	The design of safety systems should avoid complexity, apply a failsafe approach and incorporate means of revealing internal faults at the time of their occurrence.
EHF.6	Workspace design	Workspaces in which operations (including maintenance activities) are conducted should be designed to support reliable task performance. The design should take account of the physical and psychological characteristics of the intended users and the impact of environmental factors.
ECV.1	Prevention of leakage	Radioactive material should be contained and the generation of radioactive waste through the spread of contamination by leakage should be prevented.

SAP No	SAP Title	Description
ECV.3	Means of confinement	The primary means of confining radioactive materials should be through the provision of passive sealed containment systems and intrinsic safety features, in preference to the use of active dynamic systems and components.
ECV.10	Ventilation system safety functions	The safety functions of the ventilation system should be clearly identified and the safety philosophy for the system in normal, fault and accident conditions should be defined.
ERC.1	Design and operation of reactors	The design and operation of the reactor should ensure the fundamental safety functions are delivered with an appropriate degree of confidence for permitted operating modes of the reactor.
EHT.1	Design	Heat transport systems should be designed so that heat can be removed or added as required.
EHT.2	Coolant inventory and flow	Sufficient coolant inventory and flow should be provided to maintain cooling within the limits (operating rules) derived for normal operational and design basis fault conditions.
RP.1	Normal operation (Planned Exposure Situations)	Adequate protection against exposure to radiation and radioactive substances should be provided in those parts of the facility to which access is permitted during normal operation.
RP.6	Shielding	Where shielding has been identified as a means of restricting dose, it should be effective under all normal operation and fault conditions where it provides this safety function.
RP.7	Hierarchy of control measures	The dutyholder should establish a hierarchy of control measures to optimise protection in accordance with IRR17.
NT.1	Assessment against targets	Safety cases should be assessed against the SAPs numerical targets for normal operational, design basis fault and radiological accident risks to people on and off the site.

Annex 3

Mechanical Engineering Assessment Findings

The following Assessment Findings must be read in conjunction with the relevant text in the identified report sub-section

Number	Assessment Finding	Report Sub section
AF-UKHPR1000-0128	The licensee shall, during detailed design of the heating, ventilation and air conditioning systems, justify that: ■ local peak internal temperatures are derived from extreme exterior temperature conditions for the site; ■ dependant safety related equipment remains within its qualified temperature limits; ■ they are resilient against extreme exterior temperature, avoiding cliff-edge effects. Examples include flowrates, heating and thermal failures; ■ through testing, the chosen filter’s efficiency and pressure drop performance are at least equivalent to that of a modern, cylindrical filter; and ■ the chiller design accounts for temperature, relative humidity and enthalpy during extreme exterior temperature conditions.	4.1.1
AF-UKHPR1000-0129	The licensee shall, during detailed design, produce a strategy and plan to justify the Mechanical Engineering design basis for all safety related systems and components. From this, information shall be provided for an agreed sample to address the following: ■ evidence validating performance requirements; ■ limits and conditions necessary in the interest of safety; ■ qualification and testing requirements; and ■ any other requirements necessary to meet or maintain the safety case, for example examination, inspection, maintenance and testing.	4.2.1

Number	Assessment Finding	Report Sub section
AF-UKHPR1000-0130	The licensee shall, during site-specific stages, produce a strategy and plan to demonstrate suitable application of its safety categorisation and classification arrangements for Mechanical Engineering systems and components. From this, information shall be provided for an agreed sample to demonstrate how the licensee: ■ where reasonably practicable, prioritises prevention over protection in its application of defence in depth; and ■ considers unmitigated radiological consequences when categorising safety functions.	4.2.1
AF-UKHPR1000-0131	The licensee shall demonstrate, during detailed design, that the capacity of the Nuclear Island Vent and Drain System sump pump is sufficient to ensure that the tanks do not overflow.	4.2.1
AF-UKHPR1000-0132	The licensee shall demonstrate, during detailed design, that: ■ the control rod drive mechanism safety functions and performance requirements are complete; and ■ the coil stack seismic withstand is appropriate.	4.2.1
AF-UKHPR1000-0133	The licensee shall, during site-specific stages, produce a strategy and plan to justify equipment qualification for all safety related Mechanical Engineering systems and components. From this, information shall be provided for an agreed sample to address the following: ■ the performance requirements and their traceability; ■ how testing demonstrates the required performance; and ■ when testing is undertaken i.e. during verification, implementation or preservation phases.	4.3.1

Number	Assessment Finding	Report Sub section
AF-UKHPR1000-0134	The licensee shall demonstrate, during site-specific stages, that the reactor coolant pump's: ■ shaft seal injection and its supporting systems, are suitably designed and qualified to deliver their safety functions; ■ anti-reverse function is validated during system commissioning; ■ endurance test is sufficient to qualify its operational life; and ■ seismic coast down qualification method is appropriate.	4.3.1
AF-UKHPR1000-0135	The licensee shall demonstrate, during detailed design, that the pressuriser safety valve and its pilot valve are qualified for "feed and bleed" operations, when liquid may pass through the valves.	4.3.1
AF-UKHPR1000-0136	The licensee shall demonstrate, during detailed design, that the medium head safety injection pump's: ■ mission time is justified; and ■ endurance test shows that it can meet its required mission time.	4.3.1
AF-UKHPR1000-0137	The licensee shall, during detailed design, produce a strategy and plan to justify its process isolations align with 'HSG253 The safe isolation of plant and equipment'. From this, isolation and drainage information shall be provided for an agreed Mechanical Engineering sample of systems and components.	4.5.1
AF-UKHPR1000-0138	The licensee shall demonstrate, during detailed design of the residual heat removal heat exchanger, that the risk from primary circuit fluid retention is as low as reasonably practicable. This risk relates to intrusive maintenance operations.	4.5.1
AF-UKHPR1000-0139	The licensee shall, during detailed design, demonstrate that the boron dilution modification to the Low Head Safety Injection pump, reduces risks to as low as reasonably practicable. The modification should consider the hierarchy of control measures for restricting exposure and prevention of leakage.	4.7.1

Number	Assessment Finding	Report Sub section
AF-UKHPR1000-0140	The licensee shall demonstrate, during detail design, that the spent fuel cask design, including handling operations, reduces risks as low as reasonably practicable. This shall include prevention or mitigation of spent fuel assemblies falling from the cask should it topple within the Loading Pit.	4.10.1
AF-UKHPR1000-0141	The licensee shall, during detailed design, justify the design and safety case for the Spent Fuel Pool Crane. This should: ■ identify diverse, engineered prevention and protection measures for all design basis faults; ■ using the hierarchy of control measures, justify the choice of mechanical and/or control and instrumentation safety measures; ■ justify the hoist load path classification; and ■ substantiate claims made against the integrity of the fixed and telescopic sleeves.	4.11.1
AF-UKHPR1000-0142	The licensee shall, during detailed design: ■ justify the means for handling 'heavy items' such as hoist drums or motors, during examination, inspection, maintenance and testing of Fuel Building cranes; and ■ demonstrate that there is sufficient clearance between cranes to allow safe removal and replacement of such items.	4.11.1
AF-UKHPR1000-0143	The licensee shall demonstrate, during detailed design, how the Spent Fuel Pool sluice gate design arrangement aligns with the hierarchy of control measures in: ■ preventing or protecting against inadvertent opening; ■ preventing or withstanding a collision by the Spent Fuel Pool Crane whilst closed, stopping water entering either the Transfer Pit or Loading Pit; and ■ reducing the risk of water ingress into the Transfer Pit and Loading Pit via a suitable sealing design.	4.11.1