Office for Nuclear Regulation

New Reactors Division – Generic Design Assessment

Step 4 Assessment of Human Factors for the UK HPR1000 Reactor

Assessment Report ONR-NR-AR-21-013
Revision 0
January 2022

Published 01/22

For published documents, the electronic copy on the ONR website remains the most current publicly available version and copying or printing renders this document uncontrolled.

EXECUTIVE SUMMARY

This report presents the findings of the assessment of the Human Factors (HF) aspects of the UK HPR1000 reactor design undertaken as part of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA). The assessment was carried out using the Pre-Construction Safety Report (PCSR) and supporting documentation submitted by the Requesting Party (RP).

The objective of the assessment was to make a judgement, from a HF perspective, on whether the generic UK HPR1000 design could be built and operated in Great Britain, in a way that is acceptably safe and secure (subject to site-specific assessment and licensing), as an input into ONR's overall decision on whether to grant a Design Acceptance Confirmation (DAC).

The scope of my GDA assessment was to review the safety aspects of the generic UK HPR1000 design by examining the claims, arguments and supporting evidence in the safety case. The GDA Step 4 assessment built upon the work undertaken in GDA Steps 2 and 3, and enabled a judgement to be made on the adequacy of the HF information contained within the PCSR and supporting documentation.

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

- The adequacy of the HF Integration (HFI) on the project.
- The suitability of the Allocation of nuclear safety Functions (AoF) between the human and technology.
- The adequacy of HF Engineering (HFE) programme.
- The adequacy of the RP's approach to the Identification, Analysis and Substantiation of Human Based Safety Claims (HBSCs).
- The adequacy of the HF Safety Case and Design Analysis Submissions.

The conclusions from my assessment are:

- The RP has successfully demonstrated that the HFI programme has been of benefit to the safety of the generic UK HPR1000 design as it has produced several design enhancements.
- The RP has developed an HF capability – including team growth, securing specialist support, and improving technical capability – sufficient to meet the needs of the GDA process.
- The safety functional allocation between the technology and the human has been appropriately validated during GDA using a new proprietary method developed by the RP for GDA. I consider the method to represents best practice as it considers the complex nature of allocation that new technologies support. The RP recognises the limitations of its analysis and has identified where further work will be necessary by the licensee, to consider a wider range of safety functions, such as activities relating to maintenance.
- The probabilistic HRA case shows that the design is suitably tolerant to human error against ONR's risk targets. The design has been shown to meet the Basic Safety Objectives (BSO) for ONR's numerical targets 5-8 when all Probabilistic Safety Analysis (PSA) Human Error Probabilities (HEPs) are set to 1 in 100.
- The RP has demonstrated effective management of Human Based Safety Claims during GDA. This is an important enabler for the licensee. HBSCs are captured in the Fault Schedule, PSA, and Internal and External Hazard Schedules.

- The RP has submitted a further action plan to demonstrate it recognises the limitations of GDA and set out what additional work will be required by the licensee. The plan closely aligns with my own assessment.
- Many of the shortfalls against regulatory expectations I have identified during my assessment can be mitigated during detailed design, affording the opportunity during the site-specific stages to address any HFE shortfalls. It is important to note that this carries an enhanced design foreclosure risk. I consider the risks of foreclosure of design options manageable but will lead to a significant HF programme of work for the licensee.
- The quality of design and safety analysis submissions will need to continue to improve during the site-specific stage. The variability does not challenge my overall judgements, but will need effort from the licensee to resolve.
- A lack of integration between HF team derived HRA and PSA team derived HRA. This has been suitably mitigated for GDA by sensitivity analysis, but I would expect the licensee to ensure that the analysis delivers best estimate HRA data, whilst taking account of the uncertainties endemic in HRA modelling. I am confident the licensee can resolve this.
- The approach to HRA, which fails to suitably take account of, and model, the impact of credible errors on factors such as task timing, dependent failures, and workload requires improvement. This was mitigated for GDA by appropriate sensitivity analysis within the HRA.
- Some HFE submissions do not always provide suitable and sufficient evidence to demonstrate compliance with HF RGP. Site-specific design work affords an opportunity for the licensee to address this shortfall.
- The expansion in scope and scale of the HFI programme to meet regulatory expectations led to a lack of clarity in the RP's suite of submissions.
- A lack of task-driven HFE design, in preference to code and standard compliance.
- Not adequately capitalising on available OPEX and organisational learning, sufficient to inform the design and safety analysis.

These conclusions are based upon the following factors:

- A detailed and in-depth technical assessment, on a sampling basis, of the full scope of safety submissions at all levels of the hierarchy of the generic UK HPR1000 safety case documentation.
- Independent information, reviews, and analysis of key aspects of the generic safety case undertaken by Technical Support Contractors (TSCs).
- Detailed technical interactions on many occasions with the RP, alongside the assessment of the responses to the substantial number of Regulatory Queries (RQs) and Regulatory Observations (ROs) raised during the GDA. Video based inspection activities of the RP's main control room trials and the FCG3 reference plant.

Several matters also remain, which I judge are appropriate for the licensee to consider and take forward in its site-specific safety submissions. These matters do not undermine the generic UK HPR1000 design and safety submissions but are primarily concerned with the provision of site-specific safety/security case evidence which will become available as the project progresses through the detailed design, construction, and commissioning stages. These matters have been captured in 15 Assessment Findings.

Overall, based on the assessment undertaken in accordance with ONR's procedures, the claims, arguments, and evidence laid down within the PCSR and supporting documentation submitted as part of the GDA process present an adequate safety case for the generic UK HPR1000 design. It is recommended that from a HF perspective a DAC may be granted.

LIST OF ABBREVIATIONS

ALARP	As Low As Reasonably Practicable
ASEP	Accident Sequence Evaluation Program
ASG	Emergency Feedwater
ASP	Secondary Passive Heat Removal System
ATWS	Anticipated Transient without SCRAM
BEIS	Department for Business Energy and Industrial Strategy
BFX	Fuel Building
BMS	Business Management System
BNX	Nuclear Auxiliary Building
BSL	Basic Safety Level (in SAPs)
BSO	Basic Safety Objective (in SAPs)
BWX	Radioactive Waste Treatment Building
CAE	Claims, Arguments and Evidence
C&I	Control and Instrumentation
CCF	Common Cause Failure
CD	Core Damage
CDF	Core Damage Frequency
CGN	China General Nuclear Power Corporation Ltd
CRF	Circulating Water System
CoO	Concept of Operations
DAC	Design Acceptance Confirmation
DCL	Main Control Room Air Conditioning System
DR	Design Reference
DVL	Safeguard Building Ventilation
DXS	Essential Service Water Pumping Station Ventilation System
EDG	Emergency Diesel Generator
EHR	Containment Heat Removal System
EMIT	Examination. Maintenance, Inspection and Testing
EOP	Emergency Operating Procedure
FAP	Further/Forward Action Plan
FCG	Fangchenggang
FoV	Field of View
FV	Fussell Vesely
GDA	Generic Design Assessment
GNSL	General Nuclear Systems Ltd.
HBSC	Human Based Safety Claims

HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Event
HFE	Human Factors Engineering
HFIP	Human Factors Integration Plan
HRA	Human Reliability Analysis
HBSC	Human Based Safety Claims
HVAC	Heating, Ventilation and Air Conditioning
IAEA	International Atomic Energy Agency
IRWST	In-containment Refuelling Water Storage Tank
ITS	Issues Tracking System
IVR	In Vessel Retention
KDA	Severe Accident Control and Instrumentation System
LOCA	Loss of Coolant Accident
LRF	Large Release Frequency
MCD	Medium Pressure Rapid Cooldown
MCR	Main Control Room
ME	Mechanical Engineering
NPP	Nuclear Power Plant
NUREG	United Stated Nuclear Regulator
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PCSR	Pre-construction Safety Report
PIE	Postulated Initiating Event
POS	Plant Operating State
PSA	Probabilistic Safety Analysis
PSF	Performance Shaping Factor
PWR	Pressurised Water Reactor
RAW	Risk Achievement Worth
RCV	Chemical and Volume Control System
RGP	Relevant Good Practice
RHR	Residual Heat Removal System
RIS	Safety Injection System
RO	Regulatory Observation
RP	Requesting Party
RPV	Reactor Pressure Vessel
RQ	Regulatory Query
SAMG	Severe Accident Management Guideline

SAP(s)	Safety Assessment Principle(s)
SB-LOCA	Small Break Loss of Coolant Accident
SBO	Station Blackout
SBODG	Station Blackout Diesel Generator
SCD	Secondary Cooldown
SDM	System Design Manual
SE	Safety Engineer
SFP	Spent Fuel Pool
SG	Steam Generator
SGTR	Steam Generator Tube Rupture
SHERPA	Systematic Human Error Reduction and Prediction Approach
SoDA	(Environment Agency's) Statement of Design Acceptability
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SSC	Structures, Systems and Components
TAG	Technical Assessment Guide(s)
THERP	Technique for Human Error Rate Prediction
TRACER	Technique for Retrospective Analysis of Cognitive Error
TSC	Technical Support Contractor
USNRC	United States Nuclear Regulatory Commission
WENRA	Western European Nuclear Regulators' Association
V&V	Verification and Validation

TABLE OF CONTENTS

Table(s)

Annex(es)

1 INTRODUCTION

1.1 Background

1. This report presents my assessment conducted as part of the Office for Nuclear Regulation (ONR) Generic Design Assessment (GDA) for the generic UK HPR1000 design within the topic of Human Factors (HF).

2. The UK HPR1000 is a Pressurised Water Reactor (PWR) design proposed for deployment in the UK. General Nuclear System Limited is a UK-registered company that was established to implement the GDA on the UK HPR1000 design on behalf of three joint requesting parties (RP), i.e., China General Nuclear Power Corporation (CGN), EDF SA and General Nuclear International.

3. GDA is a process undertaken jointly by the ONR and 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 from the GDA process 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 for the generic UK HPR1000 design followed a step-wise approach in a claims-argument-evidence hierarchy which commenced in 2017. Major technical interactions started in Step 2 which focussed on an examination of the main claims made by the RP for the UK HPR1000. In Step 3, the arguments which underpin those claims were examined. The Step 2 reports for individual technical areas, and the summary reports for Steps 2 and 3 are published on the joint regulators' website. The objective of Step 4 was to complete an in-depth assessment of the evidence presented by the RP to support and form the basis of the safety and security cases.

5. The full range of items that form part of my assessment is provided in ONR's 'GDA Guidance to Requesting Parties' (Ref. 1). These include:

   - Consideration of 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 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 the detailed engineering design.
   - Assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final as-built design.
   - Resolution of identified nuclear safety and security issues or identifying paths for resolution.

6. The purpose of this report is therefore to summarise my assessment in the HF topic which provides an input to the ONR decision on whether to grant a DAC, or otherwise. This assessment was focused on the submissions made by the RP throughout GDA, including those provided in response to the Regulatory Queries (RQs), Regulatory Observations (ROs). Any ROs issued to the RP are published on ONR's GDA website, together with the corresponding resolution plans.

1.2 Scope of this Report

7. This report presents the findings of my assessment of the HF aspects of the generic UK HPR1000 design undertaken as part of GDA. I carried out my assessment using the 'Pre-construction Safety Report' (PCSR) (Ref. 3) and supporting documentation submitted by the Requesting Party (RP). My assessment was focussed on considering whether the generic safety case provides an adequate justification for the generic UK HPR1000 design, in line with the objectives for GDA.

1.3 Methodology

8. The methodology for my assessment follows ONR's guidance on the mechanics of assessment, 'NS-TAST-GD-096' (Ref. 4).

9. My assessment was undertaken in accordance with the requirements of the Office for Nuclear Regulation (ONR) How2 Business Management System (BMS). The ONR 'SAPs' (Ref. 2), together with supporting Technical Assessment Guides (TAG) (Ref. 4), were used as the basis for my assessment. Further details are provided in Section 2. The outputs from my assessment are consistent with 'ONR's GDA Guidance to RPs' (Ref. 1).

2 ASSESSMENT STRATEGY

10. The strategy for my assessment of the HF aspects of the UK HPR1000 design and safety case is set out in this section. This identifies the scope of the assessment and the standards and criteria that have been applied.

2.1 Assessment Scope

11. A detailed description of my approach to this assessment can be found in assessment plan 'UKHPR1000-AP-19-011 Revision 0' (Ref. 5).

12. I considered all of the main submissions within the remit of my assessment scope, to various degrees of breadth and depth. I chose to concentrate my assessment on those aspects that I judged to have the greatest safety significance, or where the hazards appeared least well controlled. My assessment was also 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. A particular focus of my assessment has been the RQs and ROs I raised as a result of my on-going assessment, and their resolution thereof.

13. The HF topic is extremely wide in scope as it includes the through life interactions that humans have with the plant design. It is also a topic which is not well codified, and one in which Relevant Good Practice (RGP) is not always well established. Taking this into account, and in order to fulfil the aims for the Step 4 assessment of the generic UK HPR1000 design, I have assessed the following areas, which are split into 4 key assessment work-streams:

- Human Factors Integration (HFI)
- Allocation of Function (AoF)
- Human Factors Engineering (HFE)
- Human Reliability Assessment (HRA) (including identification, analysis and substantiation of Human Based Safety Claims (HBSCs)

14. Outputs from these workstreams also feed into my overall regulatory judgements regarding the demonstration of ALARP and the adequacy of the generic UK HPR1000 consolidated safety case at the close of GDA.

2.1.1 Work stream 1 - Human Factors Integration

15. Suitable and sufficient HFI is a key regulatory expectation in the HF topic area (SAP EHF. 1). It is key to enabling ONR's sampling approach to assessment in the HF area as effective HFI provides confidence that HF is being considered proportionally in all areas of the design. My assessment within this work-stream considered the adequacy of the RP's HFI approach and its outcomes.

2.1.2 Work Stream 2 - Allocation of Function

16. The suitable allocation of safety functions between the human and technology on an NPP design is a key regulatory expectation under (SAP EHF.2). It guides that the dependence on human action to maintain and recover a stable, safe state should be minimised. Further, the allocation of safety actions between humans and engineered Systems, Structures and Components (SSCs) should be substantiated taking account of human capabilities and limitations (Allocation of Function). My assessment within this work-stream considered the adequacy of the RP's AoF approach and its outcomes.

2.1.3 Work stream 3 - Human Factors Engineering

17. Suitable and sufficient HFE is a key regulatory expectation within GDA in the HF assessment area (SAP EHF. 1). When effective, it provides confidence that all SSCs are benefitting from being optimised for operability and safety. My assessment within this work-stream considered the adequacy of the RP's HFE approach and outcomes.

2.1.4 Work stream 4 - Human Reliability Assessment

18. The identification, analysis and substantiation of all human actions necessary for safety are regulatory expectations set out in SAPs EHF.5 Task Analysis and EHF.10 Human Reliability. A suitable and sufficient HRA is key to demonstrating that the risks from human actions have been reduced to ALARP and is also key to supporting ONR's sampling approach. My assessment of the HRA was jointly-conducted with ONR's Probabilistic Safety Analysis (PSA) inspectors. My assessment within this work-stream considered the adequacy of the RP's HRA approach and its outcomes. This assessment considers the detailed derivation of HEPs including the adequacy of qualitative substantiation. The PSA assessment considered the HRA derived by the PSA team including its completeness within the PSA and the structural modelling.

2.2 Sampling Strategy

19. In line with ONR's guidance (Ref. 4), I chose a sample of the RP's submissions to undertake my assessment. The main themes considered were:

- Key safety risks relevant to HF.
- Key design foreclosure risks that should be considered during the generic UK HPR1000 design stage.
- The capacity and the capability of the RP to deliver a modern standards HFI programme.
- The adequacy of applied HFE codes, methods and standards, and the associated guidance used by the RP. It also considered the design outcomes.
- The adequacy of the applied HRA codes, methods and standards, and the associated guidance used by the RP. It also considered the derived HRA.

2.3 Out of Scope Items

20. The following items were outside the scope of my assessment:

- Assessment of manning levels beyond the concept of operation level (EHF.11) as this is a site-specific matter.
- Training and personnel competence (operator) (EHF.8) as this is a site-specific matter.
- Detailed procedure design (EHF.9) as this is a site-specific matter.
- Administrative controls (EHF.4) as this is a site-specific matter.
- Fitness for duty arrangements (EHF.12) as this is a site-specific matter.
- Detailed HMI design (EH.7). This was declared out of scope of GDA by the RP.
- The emergency control centre design (EHF.7). This was declared out of scope of GDA by the RP
- Severe accident response as this is a site-specific matter.

2.4 Standards and Criteria

21. The relevant standards and criteria adopted within this assessment are principally the 'SAPs' (Ref. 2), TAGs (Ref. 4), relevant national and international standards and RGP informed from existing practices adopted on UK nuclear licensed sites. The key SAPs and any 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

22. The 'SAPs' (Ref. 2) constitute the regulatory principles against which ONR judge the adequacy of safety cases. The SAPs applicable to HF are included within Annex 1 of this report.

23. The key SAPs applied within my assessment were SAPs EHF.1 to EHF.3, EHF.5 to EHF.7, EHF.10, ECS.2, EKP.5 and SC.4.

2.4.2 Technical Assessment Guides

24. The following Technical Assessment Guides were used as part of this assessment (Ref. 4):

- Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable). NS-TAST-GD-005. Revision 9. May 2013. ONR
- The Purpose, Scope and Content of Safety Cases. NS-TAST-GD-051. Revision 4. July 2016. ONR.
- Human Factors Integration. NS-TAST-GD-058. Revision 3, March 2017. ONR
- Human Machine Interfaces. NS-TAST-GD-059. Revision 4. November 2019. ONR
- Workplaces and Work Environment. NS-TAST-GD-062. Revision 3. February 2017. ONR
- Human Reliability Analysis. NS-TAST-GD-063. Revision 4. October 2018. ONR
- Allocation of Function Between Human and Engineered Systems. NS-TAST-GD-064 Revision 3. December 2017. ONR

2.4.3 National and International Standards and Guidance

25. Where standards and guidance has been used to inform my assessment, these are referenced directly within the appropriate sections. Typically, this material originates from the International Atomic Energy Agency (IAEA), other regulatory bodies such as the US Nuclear Regulatory Commission (USNRC), or professional standard setting bodies.

2.5 Use of Technical Support Contractors

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

27. Table 1 below sets out the areas in which I used TSCs to support my assessment. I required this support to provide additional capacity and access to independent advice and experience.

Table 1: Work Packages Undertaken by the TSC (ONR Contract - ONR629)

Number	Description
1.1	Review of HFE design guidance - An independent assessment was carried out of a sample of the design guidance developed by the RP to support the generic UK HPR1000 design HFE programme.

Number	Description
2.1	Allocation of function - An independent assessment was carried out of the RP's submissions relating to assessing and validating the safety functional allocation between the human and technology for the generic UK HPR1000 design. The review took account of: design basis engineering rules; historical precedents; human capabilities and limitations; and the principle of ALARP, to form a balanced opinion on the AoF adequacy.
2.2	Human factors engineering - An independent assessment was carried out of the RP's HFE submissions to form a representative and balanced view on whether the generic UK HPR1000 design takes account of HFE principles and RGP.
2.3	Human interaction with automation – A review was carried out to develop an evidence base to inform ONR's regulatory decision-making in relation to resolution of RO-UKHPR1000-0030. The review focussed on how humans interact with automation and assistive technologies.
3.1	Human reliability analysis – An independent assessment of a sample of the RP's HRA submissions was carried out to determine whether: ■ The qualitative HRA meets modern standards. ■ The RP has suitably and sufficiently derived the calculated human reliability data – and whether it is underpinned by the qualitative analysis. ■ The RP has demonstrated that the risk of human error has been reduced so far as is reasonably practical. ■ The RP has identified ALARP improvements as part of the analysis. ■ The RP has identified and codified relevant assumptions relating to the future operation of the plant.

28. Whilst the TSC undertook detailed technical reviews, this was done under my direction and close supervision. The regulatory judgment on the adequacy or otherwise of the generic UK HPR1000 safety case in this report has been made exclusively by ONR.

2.6 Integration with Other Assessment Topics

29. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot be carried out in isolation as there are often shortfalls that span multiple disciplines. I have therefore worked closely with a number of other ONR inspectors to inform my assessment. The key interactions were:

- My assessment considers the RP's qualitative demonstration of the suitability and sufficiency of human actions in the design basis analysis part of the safety case. The PSA assessment considers HRA calculations and HRA modelling used in the PSA.
- My assessment considers the adequacy of HBSC substantiation within the fault schedule. The fault studies assessment considers the adequacy of the HBSC capture and classification.
- My assessment considers the adequacy of HBSC substantiation within the internal and external hazard schedules. The internal and external hazards

assessments considers the adequacy of the capture of HBSCs within these schedules.

- My assessment considers the conceptual viability of the RP's automatic diagnosis system in HF terms. The control and instrumentation assessment considers its engineering viability as part of associated regulatory observation. I also supported the C&I assessment of the human machine interface architecture and engineering viability.
- My assessment considers the adequacy of the lighting system guidance. The electrical assessment considers its engineering viability.
- During GDA I provided input into the mechanical engineering assessment of the Heating, Ventilation, and Air Condition (HVAC) system with respect to the HF consequences of its failure.

3 REQUESTING PARTY'S SAFETY CASE

3.1 Introduction to the generic UK HPR1000 Design

30. The generic UK HPR1000 design is described in detail in the 'PCSR' (Ref. 3). It is a three-loop PWR designed by CGN using the Chinese Hualong technology. The generic UK HPR1000 design has evolved from reactors which have been constructed and operated in China since the late 1980s, including the M310 design used at Daya Bay and Ling'ao (Units 1 and 2), the CPR1000, the CPR1000+ and the more recent ACPR1000. The first two units of CGN's HPR1000, Fangchenggang Nuclear Power Plant (NPP) Units 3 and 4, are under construction in China and Unit 3 is the reference plant for the generic UK HPR1000 design. The design is claimed to have a lifetime of at least 60 years and has a nominal electric output of 1,180 MW.

31. The reactor core contains zirconium clad uranium dioxide (UO2) fuel assemblies and 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) which is connected to the key primary circuit components, including the Reactor Coolant Pumps (RCPs), Steam Generators (SGs), pressuriser and associated piping, in the three-loop configuration. The design also includes a number of auxiliary systems that allow normal operation of the plant, as well as active and passive safety systems to provide protection in the case of faults, all contained within a number of dedicated buildings.

32. The reactor building houses the reactor and primary circuit and is based on a 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. The fuel building is also adjacent to the reactor and contains the fuel handling and short-term storage facilities. Finally, the nuclear auxiliary building contains a number of systems that support operation of the reactor. In combination with the diesel, personnel access and equipment access buildings, these constitute the nuclear island for the generic UK HPR1000 design.

3.2 The UK HPR1000 Safety Case

33. In this section I provide an overview of the HF aspects of the generic UK HPR1000 safety case as provided by the RP during GDA. Details of the technical content of the documentation and my assessment of its adequacy are reported in the subsequent sections of my report.

34. The RP has produced and submitted a suite of HF documents, which collectively form the HF safety elements of the Safety, Security, and Environment Report (SSER).

35. The structure of the HF safety case is comprised of three levels.

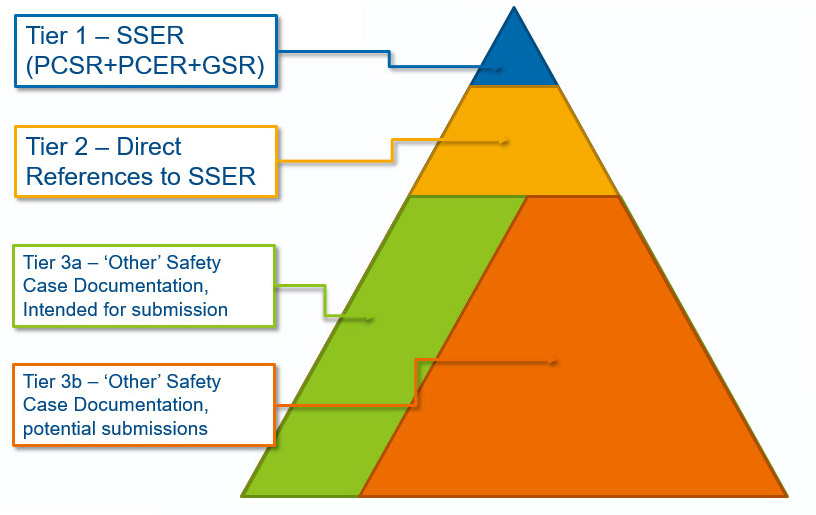

Figure 1: SSER Structure

36. Tier 1 comprises the PCSR, in which Chapter 15 presents the overarching safety case for HF.

37. Tiers 2 and 3 comprise the majority of the evidence submissions and include:

- The HF integration plan and associated documents.
- The allocation of function methodology and subsequent assessment.
- The HFE guidance documents spanning local areas and interface design.
- The HFE assessment documents.
- The qualitative HRA documents.
- The HBSC listing.
- ALARP demonstration
- OPEX submissions

38. In addition to the safety case submissions, the RP has also included a 'Further Action Plan' (FAP) (Ref.6). This document comprises the outcome from a learning exercise performed by the RP to consolidate regulatory feedback during GDA and its own assessment of the limitations in its submissions. It identified 29 future commitments for the licensee during the detailed design and site specific stage, that span the following themes:

- Human Factors Integration Plan (HFIP)
- Update RGP guidance
- Update Operational Experience (OPEX)
- Update the Target Audience Description (TAD)
- Expand the scope of the AoF work
- Support to the development of operational procedures
- Support to the development of a competent licensee and operating organisation
- HFE support to decommissioning
- Consolidation and validation of assumptions
- Develop HRA method for HCI and complete the HRA
- Conduct the V&V exercises to substantiate the design
- Support the sentencing of design modifications raised during GDA.

39. The overarching HF claim within the safety case (overall sub-claim 3.3.8) is that: HF have been appropriately taken into account in the design, assessment and management arrangements, to meet the relevant safety requirements (Ref. 3).

40. This is underpinned by four HF sub-claims:

- Sub-claim 3.3.8.SC15.1: A comprehensive programme of HF activities is used to integrate HF into the entire design process of generic UK HPR1000 design.
- Sub-claim 3.3.8.SC15.2: A concept of operation for the generic UK HPR1000 design is designed according to modern standards and RGP.
- Sub-claim 3.3.8.SC15.3: Human actions important to safety will be systematically identified. Their reliability and effective task performance will be demonstrated to be achievable.
- Sub-claim 3.3.8.SC15.4: The generic UK HPR1000 design operating and maintenance workspaces and Human Machine Interfaces (HMIs) are designed according to modern standards and good practice in HF to facilitate interaction between the personnel and the plant.

41. The requesting party has organised its submissions and safety case around these four high-level HF claims. These claims are underpinned by a series of well-developed arguments (not reproduced for brevity), which in concert, when suitably evidenced, should support the over-arching HF claim.

42. Ref. 7 ALARP Demonstration Report of PCSR Chapter 15, provides a summary of the improvements and recommendations delivered by the RP during GDA. Table 2 below summarises this.

Table 2: HF Shortfalls Identified

Source	Total	Clarification	Change to Safety Case	Design Modification	Site Commitment	Completed
Reviews against RGP	4	0	1	1	2	4
OPEX reviews	3	2	1	0	0	3
AoF reviews	10	6	0	3	0	10
HBSC Assessments	154	70	2	6	76	152
HF verification assessments	6	4	0	0	2	6
HF reviews of SSCs	105	8	23	5	73	105
Total	282	85	27	15	155	280

43. The list of HF informed design changes included into the GDA can be found in Annexe 2.

44. The goal of an HF safety case is to demonstrate that the human contribution to risk is ALARP and this is usefully summarised in the 'Concept of Operations' report (Ref. 8 CoO11). The RP claims that:

- "The radiation protection targets of Design Basis Condition (DBC)-2, DBC-3, DBC-4 and Design Extension Condition (DEC)-A can be met without operator action from the Main Control Room (MCR) in less than 30 minutes from the first significant signal.
- The radiation protection targets of DBC-2, DBC-3, DBC-4 and DEC-A can be met without action outside the MCR in less than 1 hour from the first significant signal.
- For any DBC, the battery capacity for performing FC1 and FC2 functions shall meet the requirements that their expected autonomy could be at least 2 hours without charging.
- No offsite or onsite mobile heavy equipment will be required in less than 72 hours in DBCs.
- The plant could be taken to the controlled state by the automatic protection functions for most DBCs (and, therefore, relies less on the manual intervention of operators)."

45. In addition, Ref. 9 General Safety Requirements, shows the numerical risk importance of the role of the human on the generic UK HPR1000 design.

46. ONR's SAPs contain 9 numerical targets and related requirements for evaluating site risk. Ref. 9 converts these targets to Radiation Protection Targets (RPT). For GDA it was only possible to show the human risk contribution for 5-9 due to the maturity of the analysis.

47. The targets are defined in the 'HRA Summary Report' (Ref. 10):

- RPT 5 is used to evaluate the risk of fatality to a worker on-site due to exposure to radiation from on-site accidents.
- RPT 6 is used to evaluate the frequency of any single accident in the facility which could give a dose to a worker on the site that is within a specified range.
- RPT 7 is the target for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation.
- RPT 8 is a set of targets for the total predicted frequencies of accidents on an individual facility, which could give doses in specified dose bands to a person off the site.
- RPT 9 is the target for the total risk of 100 or more fatalities, either immediate or eventual,

48. The sensitivity analysis of RPTs 5~9 is performed using a HEP range including 1, 0.1, 0.01, 0.001). The full sensitivity results are shown in the tables 10 and 11 in section 4.5. When the HEPs for all human actions are set to 0.01, the RP's radiation protection targets (which are based on ONR's numerical targets) are met.

4 ONR ASSESSMENT

4.1 Structure of Assessment Undertaken

49. This section presents my assessment of generic UK HPR1000 design GDA. It considers the adequacy of the design and safety case in relation to regulatory expectations relating to HF.

50. The structure of my assessment followed the strategy described in Section 2 of this report and has been undertaken with the assistance of TSCs who have carried out their work under my direction and supervision.

51. This section comprises the following sections:

- 4.1 Structure of Assessment Undertaken
- 4.2 Human Factors Integration
- 4.3 Human Factors Engineering
- 4.4 Identification, Analysis and Substantiation of HBSCs
- 4.5 Human Factors Safety Case and Design Analysis Submissions
- 4.6 Demonstration that Relevant Risks Have Been Reduced to ALARP
- 4.7 Consolidated Safety Case
- 4.8 Comparison with Standards, Guidance and Relevant Good Practice

52. My assessment follows on from that done at Step 2 and Step 3 of GDA (Ref. 11).

53. I have built upon the outcomes from these reports to inform the scope of my assessment to ensure that that it focussed on those areas which could have the largest impact to the generic UK HPR1000 design and safety case.

54. My assessment was guided by ONR's HF related TAGs and SAPs. In cases where I identified shortfalls there has been dialogue with the RP to resolve the shortfall or identifying if further information could be provided within GDA.

55. During GDA, I raised and closed the following Regulatory Observations:

- RO-UKHPR1000-0011, Human Factors Capability and Integration to Deliver the GDA of UK HPR1000
- RO-UKHPR1000-0030, Justification for The Use Of Automatic Diagnosis

56. I also contributed to the following ROs, which were led by a other ONR specialist inspectors:

- RO-UKHPR1000-0018, Substantiation of HRA Inputs in PSA Model (Ref. 12)
- RO-UKHPR1000-0039, Performance Analysis of UK HPR1000 Heating Ventilation and Air Conditioning Systems (Ref. 13)
- RO-UKHPR1000-0044, Identification and Use of Operational Experience (OPEX) in the UK HPR1000 Generic Design and Safety Case (Ref. 14)
- RO-UKHPR1000-0052, Design and Safety Case for Class 1 and 2 Human Machine Interfaces Employed in the Main Control Room and Remote Shutdown Station. (Ref. 15)

4.2 Human Factors Integration

57. ONR's SAP EHF.1 sets the expectation that there should be a systematic approach to integrating HF within the design, assessment and management of systems and processes applied throughout the facility's lifecycle.

58. Fundamental to the effective and proportionate consideration of the limitations and capabilities of the human within the design, is a HFI programme. It ensures that HF is properly considered, and hence contributes to the principle of ALARP. Throughout my assessment, I place significant reliance on the efficacy of the HFI process as it gives confidence that HF has been appropriately considered throughout the design.

59. ONR's expectations within this area are set out within 'NS-TAST-GD-058 (Rev 3) Human Factors Integration' (Ref. 4). These expectations can be summarised as the RP (or licensee) demonstrating suitable and sufficient processes and arrangements in the following areas:

- The capability of the organisation / HF team
- The scope of HFI
- Technical programme
- Managing issues and assumptions
- Operational experience
- Standards, codes, and methods – discussed in the relevant sections to which they apply.
- Concept of operations' (Ref. 11) – assessed at Step 3 and found to be acceptable.

4.2.1 Assessment of The RP's Human Factors Organisational Capability and Capacity

60. ONR's SAP, EHF.8 and EHF. 11 set the expectation that there will be sufficient SQEP HF resource delivering the relevant HFE and safety analysis work.

61. At the start of GDA, the RP's HF capability numbered four HF Suitably Qualified and Experienced Persons (SQEP) with a strong focus on Control & Instrumentation (C&I) and Human Machine Interface (HMI) design. I judged this to be insufficient to deliver the necessary scope of HFI required to meet regulatory expectations for GDA. The quality shortfalls in the initial submissions underpinned this judgment.

62. This led to 'RO-UKHPR1000-0011 Human Factors Capability and Integration to Deliver the GDA of UK HPR1000' (Ref. 16) being raised to highlight the need to address this shortfall. It also provided a more detailed set of regulatory expectations in this area to aid the RP in developing its capability.

63. The purpose of this RO was to seek an improvement in:

- Capability, with respect to understanding regulatory expectations for HF.
- Capacity to service the HFI programme necessary to meet the expectations for GDA.
- The scope of HFI beyond the C&I discipline into all relevant safety analysis and engineering disciplines.

64. The RP responded positively to this RO and took the following steps over the course of GDA to address the shortfalls against expectations:

65. The response by the RP can be summarised (Ref. 17) as follows:

- Developed an organogram setting out the composition of the HF team and its organisational hierarchies to demonstrate that the HF team has meaningful decision-making authority over the GDA design.
- Provided information explaining the links between the parties forming the RP, and its HF supply chain.
- Developed 19 role profiles, identifying knowledge and skill requirements for each of the HF roles in the RP and supply chain.
- Developed a comprehensive HF work programme identifying dependencies and critical path to demonstrate there was suitable and sufficient HF resource (internal and external) in place to meet workload demands.
- Supplied its HFI process and technical design change arrangements to demonstrate that HF has been appropriately integrated into the wider engineering disciplines and the design process.
- Developed metrics to track interactions with the wider engineering disciplines to demonstrate that the HFI and design change processes were engaging the HF discipline.
- Increased the HF team capacity and associated personnel from 4 to 78 within the CGN organisation.
- Created a technical support contract framework that secured the services of 18 personnel from UK HF consultancies and individual HF specialist contractors.
- Secured HF specialist training and advice and guidance support from EDF HF specialists.
- Rolled out of a comprehensive HF training programme within CGN, up to and including chief engineer level. At the time of reporting (Ref 17), 339 people had attended this course.
- Established a mentoring programme for non-HF reps within other disciplines, numbering 238.
- Establishing HF champion roles within interfacing disciplines to improve HF integration with other disciplines.
- Introduced detailed templates for HFE design reviews and HRA to maximise consistency and improve quality.

66. The introduction of these measures during GDA were sufficient to resolve RO-UKHPR1000-0011. As a result of this work, I observed a continuing improvement in the quality of HF deliverables and the scope of influence on the design by the team. The details of this form the majority of my assessment below. However, whilst quality has continuously improved, I note that at the end of GDA, the RP is still reliant on UK contract support and regulatory advice and guidance to consistently meet regulatory expectations within its GDA submissions. I have therefore encouraged the RP to continue their in-house development of HF capability to mitigate this particularly as this improvement will need to be maintained to support any future site-specific activities.

4.2.2 Assessment of The Scope and Planning of HFI

67. At Step 3, the RP demonstrated across its submissions that it understood the wide-ranging scope of HFI needed to complete a meaningful GDA. This was evidenced clearly in the HFIP. My judgement did not change during Step 4.

68. For Step 4, the RP developed a detailed technical programme that was modelled to a suitable task level, showing the critical path and resources. I consider this drove a significant improvement in the ability of the RP to increase its internal and external resource and was critical in delivering the necessary work for GDA. I commend the ability of the RP to bring this level of resource to bear in order to maintain the delivery schedule.

69. However, whilst I consider this was crucial to success, it was needed from the start of GDA, as the HFI programme delivery schedule was back-end loaded and I consider

the time pressures faced by the RP were a factor in the variable quality of the submissions. It was also a factor in securing the necessary resource and capability, which again was late in the GDA, and again appears to have been a factor in the quality of some deliverables.

70. Had such a planning approach been undertaken earlier in GDA, I consider that the suite of HF submissions would have been better integrated, more appropriately sequenced (e.g. AoF work preceding the HRA work), be of higher quality, and have a higher level of utility for future users. I raise this point to highlight the importance of early planning and capability and capacity development in the detailed design and site-specific stage.

71. Given the demonstrable benefit of the RP's HF programme, and ONR's learning from previous licensing and large permissioning activities, I consider it necessary for the licensee to have in place a suitably detailed HF programme during this time. I therefore raise the following Assessment Finding.

AF-UKHPR1000-0084 – The licensee shall develop a resourced Human Factors Integration Plan to deliver the Human Factors related elements of the detailed design and safety case. This should include, but not be limited to:

- Justifying the Human Factors activities at the team and deliverable level.
- Developing a detailed resource loaded programme showing the dependencies between activities and deliverables, including non-Human Factors activities.
- Justifying the processes that ensures that the programme remains updated, integrated, informs work activities and underpins the development of the site-specific safety case and detailed design.
- Demonstrating the graded approach for the integration of Human Factors Engineering across the entirety of the engineering, operational, and organisational design. The approach should recognise the need to integrate work from a wide range of stakeholders

4.2.3 Assessment of the Use of Operational Experience

72. ONR expects (SAPs EHF.10, EPE. 5, and AV.8) that OPEX be considered in the design and operation of new and existing nuclear power stations.

73. The RP's 'Operating Experience Feedback Review Summary Report' (Ref. 18) sets out a description of how OPEX was surveyed and collated, how it was fed into the design and assessments, and a summary of the key OPEX findings. It notes that the principal objective of the OPEX review is to ensure that shortcomings of the previous plant design can be avoided, and the good practices can be kept for the new plant design. It claims that the review process is ongoing. As a consequence of these objectives, I also expect to see OPEX used to support the identification of shortfalls, in addition to supporting the design changes that will avoid them.

74. The 'HRA Summary Report' (Ref 10) claims that OPEX was used to inform the identification of HBSCs and their assessment, although this objective is not clearly stated in Ref. 18.

75. To achieve these objectives, I expect the RP's OPEX reviews to be wide-ranging. They need to be current, i.e. take account of the most recent OPEX reasonably available, and they need to consider lessons that can be learned beyond the specific systems from which individual items of OPEX are obtained. This includes examination of

systems that are similar in concept to those applied in the nuclear context, but which are in use in other domains. Furthermore, to meet the objective of sustaining good practices to carry forward into new plant design, OPEX reviews should, ideally, consider successful performance, rather than focusing solely on past failures. This last aspect can be challenging, as few systems for recording OPEX are optimised for recording why arrangements have been successful.

76. The review process applied by the RP is set out in Reference 18. It comprises a structured process for gathering OPEX and for assessing its relevance and significance. The principal focus appears to be associated with identification of potential improvements, e.g. “The operating experience feedback review aims to ensure the shortcomings of the previous plant design can be avoided and the good practices can be kept for the new plant design”. A screening process is described after which the issue is allocated to one of three categories (corporate-level, project-level and operation-level). The resultant issue and any analysis is entered into the CGN engineering experience feedback system together with identified actions. This aligns with my expectations for a system that will support design improvements. However, it does not present an explicit link to HRA.

77. I note that some of the OPEX source data are relatively old (e.g. NUREG/CR-6400 dated 1997). More recent OPEX from specific operating stations is also cited. However, I note that much of the cited OPEX comprises design shortfalls (e.g. ‘mode regulation for main control room lighting is complex and difficult to be performed…’). Whilst this is valuable with respect to identifying potential human engineering enhancements, it does not provide comprehensive information concerning human performance, human reliability and human error. However, I note that the challenges associated with doing this as it is reliant on the quality of the original OPEX data, which is not always well supported by detailed HF analysis.

78. My TSC assessed several of the database entries cited in Ref. 18. They illustrate how issues have been recorded, investigated, and passed on to the design process. However, it is unclear how the database can be searched and, specifically, the extent to which generic issues arising in a particular system can be extrapolated to other systems. For example, a database item (Appendix 4 Item 4-26) concerns restricted space for maintenance of electric heaters, with the recommendation to consider this issue during design. It is unclear whether this issue remains aligned solely to the design of the particular heater, or whether it is flagged more generically against design for maintainability for all systems.

79. I am pleased to note that the RP clearly recognises the need for, and the benefits of, carrying out OPEX reviews to inform the design and safety analysis programmes. I return to the topic of OPEX in later sections to discuss the specific strengths and weaknesses in each area:

- 4.3 – Assessment of the RP’s approach to allocation of function
- 4.4.2.1 – Assessment of the Fangchenggang 3 (FCG3) baseline design analysis
- 4.4.2.4 – Lifecycle scope of HFE
- 4.5.2 – Qualitative assessment and substantiation of HBSCs
- 4.5.3 – Quantitative human reliability assessment

80. Whilst the recognition of the importance of learning from experience is positive, I consider the identification and learning from OPEX incomplete at the close of GDA. I am pleased to note that the RP recognises this itself and proposes a FAP action to ensure this is resolved by the licensee during detailed design:

81. The action guides the licensee to undertake further work in this area including learning from the use of the simulator for design testing and training, as well as the expansion in scope to consider learning from the ongoing design, build and operation of the reference plant. I agree with this expectation. To ensure suitable regulatory oversight and influence over this commitment I raise AF-UKHPR1000-0085 on OPEX.

AF-UKHPR1000-0085 – The licensee shall develop the Human Factors operational experience review undertaken during GDA to support the site-specific safety case and underpin the substantiation that the detailed design reduces risk to as low as reasonably practicable. This should resolve the shortfalls identified during GDA, including, but not limited to:

- Reviewing feedback from wider sources to ensure learning opportunities are included.
- Developing a process to capture learning from experience.
- Capturing learning from the reference plant as it moves through design, build, commissioning and operations.
- Capturing learning from relevant simulators on human performance data.

4.2.4 Assessment of the Management of Human Engineering Deficiencies and Assumptions

4.2.4.1 Management of Human Engineering Deficiencies

82. ONR expects (Ref. 4) that the RP establishes a suitable and sufficient process for the identification and resolution of Human Engineering Deficiencies (HEDs)

83. The RP acknowledged that HEDs were not reliably tracked during Step 1 and 2 of GDA. For Step 3, the RP established a system for tracking both HEDs and assumptions – for future validation. I also identified that there were problems with the organisational reach and agency of the HF team within the wider CGN organisational structure and thus raised RO-UKHPR1000-0011 as discussed above. The key improvement in relation to the effective management of HED was HF becoming formalised as a key stakeholder in the design change process. This meant that the HF discipline had a more effective route to influence the design with respect to HFI. However, as I discuss in the HFE section in more detail, this was not without some challenges. Specifically, whilst the design process included HF specialists it only did so on an as required basis when judged appropriate by system designers; even then, involvement was only in a review capacity. This potentially limited the opportunity for HF specialists to genuinely influence the iterative design process.

84. HED and design and operational assumptions are managed and sentenced via the ‘HF Issues Tracking System (ITS)’. The RP’s intention is to hand this database over to the licensee as part of the suite of site-specific stage documentation. As this database was in Chinese, I was not able to assess the adequacy of the database with respect to information content.

85. I therefore focussed my assessment effort in determining whether there was evidence that HF Issues were being proactively identified and suitably resolved.

86. To demonstrate the efficacy of this system, the RP produced a summary report to demonstrate effective HFI during GDA (Ref. 17).

87. By the end of March 30th, 2021, the RP's HF team had assessed and was involved with the sentencing of 168 Technical Change Notes. 12 design improvements were made based on 15 HED identified by the HF team in the:

- HRAs
- AoF work
- HF review of SSCs design and RGP identification and application work.

88. 20 design improvements were proposed by other non-HF disciplines based on identified HED.

89. From this, it is clear that these were not cursory interactions with other disciplines as the HF work has informed a number of meaningful safety improvements to the generic UKHPR100 design. For example, the HRA work identified that there was insufficient time to re-energise the valves used for the in-vessel retention feature to work. This led to a design change to be able to remotely re-power the valves from the MCR. Another example identified was the lack of time available to cross connect the emergency feed-water (ASG) tanks in a loss of coolant scenario. Several automatic and manual solutions were assessed in a multi-disciplinary workshop which assessed the HF benefits, effects to safety case, and cost to change.

90. I discuss some of these later under the HFE and HRA sections (4.4 and 4.5) of this report, but in summary, it is clear from the submissions that most analysis reports include a specific section on assumptions, HED and recommendations. In earlier reports, the detail can be somewhat lacking, but I noted a clear improvement trend throughout GDA.

91. I had my TSC assess this documentation and they found its quality to be variable in nature. As a result, it makes it difficult to systematically track and manage the effective close out of the changes. I also note that it has sometimes been difficult for the RP to judge what level of detail is both necessary and helpful for a third party – be that the licensee or the regulator. An example of this is the AoF work where the decision-making criteria in relation to the acceptability of recommendations can lack transparency. Whilst I do not consider it prejudicial for GDA, it does weaken the ALARP case.

92. I therefore raise Assessment Findings AF-UKHPR1000-0086 and AF-UKHPR1000-0144 to ensure that comprehensive and transparent records are kept of the HED resolution process as the design progresses during the site-specific stages.

AF-UKHPR1000-0086 – The licensee shall demonstrate that the Human Factors shortfalls and Human Engineering Deficiencies identified during GDA are resolved. This should include sentencing, documenting and ensuring that the Human Factors requirements are implemented in the site-specific safety case.

4.2.4.2 Recording of Analytical and Operational Assumptions

93. ONR expects (Ref. 1) that: "…assumptions in, the safety case have been clearly identified and can readily be captured in:

- (a) technical specifications;
- (b) maintenance schedule;
- (c) procedures (normal operation, emergency, accident management);
- (d) training programmes;
- (e) emergency preparedness;
- (f) operating limits;
- (g) radiation protection arrangements for operators;

- (h) lifetime records;
- (i) commissioning requirements, etc."

94. In my wider assessment of the RP's submissions, and those performed by my TSCs, I have confirmed that assumptions in relation to design features, plant performance or future operational details have been recorded. I note that the RP improved its performance in this area as the GDA progressed. This was also the subject of RO-UKHPR1000-004, reported in Ref. 19.

95. However, within even the latest submissions it was still possible to identify some tacit assumptions that have not been formally identified. I do not consider this prejudices the viability of the generic UK HPR1000 design as they typically relate to organisational factors or specific HMI features, neither of which is designed yet.

96. I welcome the fact that the RP has recognised this in its FAP for resolution during detailed design by the licensee.

97. However, these commitments assume that the process of assumption identification has been highly reliable throughout the GDA and I do not consider this to be the case. I consider it necessary for the licensee to do its own review of the HF documentation to assure itself that no tacit, yet critical, assumptions are omitted during site-specific stages. I therefore raise Assessment Finding AF-UKHPR1000-0144 to capture this.

AF-UKHPR1000-0144 – The licensee shall, as part of detailed design, demonstrate that a complete set of Human Factors related assumptions underpinning the design and safety analysis is identified. This should include reviewing the early documentation produced during GDA.

4.2.5 Strengths

- The RP has demonstrated a significant and impressive increase in HF capability, capacity, and reach over the course of GDA; growing the wider HF team within he Chinese General Nuclear (CGN) organisation from 4 to 78 over the course of the GDA.
- The RP has effectively utilised its supply chain and technical partners to improve its knowledge and understanding of RGP and regulatory expectations in HF, although further improvements will be needed during site-specific stages.
- The RP has been able to effectively plan a wide-ranging and technically complex programme of HFI. This was supported by a detailed and resource loaded programme of work, specified at an appropriate task level spanning all areas of what I would consider an adequate HFI scope.
- The RP has demonstrated that it has suitable understanding the limitations of HFI during GDA and demonstrated a conceptual understanding of what will be needed during site-specific stages. It has also performed an honest appraisal of those areas which will need improvements during detailed design, via its production of the 'FAP' (Ref. 6), which I commend.

4.2.6 Outcomes

- The RP carried out sufficient organisational and planning improvements for me to close RO-UKHPR1000-0011 *Human Factors capability and integration to deliver the GDA of UK HPR1000*. My assessment of the improvements can be found in Ref. 20 RO Closure Statement.
- However, there were a number of shortfalls against regulatory expectations and thus I have raised 4 Assessment Findings to address these HFI related shortfalls.

4.2.7 Conclusion

98. I consider the RP has met the scope and management expectations set out in ONR's 'HFI' TAG (Ref. 4) sufficient for the purposes of GDA.

99. Although starting from a low base, the RP was able to secure additional resources to both directly carry out analysis work, deliver training, and develop prescriptive methods to improve the quality of submissions over the course of GDA. I welcome that the RP's HF team was also able to significantly improve the reach and agency of the HF team over the course of GDA; growing from a largely C&I based function to one with links into the wider safety analysis and design functions. It also secured a formal role in the design change process which I welcome.

100. However, adequacy in HFI was achieved late in GDA. The result, at times, has been that submissions have been:

- Mechanistic in nature, which do not always demonstrate a comprehensive understanding of the purpose and use of a modern standards safety case.
- Not sufficiently integrated resulting in a failure to fully demonstrate risks are reduced ALARP. This is not to say they are not, simply that it can take a lot of effort to piece together the evidence from the suite of submissions, reducing the utility of the safety case for future users.
- Sometimes lacking in coherency even after multiple revisions.
- Variable in adequacy when it comes to formally capturing underpinning assumptions.
- Sometimes lacking in transparency when it comes to fully articulating the design change decision making process, sufficient to be useful should decisions need to be revisited by the licensee.

101. I therefore raise four Assessment Findings to capture and address the shortfalls above.

102. Overall, I am content these shortfalls do not undermine the adequacy of the generic UK HPR1000 design.

4.3 Assessment of the RP's Approach to Allocation of Function

103. ONR expects (Ref. 2) that: "When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated."

104. AoF is a fundamental process within complex systems design and is done by systematically considering identified capabilities and limitations of humans and technology and their relative failure likelihoods separately or jointly in delivering a function. This is done with the aim of producing an optimal design solution for function delivery and thereby minimising failure risk to ALARP.

105. Given the importance of demonstrating an optimized AoF in substantiating the fundamental viability of a reactor design, I have focussed particular attention to this area of my assessment. In support of my assessment, I engaged a TSC to conduct an independent review of the RP's analysis in this area. My assessment is based on the RP's submissions and the independent TSC review.

106. To form a judgement on the suitability and sufficiency of the RP's AoF process and outcomes for the generic UK HPR1000 design, my TSC assessed three principal submissions:

- Pre-Construction Safety Report Chapter 15 Human Factors (Ref. 3)
- Function Allocation Methodology (Ref. 22
- Allocation of Function Review Report (Ref. 25)

107. My TSC's assessment of the RP's AoF process, specifically considered the following aspects of the method:

- Suitability of the AoF Method
- Application of the AoF Method
  - Assumptions underpinning the AoF analysis.
  - Automatic to controlled state allocations
  - Automatic to safe state allocations
  - Manual to controlled state allocations
  - Manual to safe state allocations
  - Manual local-to-plant allocations
  - Severe accident allocations

4.3.1 Suitability of the AoF Method

108. The generic UK HPR1000 design is claimed by the RP as an evolutionary design of NPP, thus has inherited an existing function allocation. Accordingly, the RP has applied their allocation function process to the reassess the pre-existing allocations from the reference design.

109. The method provides a clear overarching algorithm depicting a five-step process. The five steps comprise:

- Step 1 - Function Characterisation
- Step 2 - Predominant Automation Allocation
- Step 3 - Predominant Manual Allocation
- Step 4 - Detail Assessment:
  - Shortage of Time
  - Situational Awareness
  - Extreme Environmental Conditions
  - Complex Diagnosis or Decision Making
  - Function validity for operational modes
  - Error correction difficult
- Step 5 - Validation and Trade-Offs

110. The AoF process is applied to the nuclear safety functions as described in the Generic UK HPR1000 design Fault Schedule (Ref. 21), thus ensuring a meaningful and risk informed analysis.

111. The five steps are followed to initially determine a basic AoF level and then to refine the AoF decision with respect to one of 7 automation levels described below. The final step is one of validation of the AoF decision.

112. My TSC considers that the overall structure between steps and within steps recognises the need for iteration in situations where infeasible or ambiguous outcomes might arise. AoF can never be a 'one-shot' process and iteration is invariably required in practice.

113. Each of the five steps is further described in more detail by means of its own algorithm and descriptive text. My TSC examined each of these algorithms and found them to be clear in their depiction and, given the constraints that only a very few words can be used in the diagram, particularly noted that the succinct phrases used are clear in their intent.

114. In addition to the final checking step depicted in their algorithm, a further step exists outside the algorithm for the informed review of function allocation outcomes. My TSC considered this additional step in its assessment of the method as applied in practice.

115. The process provides for three pathways through the algorithm for considering human – automation integration which are: where the function is predominantly automated; where the function is predominantly implemented by the human, where no predominant allocation between human and automation exists. Therefore, the method allows for hybrid solutions to function allocation.

116. The process acknowledges three forms of functionality that can be fulfilled by the human or automation as follows: information acquisition; information processing or decision-making; and the execution of control actions upon the plant to implement those decisions based upon the information acquired.

117. Each of these three forms are further categorised into seven different levels of automation. These capture the AoF outcomes. These are described below.

118. Information Acquisition Automation Level:

- Operator monitors parameters directly from source without any automated assistance.
- Automation provides a range of relevant information for the operator to review which may include an alarm for the underlying failure.
- Automation proposes and prioritises relevant information for the operator to review and accept.
- Automation monitors conditions and gives operator a limited opportunity to review and accept.
- Automation may alert operator that conditions are being monitored at different phases of the function and will always alert the operator that the information is correct or that it could be incorrect. Automation manages all data acquisition.
- Automation acquires all necessary information, monitors conditions and only makes operator aware if the information could be incorrect.
- Automation monitors conditions but does not share this with the operator.

119. Information Processing and Decision-Making Automation Level:

- Operator assesses values and trends to make a decision directly from source with no basic assistance from automation.
- Operator assesses basic trends and values provided by the automation to diagnose the problem and make a decision.
- Automation proposes and prioritises analyses/diagnoses and associated strategies for the operator to review and select from.
- Automation presents result of the analysis and makes a decision based on a diagnosis, giving the operator a limited opportunity to validate and challenge if needed.
- Automation may alert operator that data analysis is performed prior to and during information analysis and decision-making. Automation will always inform the operator once a diagnosis and/or decision has been made. The operator does not intervene.
- Data analysis and decision making is undertaken and information is made available to the operator.
- Data analysis and decision-making is undertaken by automation without informing the operator.

120. Execution Automation Level:

- Operator selects procedure and initiates any action manually without any support from automation.
- Automation provides enhanced assistance allowing for remote operation of simple actions (e.g. starting a pump or sequencing).
- Automation will fully execute the function but only with operator approval.
- The operator has a limited opportunity to make a positive response to prevent the proposed action before it is fully undertaken by automation.
- Automation may alert operator that process is performed prior to and during execution. Automation will always inform the operator once the process has been achieved or has failed. The operator does not intervene.
- Automation initiates its proposed response and only makes information available to the operator if the function has failed.
- Automation initiates its proposed response. Operator is not directly informed that the function has been undertaken.

121. My TSC considers these broadly align with various automation taxonomies that have been proposed in other industries. The guidance supporting the overall algorithm addresses important HF deficiencies that can affect human performance and reliability such as situation awareness, cognitive complexity, and workload. Accordingly, it appears to meet the expectations for analysis set out in SAP EHF.5 for task analysis in paragraph 450.

122. The text description of the algorithm and its contents is complex. However, the overall structure of the document makes a potentially complex process clear in its depiction and description. My TSC therefore considers that the overall process the RP has developed is systematic and clear in accordance with the expectations set out by EHF. 2 and the TAG for AoF (Ref. 4).

123. Further, my TSC considers that the process offers a better solution to the AoF problem than previous, older, Fitts' list type analytical tools as it goes considerably beyond the simple binary outcomes delivered by these methods. It offers more sophisticated and graded AoF outcomes which are necessary given the range of automation options provided by current C&I technologies.

124. The RP confined its scope of AoF analysis to function delivery in important post-fault primary lines of defence. The high degree of automation in preceding PWRs is reflected in a predominance of already automated functions. The (unsurprisingly) few recommendations (nine) for change during the detailed design concern further automation to deliver a function (six cases) and the re-classification of equipment involved in functions from FC2 to FC1 (three cases) of some equipment. One recommendation advises reclassification and automation.

125. My TSC concluded that for post fault primary lines of protection in the generic UK HPR1000 design, the evidence from the RP's analysis shows that human involvement in function delivery is now excluded to the extent reasonably practicable with current automation technology.

126. There are however limitations in the scope and substantiation of the RP AoF submissions.

127. Where AoF analysis determines that allocation remains with the human in post fault primary lines of protection, it is because it is too complex to automate. My TSC's expectation was that this would then feed into the HRA programme for substantiation, but this was not always evident. Too difficult to automate does not mean that the function can be credibly delivered by the human. Such a demonstration should include task analyses and should make reference to specifically relevant OPEX e.g. derived from simulator post-fault studies where practicable.

128. The lack of clear integration is a shortfall, but one explicable by the AoF analysis being performed late in the GDA process and outside of the HRA programme. It is a shortfall that the RP is aware of one that will need to be addressed during site-specific stages. I therefore raise AF-UKHPR1000-0145 which includes update and integration of the processes moving forward and a requirement to demonstrate that safety important functions allocated to the human are feasible and can be performed to the required level of reliability. It also addresses several other shortfalls discussed below.

129. This, and subsequent shortfalls discussed later, are sufficient to raise the following AF.

AF-UKHPR1000-0145 – The licensee shall, as part of detailed design, demonstrate that the allocation of function analyses addresses all necessary safety significant functions. This should include, but not be limited to:

- Ensuring the work to address this Assessment Finding is integrated to avoid design foreclosure.
- Ensuring the output links to, and informs, the human reliability analysis and substantiation of human based safety claims.
- Demonstrating that those functions identified as too complex for automation, can be delivered by the human to the required level of reliability. Where this is not the case, further analysis should be undertaken to establish that risks have been reduced to as low as reasonably practicable.
- Ensuring that diverse functions, emergent functions, severe accident, and non-reactor safety functions, are addressed.
- Ensuring that the allocation of function decision making, up to and including design changes, is appropriately documented.

130. My TSC found that the scope of the RP's AoF review has been confined to functions in the 'Main protection line' and thus excludes instances where the function is claimed as a diverse line of protection. This situation is at odds with the process outlined in the methodology document (Ref. 22) which states "The feasibility of human undertaking a function as backup should be assessed as a part of a separate allocation function assessment".

131. This represents a shortfall because on a highly automated design, the human plays an important role in providing additional and diverse defences against technological failures. However, I am pleased to note that the RP recognises this in its FAP HF-AOF-08: AOF review for the diverse manual functions.

132. My TSC noted that the RP's method has also not considered normal and diverse safety functions. It argues that such functions are considered within the engineered systems rather than at the level of goals, subgoals or safety functions that they consider these to make no meaningful contribution to AoF. I do not consider this a valid claim as it assumes, and relies upon, significant HF knowledge in the area of AoF on the part of the designers and automation decisions are necessary in areas of the plant such as fuel route.

133. I therefore included within AF-UKHPR1000-0145, the requirement to ensure that the licensee does not ignore the AoF considerations relating to normal and diverse safety functions.

134. I note that the AoF process was performed late during GDA, and is not complete at the close of GDA. As AoF is a key input to the early stages of the design process, this poses a risk of late design changes during the site-specific stages. As the FCG3

design is evolutionary, I do not consider this a significant risk. I have therefore included the requirement for this as part of AF-UKHPR1000-0145.

135. To conclude, overall, I judge that the RP's method fulfils the expectations set out by SAP EHF. 2 and the TAG for AoF (Ref. 4).

136. The detailed algorithmic structure manages the potential complexities in the interactions between the different sets of considerations and this makes a potentially powerful method.

137. I consider that the method, if applied as described, offers improvements over existing – and largely outdated – methods as represented by US NRC and IAEA documents (Refs. 23 and 24). The method has brought the increased capabilities of automation relative to the 1980s and 90s, as represented by the US NRC and IAEA documents, into the modern era. The method has the potential, in respect of the AoF arguments, to support the RP's safety case claim 3.3.8 that "Human Factors have been appropriately taken into account in the design, assessment and management arrangements, to meet the relevant safety requirements."

4.3.2 Application of the AoF Method

138. My TSC found that the RP's AoF analysis effectively capture the assumptions used to underpin the AoF analysis. The validity of such assumptions will need to be validated during the site-specific stages and any changes considered against AoF decisions. I assume this will be addressed as part of normal business as it raised in the FAP for the licensee (FAP item 26).

139. To gain confidence in the application of the RP's AoF method my TSC assessed a sample of the AoF decisions relating to the following AoF types from Revision A* of Ref. 25:

- Automatic to controlled state allocations
- Automatic to safe state allocations
- Manual to controlled state allocations
- Manual to safe state allocations
- Manual local-to-plant allocations
- Severe accident allocations

140. The RP's analysis of the automatic to controlled state assignments demonstrates pre-existing automation to be credible within the context of GDA. It considers a total of 73 Safety Functions. The RP's analysis of the automatic to safe state (and final state) assignments demonstrates pre-existing automation to be credible. It considers a total of 3 Safety Functions. The RP's analysis of the manual to controlled state demonstrates pre-existing manual allocation to be credible within the context of GDA. It considers 7 Safety Functions.

141. The RP's analysis of the manual to safe state fails to fully substantiate the credibility of the human actions associated with the safety function. It considers 28 Safety Functions. This is because the AoF method does not integrate with the HRA, nor does it include provision for detailed HRA within the method itself. This is part of AF-UKHPR1000-0145.

* *The RP subsequently issued revision B of the AoF analysis report. It considers additional functions but does not meaningfully alter my assessment conclusions.*

142. However, it does offer some limited confidence as the method guides the user to consider several relevant Performance Shaping Factors (PSFs) when determining the AoF, such as the impact of cognitive and physical tasks.

143. The RP's analysis of the manual local functions state demonstrates pre-existing manual allocation to be credible within the context of GDA. It considers 2 safety functions. The RP's analysis of the manual functions for severe accidents demonstrates pre-existing manual allocation to be credible within the context of GDA. It considers 5 safety functions.

144. The outcome of the RP's analysis includes the following recommendations for changes to AoF during detailed design:

- Due to the shortage of time for isolation of the emergency feedwater system (ASG-FFR-01-M11) in the most onerous scenario, It is recommended that complex automation is applied to support diagnosis.
- The function, isolation of the water intake pipeline of the Chemical and Volume Control System (RCV) charging pump from VCT and hydrogenation station, is currently FC2, which is inconsistent with the design rule that manual functions to reach a controlled state should be classified as FC1. A design modification is proposed to automate this function.
- A similar recommendation was made for the medium head safety injection system (RIS-FFR-19-M11). It was recommended that the classification be increased to FC1 and design change (to be considered during detailed design) such that MHSI injection is triggered manually and will initiate the Medium Pressure Rapid Cooldown (MCD) function automatically.
- Automation of the containment spraying (cooling) function was recommended.
- Automation of the emergency boronation system was recommended.
- Automation of the target value control for the Atmospheric Steam Dump System (ASDS) was recommended.
- A change from local manual to remote manual to re-energise the In Vessel Retention (IVR) valves was recommended.
- A change from local manual to remote manual for the operation of containment venting was recommended.
- A recommendation for further analysis on the functions excluded from the main protection lines because of the updating of the Fault Schedule was made.

145. I consider these recommendations to be conceptually appropriate, and in keeping with iterating the design to an ALARP position as they offer clear safety benefits to the design. However, it is important that the licensee consider these recommendations holistically, i.e. reducing task difficulty / complexity for one task may inadvertently increase it for other dependent or related tasks.

146. However, my TSC found a lack of transparency or clear justification to support the RP's sentencing of recommendations arising from the AoF process. My TSC explored this shortfall via RQ-UKHPR1530 AoF Review Assumptions and Recommendations but the RQ response failed to provide the additional clarity necessary. As the scope of the AoF analyses undertaken by the RP is not yet complete there may well be future AoF analyses that lead to further recommendations and an improvement in sentencing transparency is required.

147. Overall, I consider that the RP has sufficiently demonstrated (for GDA) that the reference design broadly meets the engineering hierarchy expectations within ONR's SAPs. The design minimises the responsibility of the human to directly intervene following a fault, and it has provided evidence that the analysis has demonstrably influenced the design to further reduce risk in line with the principles of ALARP.

148. There are, however, limitations in the scope and substantiation of the RP AoF submissions.

149. My TSC observed that where AoF analysis determines that allocation remains with the human in post fault primary lines of protection, it is because it is too complex to automate. Whilst the RP's AoF process also determines whether the action is beyond the capabilities of a human and requires redesign of the means by which the safety function will be achieved if this is judged to be the case, it is not always apparent that the RP has undertaken the necessary HF analysis to substantiate that the fulfilment of functions that are too complex for technology are feasible for the human in the fault context in which they will need to be delivered as part of the existing HRA. Whilst the RP could reasonably argue that this could be done, the need for this is not recognised by the RP as an explicit FAP item. I would expect explicit links between the HRA and the AoF process and these are not always present. The AoF process should be a direct input to the HRA process, or at the very least have its own programme of subsequent task substantiation. This is not captured in the RP's FAP. This is part of AF-UKHPR1000-0145.

150. The RP has excluded from their scope, AoF analyses for diverse lines of protection in post fault scenarios where the human is more likely to have a role in implementing functions. For the safety case to demonstrate that these lines of protection are effectively delivered by human actions, AoF analyses of human involvement are required. I welcome that the RP recognises this shortfall in its FAP and has made a commitment to apply its AoF method to these functions.

151. Whilst the role of humans in severe accidents has been analysed the results reported are confused and inconclusive. As the severe accident response is largely out of scope for GDA, I consider this acceptable, but it will need to be revisited during the site-specific stages. I consider this can be addressed via Assessment Finding AF-UKHPR1000-0145.

152. The RP has also excluded from their AoF scope, the analysis of situations where a human failure to fulfil a function may lead to a latent failure, i.e. one which is only revealed when a demand is made, in safety-related equipment. Such functions would arise in test, calibration or maintenance. This is important not only because the safety case would not be complete without it but also because there are now increasing levels of automation in the shape of information technology being proposed for use in test calibration and maintenance tasks.

153. The RP has further excluded from their AoF scope, situations where a human failure to fulfil a function may initiate a revealed failure at that moment or shortly thereafter. For example, where the pre-configuration of protection is required in the operation of the reactor crane or other routing or in the fuel route.

154. Accordingly, I conclude that an expansion on the scope of AoF analysis is required to ensure that the proposed mix of human and automation is appropriate for functions involved in diverse lines of protection, test, calibration and maintenance or protection pre-configuration and severe accident response. I therefore included within AF-UKHPR1000-0145 a requirement to widen the scope of AoF analyses post GDA.

155. My TSC noted that the sentencing of recommendations from the RP's AoF analyses appeared to be logically inconsistent and the justification/explanation not always clear, the process of sentencing not always clearly described and there no demonstration that the sentencing outputs meets the ALARP principle. Therefore, I conclude that greater transparency is required in the sentencing process and include this requirement as part of AF-UKHPR1000-0145.

4.3.3 Strengths

156. The AoF method provides a clear overarching algorithm depicting a five-step process. This is supported by clear descriptive text. I am pleased to note that the overall structure between steps and within steps recognises the need for iteration in situations where infeasible or ambiguous outcomes might arise.

157. The guidance supporting the overall algorithm clearly addresses important HF deficiencies that can affect human performance and reliability such as situation awareness, cognitive complexity, and workload. Accordingly, it appears to meet the expectations for analysis set out in SAP EHF.5 for task analysis.

158. I therefore consider that the AoF process the RP has developed is systematic and clear in accordance with the requirements of EHF. 2 and the TAG for AoF (Ref. 4).

159. This overall structure is intended to be applied to functions described within the fault schedule (Ref. 21). Accordingly, I consider that the information fundamentally input to the process ensures that the overall AoF process I have assessed is suitably linked to matters involving nuclear safety. This meets the requirements of EHF 2 for AoF.

4.3.4 Outcomes

- The RP developed a best practice methodology for determining AoF for nuclear safety functions for GDA.
- It demonstrated the methodology via limited practical application.
- Within the limitations of GDA, and limited by its late application, it demonstrated the AoF of the generic UK HPR1000 design.
- During the course of my assessment, I identified a number of AoF shortfalls against regulatory expectations, which are the subject to a single Assessment Finding AF-UKHPR1000-0145. This finding was raised to address:
  - The lack of completeness of the AoF analysis. I consider focussing on the post fault safety functions sensible given the late application of the AoF process in GDA but the AoF process will need completing during the site-specific stages to demonstrate an ALARP design.
  - The AoF method appears to assume that if the safety function is too complicated to allocate to the technology then it is acceptable for the human to deliver it. This is not a valid assumption.

4.3.5 Conclusion

160. By virtue of it being an evolutionary PWR design, the generic UK HPR1000 design inherits over 50 years of design improvements from previous generations of PWR. Throughout that period safety objectives and increasingly sophisticated automation has progressively allocated more functions to automation for post-fault functions. This is reflected in the predominant number of functions already automated in the RP's AoF studies. The work conducted by the RP raises a very small number of recommendations (for the detailed design stage) for reallocation of function towards further automation and these include local manual to remote recommendations.

161. Therefore, I conclude that for the post fault primary lines of protection for generic UK HPR1000 design, human involvement in function delivery is likely now excluded to the extent reasonably practicable with current automation technology. Additional functions, and human allocated functions, will be further analysed in the site-specific stages under the relevant Assessment Findings.

4.4 Human Factors Engineering

4.4.1 Assessment of Human Factors Engineering Guidance and Methods

162. ONR expects (Ref. 4) that: “HF analysis is consistent with relevant standards and good practices, and applies recognised HF methods. Where novel or unfamiliar analysis methods are proposed by duty-holders, Inspectors should seek assurance of the provenance and validity of those methods to inform nuclear risk assessments and applications. Where ‘in-house’ standards and guides are proposed, assessors should determine their basis and assure themselves of their technical credibility”. This expectation guides my assessment of suitability and sufficiency of the HFE guidance and methods applied during GDA.

163. This section presents the findings of my assessment of the RP’s HF Engineering Guidance and Methods for the generic UK HPR1000 design undertaken as part of GDA.

164. Throughout GDA I have assessed the RP’s HFE submissions but for Step 4 I elected to engage two TSCs to perform independent assessments. One conducted an independent assessment of the adequacy of the HFE guidance and methods and one assessed how effectively this guidance was applied.

165. My assessment, and that of my TSCs, was based on the ‘Pre-Construction Safety Report’ (Ref. 3) and supporting HFE documentation submitted by the RP. My TSC’s assessment focused on the suitability of the guidance materials developed and used by the RP to guide and inform the design of the generic UK HPR1000 design on HF and ergonomic aspects.

166. This section is split into the following sub-sections:

- Overall Approach
- Assessment of the Alignment of generic UK HPR1000 HF design guidance with RGP
- Assessment of the Scope of the HF Design Guidance
- Assessment of the Accuracy and Relevance of HF design guidance
- Assessment of the Usability of HFE Design Guidance

4.4.1.1 Overall Approach

167. The RP produced a set of three HFE guidelines documents to support and inform the application of HF to the design of the generic UK HPR1000 during GDA. These cover control room design, local area design (i.e. local to plant aspects outside of the control room) and HMI design. At a high level, I consider these broad topic areas to be sufficient to encompass the totality of the generic UK HPR1000 design.

168. The PCSR claims that the design aligns with modern good practice. Much of the evidence presented within the guidance does confirm that RGP has been used in the development of the guidance. However, the application, scope, structure and pertinence of the guidance does have some shortfalls. While the guidance addresses a wide range of HF topic areas the evidence to justify that it was comprehensive for the design challenges faced during the generic UK HPR1000 design GDA is insufficient.

169. For example, my TSC found that within the submissions, there is insufficient evidence to substantiate that the guidance was informed by the known and expected tasks to be performed during all phases of operation of the generic UK HPR1000 design or their safety significance (and by inference that of any associated requirements). As such, the adequacy of the guidance offered in terms of it supporting specific tasks cannot be confirmed. This is an important given the RP’s approach of using up-skilled non-HF

designers to ensure HFI via the application of guidance and criteria. This could have been partially addressed by closer integration with the HRA, but this was not evident.

170. Furthermore, they found instances where the guidance offered was evidently not relevant to the NPP context (e.g. the presentation of lighting levels for “retail shops”).

171. However, they did find that the generic guidance did appear to be based on RGP with general referencing to recognised international standards and guidance documents. Unfortunately, the exact source of guidance within the HFE guidelines was not always suitably and/or sufficiently referenced. This potentially limited its utility as it could mean the end user may have struggled to trace sources for additional exposition or context.

172. The form of the guidance may have limited its utility when being applied by up-skilled designers. The presentation was typically narrative, with lengthy sections that discuss and outline topics and the HF design requirements that are pertinent to them. The use of such text is welcomed, as it can provide an easily digestible introduction to the topics covered, however, this presentation style lacks clarity on what the requirements to be applied are. Coupling such text with specific, measurable, attainable, relevant and time-based (SMART) requirements would have provided improved clarity to better allow verification and validation (V&V) to be undertaken at later project stages.

173. Similarly, the guidance occasionally includes options that require designers to make a choice. As the documentation is intended for use by non-specialist HF system designers this is not considered to be prudent, especially where the options are somewhat opaque and contained within more general text as opposed to definitive, criteria based guided choices.

174. Beyond the structure and content of the guidance, it is necessary to consider how it is applied. As defined within the guideline documents, a process was established for their application. The process covered the basic aspects of who was to apply the guidance, how and when. It also defined how design challenges, conflicts and compromises were to be addressed and managed to an ALARP solution.

175. Whilst the design process included HF specialists it was somewhat reactive as it only did so on an as required basis when decided by system designers. Even then, involvement was only in a review capacity. This potentially limited the opportunity for HF specialists to genuinely influence the iterative design process.

176. The noted shortfalls are of concern, however, they do not necessarily prevent a design from emerging from the GDA process that cannot be operated both safely and securely, given that the design is evolutionary in nature and thus is likely to benefit from considerable implicit and tacit learning in terms of safety and security. Section 4.3.2. of this report explores further whether the shortfalls identified in the general application of HFE guidance have resulted in this.

177. I am pleased to note that the RP notes similar weaknesses in the extant design guidance in its FAP such that I am confident that could support the licensee to rectify these shortfalls during the site-specific stages.

4.4.1.2 Assessment of the Alignment of Generic UK HPR1000 HF Design Guidance with International Relevant Good Practice.

178. For a project of the scale of the generic UK HPR1000 design it is essential that a holistic approach is taken to the development and application of design guidance. The RP has attempted to do this through the development of three specific guidance documents (Refs. 26, 27 and 28); this section considers how successful this has been in terms of the alignment of the guidance documents with RGP both within and between the different documents.

179. The design guidance provided within the three key guideline submissions (Refs. 26, 27 and 28) appears to be grounded within a large set of recognised RGP. This is evidenced by the RP's provision of supporting submissions that seek to justify and define the suitability of the codes and standards applied during the development of the guidance. Ref. 29 (Suitability Analysis of Codes and Standards in Human Factors) defines and seeks to justify the RGP that has been applied.

180. Within this document, for each RGP item analysis is provided to summarise the guidance and justify its suitability. Therefore, once suitability is justified it is reasonable that the guidance offered by the item of RGP could be captured and/or referenced within the RP's own guidelines documents.

181. In justifying the inclusion of an item of RGP, the RP employed criteria that explored the applicability of the guidance and its origins. My TSC found that it was apparent from this justification that while the standard set chosen for RGP is international, efforts have been made to localise it by the inclusion of UK specific guidance.

182. In assessing whether an item of RGP is relevant the RP considered whether it has been previously applied during earlier GDAs undertaken by ONR. This inclusion provided some useful context although I consider it is insufficient to fully demonstrate that an item is applicable RGP. Within the RP's justification of RGP status, previous GDA use does appear to be afforded significant weighting.

183. There are several reasons for this. First, I do not consider that the RP can be aware of the exact context and reasoning behind an earlier RP's use of a standard or piece of guidance. The application to an earlier GDA may therefore have an entirely inappropriate context when compared to the generic UK HPR1000 design.

184. Second, the crux of the goal setting nature of nuclear safety regulation in the UK is to avoid prescription and in doing so to place the onus on duty holders (in this instance the RP) to justify the relevance of the RGP it applies.

185. The most recent previous GDA was that of the Hitachi-GE Advanced Boiling Water Reactor (ABWR) which was finalised in 2017; those of the Westinghouse AP1000 and EdF/Areva UK European Pressurised Reactor (EPR) finished Step 4 of the GDA process nearly 10 years ago. These dates mean that it reasonable that RGP may have changed in the interim period.

186. Although much of the guidance offered within the three guidelines documents can be shown to be derived from, and aligned with, the stated RGP, this is not universally the case and instances are apparent where the source of information is indistinct. For quality assurance purposes this is a concern.

187. For example, within the 'TAD' (Ref. 30) three distinct and disparate sources of anthropometric data are referenced yet the actual tables within the document do not confirm the source of the data points to be used. This shortfall is repeated where the information is applied within the HFE guidelines documents (Refs. 26, 27 & 28). In this instance, therefore, I have concerns that the anthropometric data applied to the design has been selected from variable sources to suit a specific need of the RP, I provide further discussion of this in section 4.4.2.6.

188. The lack of specificity on the source of some information within the guidelines is compounded by the hierarchy of guidance sources noted by the RP (see section 4.4.1.3 for further discussion). The inclusion of a hierarchy suggests that criteria and requirements gained from certain sources have greater significance than others. This could have been captured if a more defined and numbered approach to the presentation of guidance and requirements had been used.

189. Furthermore, and driven by the lack of specificity that is often apparent, it is unclear whether some of the quoted references have been used. The wording and structure of the RP's guidelines does not always match my view of the source material and in other instances I am concerned that elements of guidance offered have been reproduced from the original RGP source. This approach raises concern over potential conflict, where information is derived from numerous sources. Such instances, although not overly prevalent, do appear to exist and can be identified by fairly basic presentational anomalies. For example, in the 'Guidelines for Local Area design' (Ref. 28) Figure 3.7-1 uses 4 numeric labels, but in the accompanying text letters are used to refer to these aspects.

190. The use of sections of narrative text could be problematic. Such a presentation style could hinder the traceability of the guidance offered. The use of structured, numbered requirements would more easily allow reference to RGP sources.

191. The guidelines refer to other references for further information. References to general HF literature can be useful for offering additional context or corroborating criteria or guidance. However, given that the guidance was produced to support system designers with basic HF training, I consider that where additional information could have been useful it should have been provided within the guidance rather than referenced to. Referencing to useful additional material can often be a deterrent to its use, especially if the reader does not have ready access to all the source references.

192. In conclusion, I am satisfied that the basis of the HF guidelines developed for the design of the generic UK HPR1000 is drawn from RGP and that the majority of the guidelines can be shown to have been derived from such sources. However, I have some minor concerns over the RP's means and scope of justification for the selection of RGP. I do not consider this to have had a large impact on the RGP sources selected and the alignment of the guidance with those. As has been discussed in relation to the scope of the guidance I am concerned over the traceability of the guidelines to the identified RGP due, in part, to the manner of presentation. It is therefore welcome that the RP has identified the need to update the guidance material during the site-specific stages. The shortfalls discussed above relating to the utility of the guidance could be addressed as part of this update process and I consider this can be addressed as part of normal business.

4.4.1.3 Assessment of the Scope of HFE Design Guidance

193. I would expect suitable HF guidance and requirements to be sufficient to address all key HF topics at a level of detail and complexity that is sufficient both to adequately inform design and to be usable by end users.

194. Based on my TSC's assessment of the RP's guidance documents, it is my judgement that the breadth of HF topics covered by the three guidelines documents (Refs. 26, 27, and 28) is, given the defined scope of GDA, is reasonable for the design of a NPP. However, areas for improvement remain in the scope and certainly the extent of the HF guidance offered to the generic UK HPR1000 designers.

195. My TSC assessed the topic areas covered within the three submitted guidelines documents (Refs. 26, 27 and 28) and considers that between them they have addressed a suitable scope for HFE guidance for NPP design. In reference to the HFE sub-topic areas they identified that all sub-topics are apparent that should be evident in proprietary HFE guidance for NPP design, to a greater or lesser extent. This is despite certain sub-topics identified (e.g. HMI design) being mainly out of scope for GDA.

196. My TSC considered the number of examples of pertinent guidance applied to these different sub-topics. In all cases the source material is numerous.

197. Table 3 below shows the number of examples of discretely pertinent sources of RGP for each of the identified sub-topics that are referenced within the guidelines. It demonstrates a wide-ranging literature review used to inform the development of the HFE guidance.

Table 3: Identification of number of RGP sources references by the RP against identified HFE sub-topics

HFE Sub-topic	Number of referenced RGP sources that address the topic within RP's HFE guidelines
Access and Egress	32
Workstation and workspace design (temporary and permanent)	27
Facility, area and equipment layout and arrangement	21
Control Room design	35
Environment (lighting, temperature, noise and vibration	23
Controls and displays (including communications equipment)	25
Advanced Human Machine Interfaces (HMI) and Human Computer Interaction (note out of scope aspects defined in Section 2.3)	21
Alarms, warnings and cautions	17
Manual Handling	18
Labelling and Signage	22
Working equipment (hand tools, power tools etc)	17

198. In addition to the guidance documents, the RP submitted supporting documentation (Ref. 29) that aimed to justify the scope and extent of HF design guidance applied to the design of the generic UK HPR1000.

199. From this document it was evident that a structured and targeted process was followed in the selection and collation of RGP. The process was hierarchical in nature and considered five distinct levels of source material comprising:

- Level I: Laws and Acts
- Level II: Regulations
- Level III: Approved Codes of Practice (ACoP)
- Level IV: Guidance Documents
- Level V: Codes and Standards

200. It is disappointing that this selection process, as evidenced by statements within the suitability analysis document (Ref. 29), concluded that none of top three levels is applicable to HF.

201. I do not consider this claim valid. At those levels it is perhaps reasonable to claim that there is little that is directly and explicitly related to HF. Although such materials may not explicitly mandate HF activity or requirements there is inference within them that HF is required.

202. Aside from operational and organisational aspects which are out of scope for GDA there is an obvious inference to HF within the design of equipment such as that considered by LOLER and its associated ACoP and this is reflected in the guidance

offered by the RP despite a claim that documents at such levels are not relevant to HF requirements.

203. The overriding principle within UK health and safety law is that risks are reduced to an ALARP position. There may not be explicit reference to HF requirements within UK law (and associated materials) but HF is a significant contributor to achieving an ALARP design and therefore materials at the higher levels of the RP's hierarchy are applicable. I would not expect repetition of direct requirements and clauses from such materials within proprietary guidance, but I would expect the overall ALARP expectation to be evidently writ through them with a defined means as to how compliance with HF requirements would help achieve it. My TSC's assessment did not find this to be uniformly the case within the guidance.

204. Despite this, of the documents identified as being source material for the guidance, my TSC found none which I would not consider to be RGP and as a set they are representative of a reasonable breadth of HF topics pertinent to NPP design.

205. The materials gathered were acquired from numerous appropriate international sources. Within the suitability analysis document (Ref. 29) detailed justification against set criteria is provided for each selected standard; this is welcomed.

206. As noted above, the breadth of HFE topics is largely appropriate with detail offered to inform design judgments. However, some notable absences were apparent, particularly in terms of informing design decisions with the necessary understanding of required operational tasks.

207. This is most apparent in the guidance to support EMIT and that for operational lighting.

208. Although the HFE Guidance for Local Area Design addresses areas and equipment that are likely to be employed in maintenance, this is not explicit and the guidance focuses more closely on aspects required for operational use without acknowledgement of the additional or alternative complications that would be experienced during maintenance tasks. It also fails to provide any explicit guidance on how to incorporate 'poke-yoka' (mistake proofing) principles into component design, e.g. the use of keyed sub-components.

209. For lighting, my TSC found that the HF guidance fails to specify an illuminance level, although this is captured by electrical engineering guidance. However, where battery back-up is advised to be provided, this is based on common 1 hour standard. For risk important HBSCs, this run time may be inappropriate. There is little benefit in providing a battery with a one hour run time if HBSC duration comfortably exceeds this. This topic is discussed in more detail within the electrical engineering assessment report (Ref 31.) and the shortfall in regulatory expectations is reflected in AF-UKHPR1000-0147. HFE guidance should specifically recognise the need to consider the task characteristics, as what is appropriate in one situation may not be in others. It is an inherent risk of a simple standard based approach to design.

210. My TSC was unable to identify any significant safety case led influence in the development of the guidance or its application during design. As discussed above, the guidance is generally comprehensive in addressing typically expected HF design topic areas pertinent to NPP design. But what is missing is how safety significance influences the application. Within the guidance there is no evident hierarchy to the guidance and requirements offered that cites or uses information gleaned from the safety case.

211. My TSC assessed the RP's stated process for the implementation of the suite of HFE guidance and what opportunities exist within it for the design to be informed by safety

case related aspects. The safety significance HBSCs are such that the design effort associated with the SSC related to them may need to be graded based on risk importance (it is theoretically possible to apply the same level of design effort to all SSCs, but this is not evident in the RP's design process).

212. The lack of hierarchy or targeting of guidance indicates that they have been developed without input from safety case. It would have been beneficial to provide the HF guidance in a more defined formal, numbered hierarchy. As well as better capturing their origin and allowing compliance work to progress in a more structured manner, this would have allowed the reflection of safety significance.

213. The presentation of the guidelines is such that designing against them and subsequently verifying compliance has proved challenging based on the evidence submitted to ONR in the form of design reviews. Guidance material is mostly presented as narrative text, supported (on occasion) by more specific data captured within tables and diagrams.

214. This presentation style can provide a good summary of a specific topic and communicate key aspects. However, the provision of definitive guidance using defined, measurable, numbered and ranked requirements may have been more effective given the target users (system designers) and way in which it was used to provide evidence of HFE.

215. A lack of evidence supplied to demonstrated compliance against the HFE requirements has been a recurring shortfall throughout GDA and I attribute that to this lack of specificity. I consider that the design of the guidance has failed to fully consider the range of users and their differing utility requirements – specifically the system designer with one week of HF training.

216. The reliance on HF assessment post design can be problematic as it can be difficult for an HF SQEP to determine whether a trade-off between competing HF requirements has been effectively brokered. To minimise this risk, the guidance needs to support such situations and it is not clear that it does this effectively. However, I do note that one of the aims of the RP's HF training delivered to the various engineering disciplines was to provide sufficient understanding to know when to seek help. I therefore consider the approach to be pragmatic and appropriate for GDA, given the evidence of a largely fit for purpose output from this process – as discussed in the next section 4.4.1.4. However, I would expect the licensee to devise a solution that finds a more even balance of HF SQEP input vs HF SQEP post design analysis.

217. The HFE guidance appears to be closely derived from established ergonomics texts, guidelines or standards. Whilst the data that are presented do appear to come from these established and creditable sources, this does introduce two risks.

218. First, whilst the approach can assist in ensuring that the data are comprehensive, it can also mean that some of the requirements are not relevant to the NPP application. This may make it difficult for system designers with limited ergonomics background to recognize applicability of requirements and their significance. I consider that it would have been preferable to have been more selective therefore in the selection and use of materials from the defined RGP sources.

219. Second, as already discussed, selecting guidance data from different sources introduces the risk that some of the data are contradictory or not directly comparable.

220. In conclusion it is apparent that the generic UK HPR1000 HFE guidelines documents have generally covered a suitable scope, and to a suitable extent, provided sufficient

detailed information that should allow design to be informed, often by specific measurable requirements.

221. However, I have concerns that in deriving the scope and extent of guidance the RP has misunderstood the relationship between HF and the higher levels of laws and regulations that apply to the generic UK HPR1000 design and in doing so may not have fully considered the contribution of HF to achieving an ALARP design.

222. Furthermore, with regard to the utility of the guidance, the sometimes-narrative nature will have presented challenges to system-designers in: identifying and extracting the exact requirements; understanding their significance; and brokering any conflicts in the requirements. There is evidence that is has created difficulties for the HF team in generating suitable and sufficient evidence to fully substantiate all facets in the GDA design scope.

223. Despite this, the comprehensive scope of the HF guidance has ensured that the design has received HF attention across the board – as evidenced by the HFI summary report and the submissions provided to close RO-UKHPR1000-0011.

224. To address the identified shortfalls, I raise AF-UKHPR1000-0146

AF-UKHPR1000-0146 – The licensee shall demonstrate that the Human Factors Engineering design guidance to support the detailed design resolves the shortfalls identified during GDA.

4.4.1.4 Assessment of the Application of HFE Design Guidance

225. In addition to the adequacy of the guidance, my TSC assessed how that guidance has been deployed and applied by the RP. This is distinct from my assessment of the HF Engineering outcomes (Section 4.4.2) which considers the outcomes from applying this guidance to resulting generic UK HPR1000 design.

226. ONR expects a structured and systematic approach to the integration of HF into the design process (SAP EHF.1. Ref. 2): “A systematic approach to integrating human factors within the design, assessment and management of systems and processes should be applied throughout the facility’s lifecycle.”

227. This expectation is reinforced by TAG ‘NS-TAST-GD-058 Human Factors Integration’ (Ref. 4). The TAG identifies that HFI as a practice is internationally commonplace (see ‘IAEA SSR-2/1: Safety of Nuclear Power Plants: Design’ (Ref. 32)) and recognised; although the exact means by which it is achieved can (necessarily) vary, particularly in terms of scale. For GDA I expect significant, evident effort in HFI. Such evidence should include structured, programmed and timely activity with an appropriate level of authority.

228. As such my TSC assessed the submissions which describe the means and processes by which the RP has integrated HF into the design process with respect to the development and application of HFE guidance. Wider consideration of the RP’s overall approach to HFI is captured in section 4.2 of my assessment.

Definition and alignment of HFI processes

229. Within the three submitted guidance documents, information is provided on how the guidance is to be applied and by whom. Such information is provided early in each document and this is welcomed.

230. The application guidance concerns both the direct application of the guidance in terms of how users are to use and apply it and the wider process for the integration of HF (specifically the guidelines) into the design development of the generic UK HPR1000 design. Aspects are defined such as the scope of the guidance, their intended user group, the relevance of the HFE guidance documents to the overall HFI approach for the generic UK HPR1000 design, the positioning of the guidance within a wider document structure, how they contribute to the CAE approach, how RGP has been applied within their development and how they are to be applied. The provision of information such as this should offer an understanding and context to the specific guidance latterly provided and should give users an understanding of the significance of the guidance offered and how and where to apply it.

231. Overall, the inclusion of this information is useful and should provide users with an easily accessible reference to the necessary processes for the integration of HF into design, particularly where it is necessary to resolve design conflicts and challenges, i.e., where a multi-discipline compromise position is needed (and which must be justified as being ALARP). Furthermore, the content demonstrates a recognition and understanding of the need for HFI and the benefits it can bring.

232. However, while each of the guidance documents provides a description of the processes for their application, they are not uniform (or at least not expressed uniformly).

233. It is therefore possible that this may have contributed to some of the variation in design review submission quality. In particular, the apparent process for the HF input to the design of the MCR is distinct from those for HMI (Ref. 26) or local area design (Ref. 28).

234. The defined approach (captured mainly within section 1.5 of the document (Ref. 26) is only defined loosely within text. It does consider some key, relevant points such as the need for HF specialist support to be sought where non-compliances are identified yet how this is achieved is absent. Latterly (section 1.9 (Ref. 26)) more information is provided on the exact application of the guidance and the overall design philosophy that builds from establishing the overriding purpose of the MCR through to use of detailed design requirements to reach a design that can achieve that purpose.

235. Within both the ‘Guidelines for HMI’ (Ref. 26) and local area design (Ref. 28) a significantly more detailed and prescribed approach is apparent with the use of a flow chart in both to outline the steps of the process and in particular the sequence in which HF design input occurs and where particular decision points are apparent. I consider that the more defined approach taken by these two documents is preferable to that provided within the ‘Guidelines for Control Room design’ (Ref. 27).

236. I am not concerned by these discrepancies in HFI process between the MCR layout and subsequent HMI and local area design guides. It is likely that the – in comparison – differences in design maturity explains the difference in process detail. The MCR layout existed prior to the start of GDA, the UK HMI design and local area design did not. The layout is broadly similar to other Gen III designs assessed for GDA and has been subject to simulator operability testing as part of the Chinese domestic regulatory assessment.

237. However, of more concern is the process detail discrepancies between the guidance documents for HMI and local areas. For example, within the local area design guidance document (Ref. 28) two additional steps related to identifying the nuclear safety significance of the equipment and accordingly either taking a full, detailed approach or a more general one with HF specialist involvement as required. The inclusion of such a step to distinguish between items of equipment or plant areas

within Local Area design is understandable. The apparent lack of such consideration of nuclear safety significance in HMI design, is not.

238. There may be appropriate explanations for the variability between the design processes, but these were not suitably justified by the RP for GDA. It is thus possible that this has resulted in an inconsistent approach to HFI, but I am content that this is suitably mitigated for GDA by several factors:

- The focus of the HF design work has been one of reviewing the reference design, which is an evolutionary PWR design with few novel features.
- Where there is novelty, the RP has demonstrated a proactive and comprehensive HF led analysis, for example for automatic diagnosis and the in-vessel retention concept.
- The application of the HFE design process is more the focus of the site-specific stages and not GDA. For GDA the aim is to demonstrate that the design could be built and operated safely and securely. The design of HMIs and detailed design of SSCs linked to HBSCs are programmed for the site-specific stages.

239. Whilst I consider the differences in HFE HFI approaches are suitably mitigated for GDA, a more closely integrated and graded approach will be required for the site-specific stages. This is bounded by AF-UKHPR1000-0084.

HF Specialist involvement in design

240. The guidance documents make it clear in several instances (e.g. section 1.5 of the ‘Guidelines for Control Room Design’ (Ref. 27)) that successful HFE design is the responsibility of designers, not HF specialists.

241. The expectation that designers take some responsibility for the integration of HF into the generic UK HPR1000 design is encouraged. Such an approach is demonstrably in line with the principles of HFI. However, given the scale and complexity of the plant, and the often specialist and complex nature of HF as applied in the nuclear context, I am concerned that the responsibility appears to be exclusively that of the designers.

242. The RP’s stated position of designers being responsible for the HF input to design is borne out by the processes described within the guidance documents, even in the local area design (Ref. 28) and HMI design (Ref. 26) guidelines where the design process is more explicitly outlined. HF specialist involvement is limited and is, by definition, driven by frequently qualitative judgements made by SSC designers.

243. While some formality in driving such judgements is apparent in the criteria to be applied, they are supported by limited guidance. As such, notwithstanding the limited opportunity for HF specialist involvement, the opportunity is further limited by the need for partially qualitative judgement on HF topics by non-specialist HF system designers.

244. I understand that this process has been driven by the rapid need to expand the scope of HFI over the course of GDA and the small size of the HF Team at the start of GDA. However, my expectation for specialist HF involvement in a design project as significant (in terms of both safety significance, overall size and complexity) is for greater HF led involvement in the iterative design process.

245. The RP’s approach appears to engage HF specialists in only a limited, review based, capacity at the discretion of non-HF specialist designers and, crucially, at a point after designs have been generated thus potentially limiting the opportunity for the HF specialists to influence and shape design other than in a limited manner. The limited involvement of the HF specialists is disappointing but recognised as another facet of the capability challenges that the RP faced.

246. Conceptually, this approach does not meet regulatory expectations, as per TAG NS-TAST-GD-058 “Human Factors Integration”. Regulatory expectations are that “HFI requires that HF is an integral part of a project including both the design and safety case aspects”. The meaning of “HF” here relates not only to the provision of HF guidelines and standards but to ensuring that HF is integrated into the design in a timely way, by those who are SQEP to undertake such activities.

247. Such an approach in isolation, and applied to a design process that was aiming to deliver a detailed design right through to operation, would be not acceptable. Whilst this is still a significant shortfall against expectations, I consider that it is suitably mitigated for GDA by several factors, including those described in paragraph 237:

- The current HF review approach has demonstrably identifying HEDs – 283 deficiencies identified as of Jan 2021, 103 HEDs sentenced, and 22 design modifications (Ref. 17).
- The HFE process is not being performed in isolation. The HRA work is being driven by HF SQEPs and there is evidence that this work is driving positive design changes and identifying HEDs.

248. To conclude, I understand why the RP has taken the approach it has, and the approach is acceptable for GDA. However, I would expect improvements to be made by the licensee, as the complexity of the HFE work will increase during the site-specific stages as the design develops. This is bounded by AF-UKHPR1000-0084 to ensure that the HEDs identified above are resolved early in the site-specific stages to ensure a risk informed and proactive HF involved design process.

4.4.2 Assessment of the Application of Human Factors Engineering Guidance and Methods

249. ONR expects (Ref. 4) that: “…the HF analysis is consistent with relevant standards and good practices, and applies recognised HF methods”.

250. This section presents my assessment of the application of the RP’s HFE guidance and methods, I have divided my assessment into the following specific technical aspects:

- HFE influence on the FCG3 baseline design
- The RP’s system specific reviews
- The RP’s reviews of centralised control facilities space design
- HF guideline compliance in centralised control facility design
- The RP’s management of emergent HEDs
- The RP’s intended HFE Project Licensing programme
- HF implementation seen in a sample of RP’s equipment specifications
- Comparison of the RP’s evidenced HFE scope with a NPP lifecycle

4.4.2.1 Assessment of FCG3 Baseline Design Analyses

251. The generic UK HPR1000 design is an evolutionary NPP derived from the FCG3 reference design. This in turn is derived from the French 900MW three loop reactor design M310.

252. The RP has supplied evidence of HF processes undertaken upon the FCG3 design. It is reasonable to consider that many HF attributes of the reference design will carry forward into generic UK HPR1000. Accordingly, My TSC considered the HF evidence in the RP’s ‘Baseline HF Assessment Report’ (Ref. 33) and sought evidence of the effectiveness of those HF processes in the HF verification of workspaces and HMI involved in risk significant HBSC’s (Ref. 34).

253. From the FCG3 Baseline Report (Ref. 33), the TSC established that the RP's HF team has:

- Identified and examined HEDs relevant to their design contained in Operating Experience (OPEX) reports.
- Undertaken an analysis of functions and then allocated functions for process control and monitoring to humans, technology or jointly.
- Undertaken task analysis to establish whether tasks can be successfully effectively and reliably undertaken.
- Undertaken verification and validation studies by means of task simulations with experienced and trainee operators to establish that the FCG3 intended design is compatible with human needs and the functional requirements of tasks.

254. As my TSC's assessment scope focuses upon the design of the built environment work layouts and workstations, they focused upon Section 6.5 and Appendix C of Ref. 28 concerning the centralised control facilities: the MCR, RSS and Emergency Centre Control Panel. They also examined section 6.6 where HEDs in relation to other SSC's, predominantly local-to-plant, have been considered by the RP.

255. As part of its domestic licensing programme, the RP had previously conducted trials of the MCR design using trainee and qualified operators in a static mock-up of the MCR. The layout for the generic UK HPR1000 is shared with FCG3 reference design so the RP chose to submit evidence gained from these trials to support the HFE demonstration of the built environment and layout.

256. These verification sessions were undertaken during four, five-hour sessions over four working days. Subjective questionnaire-based debriefing of trial subjects and independent observation means that the following HEDs have been considered by the RP:

- Access
- Visibility
- Operability
- Comfort and convenience
- Preferences for alternative overall design schemes and between alternative design features

257. In addition, during debriefings, operators raised matters not included within the structure of the written questionnaires. These HEDs included shortfalls such as:

- Viewing distances being too great or target displays too small
- Sizes positions and spacing of workstations
- Opinions on lighting

258. From this my TSC was able to establish that HF requirements from published standards and guidelines have been applied to the generic UK HPR1000 design main control room built environments and local-to-plant workstation layouts.

259. However, my TSC noted the time spent on these trials. As a proof of concept, I consider the trials adequate to support the evidence required. However, for the site-specific stage, where the HMI will need to be validated, I expect that more comprehensive V&V work will be undertaken by the licensee under normal business.

260. The RP's consideration of other SSCs is contained in Section 6.6 of Ref. 34. The range of HF applied to design appears to be narrower than for the MCR and have largely focused upon:

- Reach envelopes and clearances required for the operation of valves
- Space requirements for maintenance of transportation
- Tasks involving lifting equipment
- The provision of additional interlocks to preclude human errors

261. For both the MCR and other SSCs, reference was made to light and lighting for workplaces in compliance with 'BS EN 12464 – 1, June 2011' (Ref. 35) and to emergency escape lighting provisions.

262. The RP has also undertaken a verification of workspaces based upon FCG3 (and submitted the appropriate elements as evidence in GDA) (Ref. 34) specifically informed by relationships of design to HBSC's. This was undertaken with the express purpose of establishing that human actions required in HBSC's can be accomplished in line with identified time requirements (e.g. transient timescales) and human performance criteria in particular for risk important tasks.

263. Seven scenarios were appraised in the FCG3 simulator using qualified and partially trained operators by:

- Tracking of errors.
- The application of workload assessment.
- Estimation of situation awareness and overall effectiveness in maintaining control of key safety parameters relevant to the scenario.
- In the six scenarios where actions were based upon the MCR, no results identified shortfalls with the built environment or layout.
- The seventh scenario involved actions undertaken local to plant in a scenario where a failed ASG tank required the manual implementation of another ASG tank.

264. In this last case, the local to plant actions involved the addressing of valves in several different rooms. The analysis demonstrated that relevant rooms and valves could be accessed on timescales compatible with the fault transient involved.

265. My TSC noted that the FCG3 baseline design report does not address all the classes of built environment factors that are relevant to HFE. For example, they found no reference to deliver acceptably low levels of noise and vibration, and a habitable thermal environment, nor verification of the same.

266. In March 2021, the RP organised a virtual inspection of the FCG3 plant. The purpose of the inspection was a confidence building exercise to gain observable evidence of the integration of HF concepts and guidance into the design and layout of the plant. The RP presented a pre-recorded plant walk-down of a selection of risk important SSCs, comprising, inter alia, pumps, valves, pipework, spaces, and electrical equipment.

267. What was apparent from the session was that the RP had a good understanding of the importance of accessibility around risk significant components and locating them in positions that maximise accessibility for maintainers. For example, I was able to verify many of the features I would expect to see in an NPP design with consideration of EMIT at the forefront of the design process:

- Valve controls located at waist hight, maximising user leverage.
- Valves located in a place which was freely accessible, not requiring ducting or climbing under or over other SSCs.
- Permanent lifting features located directly above heavy SSCs.
- The appropriate use of spool pieces to minimise the risk of component to component contact during removal and fitting.

- Demarcated set-down areas next to heavy components to minimise the load path distance.
- Clear and permanent labelling of SSCs.
- Access and egress routes that were generally sufficient for two people to pass.

268. This session demonstrated that the RP's designers are aware of task-related HF when considering engineering operations. This is despite weak evidence of a task focus in the design process. I consider, based on what I observed during the plant walk-down, that the RP can develop a plant layout that facilitates the execution of local-to-plant EMIT and operational tasks whose design can comply with HF expectations for those types of operations and tasks. Further task analysis will be required during the site-specific stages to verify the task specific elements of the layout and I welcome the fact that the RP recognises this in its FAP (Ref. 6) I consider this normal business for the licensee.

269. It is was evident from the videos taken at FCG3 that the designers have recognised the importance of providing the user with an operable design. I was able to confirm that there was consideration of EMIT need, access and egress, and the need to provide an optimised work environment for local to plant tasks.

270. To conclude, the evidence presented supports the RP's claim that 'The UK HPR1000 plant operating and maintenance workspaces and Human Machine Interfaces (HMIs) are designed according to modern standards and good practice in HF to facilitate interaction between the personnel and the plant.' sufficient for GDA.

271. However, the RP's assessment of the baseline design does not provide the same level of assurance. I consider this to be function of the scope and depth of assessment undertaken during GDA. The licensee will need carry out a proportionate confidence building review of the FCG3 baseline design to ensure it has a clear understanding of what features can be considered to not require any additional HFE design work. I consider this normal business during detailed design.

4.4.2.2 Assessment of High-Level Analyses

272. To demonstrate that the SSCs for the generic UK HPR1000 design will meet HFE RGP, the RP conducted a series of reviews. These relied upon checklists that the reviewers developed based on the RP's HF guidance.

273. The high-level HF reviews considered:

- General Layout (Ref. 36),
- Generic Layouts of typical SSCs (Ref. 37).

274. The checklists were applied during multi-disciplinary compliance workshops utilising HF and system-designer SQEPs.

275. For GDA, and based on my TSC's assessment, I consider that the selection of checklist items for review of tasks and functions was generally appropriate and that the individual checklist items captured the essence of the requirements specified in the guidelines. This is true whether the text replicated the guideline or whether the reviewers had rewritten them. As noted above, my TSC identified several shortfalls with the design of the guidance material, and there has been a continual challenge during GDA for the RP to deliver clear and unambiguous evidence of compliance with appropriate HFE criteria in its design reviews.

276. For these high-level reviews the functional and task requirements were developed at a generic level. They did not consider the task involvement in specifically identified functions or tasks. The RP had selected facilities and systems for its consideration and

therefore provided a pre-selected and limited sample for their provision of evidence on HFE. My TSC found that in the References 36 and 37, the RP has been unable to apply more than a third of its checklist items to the MCR RSS and Technical Support Centre (TSC) designs as they are not yet sufficiently detailed.

277. It is necessary to ensure that guidelines have been applied as intended. My TSC included consideration of this in their assessment and found that the RP has generally achieved this noting the shortfall cited above regarding evidence quality. I consider this approach offers some confidence that the design can support reliable task performance.

278. However, this does not demonstrate task feasibility. The verification of the design should include both design and task verification activities. In this case, the task verification aspect is absent, although I note that the HRA submissions do partly address this gap. I am pleased to note that the RP recognises this shortfall in its FAP for resolution by the licensee during detailed design.

279. Given the importance of this further work in supporting the safety case and ultimately ensuring safety, I raise AF-UKHPR1000-0147 to include this expectation as part of the future V&V work.

AF-UKHPR1000-0147 – The licensee shall, as part of detailed design, undertake proportionate task verification and validation activities for all risk important human based safety claims including, but not limited to:

- Examination, Maintenance, Inspection, and Testing
- Normal Operations
- Fault Responses
- Interactions with risk important structures, systems, components and equipment.

280. Because of lack of task feasibility demonstration, my TSC undertook other steps, which I later describe, to confirm whether the design outcomes from the HFE processes do meet HF requirements and can support reliable task performance.

281. To conclude, whilst I am satisfied that the RP's work provides limited verification of the incorporation of HF guidelines into the design, it does not fully satisfy s the more fundamental requirements that the RP demonstrates task feasibility, to the extent practicable at GDA, by showing that the built task environment does not compromise human performance and reliability. In particular, it is important the designs supports the reliable performance of tasks important to safety. I welcome the fact that the RP recognises this in its FAP, and proposes additional work in both the HFE and HRA areas to address this. I also consider it somewhat mitigated by the fact that the lack of design maturity both makes task verification exercises difficult at this stage, and affords the opportunity to address this shortfall in the site-specific stages.

4.4.2.3 Assessment of SSC Specific Analyses

282. The RP undertook and submitted the following HFE reviews comprising a range of risk important and bounding SSCs and their locales:

- Nuclear Island Crane Operations (Ref.38) – Selected by the RP based on safety classification and the dropped load risk
- The HVAC system, (Ref.39) – Selected by the RP on the basis that it maintains habitability for the MCR and RSP room

- ASG Pump Room: (Ref.37) – Selected by the RP on the basis that the SSCs within the ASG pump room require frequent inspection or dismantling. Some valves are required to be manually operated during emergency conditions.
- REN Sampling Room (Ref.37) – Selected by the RP based on frequency of use and risk importance.
- Steam Generator Room (Ref.37) — Selected by the RP based on its risk importance and OPEX identified access / egress challenges.

283. My TSC sampled the crane operations report, the ASG pump room, REN sampling room, and Steam Generator (SG) room assessments. I had already looked at the HVAC report as part of my supporting assessment for RO-UKHPR1000-0056 HVAC.

284. My TSC found that design review of the NI crane is limited in the fact that the RP has not specified a vendor for the crane or the related handling tools. Therefore, there is little direct verification and validation that can be carried forward into the site-specific stage. The RP recognises this in the report. The assessment therefore fails to validate the NI crane at this stage. I do not consider the lack of design maturity to be prejudicial to my overall GDA conclusions regarding the viability of the generic UK HPR1000 design as this aspect of the design will be progressed during detailed design so opportunity exists to ensure suitable HFI is applied during this phase as part of normal business by the licensee.

285. The RP's assessment of the three rooms considered in Ref. 37 focused on layout. The RP claims that it conducted a task-based assessment. However, my TSC found that whilst it does contain a rudimentary task sequence, this is simply used to structure the application of the HFE guidance rather than for the consideration of human error. In this manner the RP provides some limited evidence of compliance (or not) of general HF layout rules pertaining to access and egress. My TSC found that, from the report, it is clear that there is generally enough room around major SSCs to support suitable and sufficient access. The report shows the space available comfortably exceeds that required by the equipment with respect to set down areas and accessibility for manually operated valves. These findings supports my own observations during my inspection of FCG3.

286. However, what it fails to do is demonstrate the suitability of load paths or dynamic space requirements. This will be necessary in the site-specific stage to show dynamic clearances are adequate during removal and installation tasks. This shortfall is covered by AF-UKHPR1000-0147.

287. In other areas, my TSC found the evidence for compliance against HFE principles was limited. For example, a claim of compliance against lighting levels of 300 lux simply states that: 'Lighting levels for tasks requiring some perception of detail are suitable.' I consider this another claim and not evidence. Unfortunately, this sort of HFE verification shortfall has been common throughout GDA – a claim being evidenced by another claim. I accept it can be difficult to attempt to verify a conceptual design when design detail is sparse, but in that instance, if an actual measurement cannot be taken, it is then important to cite the technical specification for the item. In this case, the luminaires in the sampling room.

288. To date, the HFE reviews undertaken are largely confined to design verification activities (verification that the design meets HFE standards) relating to the built-environment and facility layouts. Conspicuous by its absence is the lack of suitable task-verification. I note that this is difficult when a design lacks maturity as task verification requires a high degree of detail not present for GDA. However, I recognise the RP's work in this area conducted for the MCR as part of its domestic licensing programme (not assessed for GDA) and its AD trials conducted for GDA which are

discussed in Section 4.2.2.5). This shortfall will be managed via AF-UKHPR1000-0147.

289. The HRA work goes someway to provide some level of task verification but it is limited in scope for local to plant activities and does not adequately consider HFE standards as part of its analysis. So, whilst it does give some confidence of the task credibility, it still leaves a gap. One which is explicable by the lack of design maturity, but one which also places a significant burden of HFE work on the site-specific stage which has attendant design foreclosure risks if this work is not suitably prioritised.

290. To conclude, the RP's system-specific HF reviews, along with my own inspection activities, and the evolutionary nature of the design, provide some confidence that the basic layout of the generic UK HPR1000 design is suitable and sufficient for GDA, and risks in this area are generally mitigated. However, there is a significant body of HFE work that will be required to underpin the detailed design of the SSCs with respect to both design and task verification.

4.4.2.4 Lifecycle Scope of HFE

291. ONR expects HFE to be applied to all phases of the project lifecycle (TAG058). Thus, HFE should be considered in the following:

- The organisation and management of HF in the design processes.
- Design for construction and assembly.
- Design for commissioning.
- Design for operation, test, calibration, maintenance and repair.
- Design for in-service modifications.
- Design for decommissioning and long-term care and maintenance.

292. Typically, the assessment of design for Assembly, Commissioning, EMIT and Decommissioning is performed under the relevant GDA assessments by specialist disciplines within ONR, e.g. ME and Nuclear Liabilities. I have therefore not assessed specific elements of the design to avoid duplication. However, I have sought proportionate evidence that HFE has been suitably and sufficiently integrated across these topic areas to give confidence that HF principles have been followed.

293. When considering my assessment, it is important to note that:

- Detailed design will be undertaken by the licensee during the site-specific stage. Thus, there is opportunity to address detailed design shortfalls at this stage.
- The nuclear liabilities assessment of decommissioning concludes that the RP has provided information on dismantling activities that meets relevant regulatory expectations and is appropriate to GDA. The information is adequate to substantiate the claims and sub-claims that the design and intended operation will facilitate safe decommissioning and can be decommissioned using current methods and technologies, as they relate to dismantling.
- The ME assessment concludes that for the purposes of GDA the RP has, understood generic UK HPR1000 design EMIT requirements; and improved its understanding and importance of HSG253 to achieve safe isolations.

294. The RP Claims: (Sub-claim 3.3.8.SC15.4) The UK HPR1000 plant operating and maintenance workspaces and Human Machine Interfaces (HMIs) are designed according to modern standards and good practice in HF to facilitate interaction between the personnel and the plant.

295. My TSC assessed a number of overarching HF sources for evidence that the RP has integrated HFE into the plant life-cycle. These included:

- The HF chapter of the PCSR (Ref. 3)
- HFE design guidance (Refs. 26, 27, and 28)
- Chapter 24, Decommissioning PCSR (Ref. 40)
- Consistency Evaluation for Design of Facilitating Decommissioning report (Ref. 41)
- PCSR Chapter 30 Commissioning (Ref. 42)
- Summary Report for HFI (Ref. 17)
- The Further Action Plan (Ref. 6)
- The Baseline HF Assessment Report (Ref. 33)
- Human Reliability Assessment Report for SG Access and Inspection (Ref. 43)
- Human Reliability Assessment for Safety Valve Maintenance Activity (Ref. 44)

296. I do not consider this claim suitably and sufficiently substantiated as my TSC found insufficient evidence for the consistent application of HFE to specific phases of the plant life-cycle. Nor did they find much in the way of specific SSC HFE guidance aimed at optimising human performance for commissioning, EMIT or decommissioning tasks. For example, I would expect poke yoke principles (e.g. use of keyed sub-components) embedded in the HFE guidance. This is common shortfall in GDAs where a lack of design detail means that it is not always possible to demonstrate poke yoke for GDA. However, it does not preclude effective HFE outcomes as many HFE poke yoke principles are embedded into engineering design practices and can be addressed the detailed design as normal business for the licensee.

297. On this basis, I sought evidence of effective HFE outcomes in the design despite a lack of HFE integration. HFE expertise specific to commissioning, EMIT, or decommissioning, often lies within the engineering disciplines predominantly working in these areas, so it is not unusual to see good HFE principles applied despite a lack of formal HFI.

298. In this case, I was able to identify some evidence which partially substantiates the RP's claim (3.3.8).

299. Chapter 24 (decommissioning) (Ref. 40) of the PCSR does at least reference HF as being an important contributor to decommissioning reliability, and within the Consistency Evaluation for Design of Facilitating Decommissioning report (Ref. 41), a number of design principles relevant to HF are cited (although explicit links between these and any underpinning HFE guidance are not made). These include:

- The equipment should be designed to reduce the contaminant accumulation and minimise the generation of radioactive waste.
- Design of lifting equipment should take the installation/dismantling operation into account.
- Route or area required for dismantling should be considered at the design phases.
- Dismantling techniques should be considered at the design phases, including conventional dismantling techniques that can be largely used for NPP's dismantling.
- The arrangement should be as compact as possible to reduce the size of radioactive areas thence of radioactive waste, while providing adequate space for equipment ingress and egress.
- The accessibility and laydown areas of equipment and components during decommissioning should be considered.
- The retention and deposition of radioactive substances in systems should be avoided as much as possible.

- Embedment of pipes, fittings and equipment in floors should be practically avoided. The pipes, fittings and equipment passing through walls should be designed carefully.
- The layout should facilitate the decommissioning work and provide effective shielding during dismantling.

300. I note that the RP has performed an OPEX review on Decommissioning (Ref 45) which tacitly captures learning associated with human failures in decommissioning and what can be done to address these with respect to design improvements. Again, however, explicit links to the HFE work were not made.

301. I also note from the HFIP summary report that, in recognition of the importance of HF in decommissioning, the RP recruited a decommissioning engineer into the HF team to reinforce the links between the two disciplines. The RP's GDA programme also includes allocating resources to support decommissioning and EMIT. However, Chapter 30 of the PCSR Commissioning (Ref. 42) does not cross reference with HFE.

302. My TSC found evidence of detailed, but limited in scope, analysis of EMIT for the generic UK HPR1000 design within the HRA suite. For example, References 43 and 44, assesses the EMIT claims associated with a generic Pressure Relief Valve (PRV) and a SG. Both submissions also result design improvement recommendations for the detailed design.

303. The PRV EMIT HRA looked at the reliability of the following activities:

- Check the validity of the pressure gauge.
- Conduct the calibration.
- Conduct leak tightness test.
- Remove, transport and refit the PRV.

304. In performing the assessment, the RP identified a number or design improvement options that could reduce the likelihood of EMIT error. These comprised recommendations focussed on the use of the latest valve test equipment, instead of the reference equipment used as the basis for the HRA. My TSC did however note that there were no recommendations associated with the design of the valve itself.

305. The SG EMIT HRA looked at the reliability of the following activities:

- Open the access aperture.
- Install the block plate.
- CCTV inspection of the surface layer on the primary side water chamber;
- Ultrasonic Test of the ligament area of manway and circumferential weld of SG including the weld between tube sheet and primary head (lower weld), weld between tube sheet and secondary side lower cylinder (upper weld).
- Eddy current test of the SG tube (Plug the SG tube if necessary).
- Restoration of the SG.

306. The RP found that to facilitate 95th% entry to the SG would require an aperture 618mm^2. The design of the actual aperture was smaller, which would have been prejudicial to effective access and emergency casualty evacuation.

307. The RP has raised a recommendation to increase the SG access aperture subject to a full structural integrity impact assessment; sufficient for a UK male 50th percentile operator. I therefore raise AF-UKHPR1000-0148 – for the licensee to confirm that this design change has been implemented, or if this not practicable to do so, alternative remote inspection methods are available that can reliably replace the need for personnel access.

AF-UKHPR1000-0148 – The licensee shall, as part of detailed design, justify that the steam generator access aperture is consistent with UK anthropometric design requirements.

308. There is also evidence supporting the RP's claim of integrated HFE in the design outcomes. I was able to confirm that there is evidence of a design that appears to have taken account of the HFE principles relating to access / egress and EMIT.

309. Whilst it was not possible to confirm poke yoke principles had been followed at the sub-component level, I can confirm that the areas sampled, such as heavy equipment SSC (pumps, motors, and valves) had permanently fixed lifting equipment above them to facilitate installation and removal. Spool pieces were employed where appropriate to do so to simplify installation and removal. Set down areas – co-located with the equipment – were present and demarcated. The RP was also able to specifically articulate the HF thinking that had informed the design; although this is often lacking in the submitted documentation.

310. I also draw some confidence in the evolutionary nature of the design which means that it is likely that improvements in design throughout the life cycle have been made, informed by operating experience of earlier and same generations of plant.

311. To conclude, the RP has not fully substantiated the claim that HFE is applied to all of the generic UK HPR1000 design operating and maintenance workspaces. Where it has produced sample assessments, the evidence is not always sufficient and sometimes found to be lacking in objective detail. However, it is clear that the RP has expended considerable effort and resource in conducting its reviews and there was an upward trend in quality as the GDA progressed. There is also a lack of clarity in the submissions when it comes to articulating the links and subsequently evidencing these links between interfacing workstreams, disciplines and HF. In addition, there is a lack of evidence to conclude that HFE supporting the concept of poke yoke has been applied to the design of SSCs, although I note the design immaturity of many of the SSCs. This shortfall is bounded by AF-UKHPR1000-0084 and AF-UKHPR1000-0147

4.4.2.5 Design Concept for MCR and RSS

312. ONR expects (SAP ESR.1 and EHF.7) that suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary, at appropriate secondary control or monitoring locations.

313. Whilst the HF design and assessment of the MCR user interfaces is outside the scope of GDA, it is appropriate to consider the design concept. My assessment (supported by my TSC) of the RP's MCR design concept is based on Ref. 46.

314. The RP's design concept makes provision for four principal roles for centralised control. These comprise: Nuclear Island Operator, Conventional Island (secondary side) Operator, Safety Engineer, and Unit Supervisor. There are also significant spatial provisions allocated for other work areas supporting additional MCR workers, e.g. local-to-plant operators / maintainers.

315. The concept of two operators, supervised by a more senior operator is conventional and common internationally. As is the role of the safety engineer, who is typically tasked with providing independent challenge during fault conditions, to detect and correct misdiagnosis. I observed, a full crew operating the FCG3 simulator and, as expected, the concept seemed to operate effectively. I am content with this concept, subject to further validation as part of future Integrated System Validation trials which are normal business for the licensee.

316. The principal user interfaces for the four roles are delivered by a networked computer platform - Plant Computer Information and Control System (PCICS), which is safety functional classification 3. The concept employs a series of large screen overview panels at the front of the MCR supporting situational awareness and decision making, and discrete single user screen-based locations. Again, this is similar to other international Generation III and beyond design concepts and designs that have successfully completed GDAs.

[redacted]

318. The Unit Supervisor and the Safety Engineer sit behind at similar desks [redacted].

[redacted]

319. Should a nuclear safety incident arise where the computer platform is unavailable or its reliability is compromised, then operation to safely shutdown the reactor can be implemented via a diverse Emergency Control Panel (Item 19 in Figure 3).

320. Additionally, two other workstations are provided in the MCR. These are the Severe accident Human interface Panel (SHP) and the Diverse Human Interface Panel (DHP) which are used in fault and emergency conditions. Both are safety functional classification 1 providing diverse, high reliability plant information.

321. The SHP is the HMI used to deal with severe accidents. In the event of a severe accident, plant control is transferred to SHP Operation Mode. In SHP operation mode, the control room staff will use the SHP to perform the accident mitigation functions for the identified severe accidents in the plant.

322. In the event of a fault on the reactor control protection system, plant control is transferred DHP operation mode wherein the operators will use DHP to bring the reactor to within safe operating conditions. The DHP is used for confirmation checks when there are concerns over the validity of the primary interface.

324. The general layout of the control desks offers the potential for some visual oversight by the Safety Engineer and/or Unit Supervisor of the nuclear and conventional Island operators. The proximity between all personnel means that verbal communication should be supported if the specified background noise levels are met.

325. However, the supervisory role of a head-down screen-based control room is different to that of a traditional panel-based control room, and these differences need to be recognised as they potentially impact the conduct of operations and importantly the HMI design. They potentially limit how the supervisor can promote error prevention as well as error detection. I have not noted any recognition of these differences or how they will impact the design by the RP. However, as the detailed HMI design is yet to developed, it does not prejudice the viability of the design. I raise Assessment Finding AF-UKHPR1000-0149 to ensure that this is suitably and sufficiently addressed during the site-specific stage.

> AF-UKHPR1000-0149 – The licensee shall substantiate the human factors aspects of the supervisory human machine interface provided in the primary control locations. The human machine interfaces design for supervision should recognise the role differences between operation and supervision.

326. The level of diversity in the HMI matches my expectations for a modern NPP MCR. The adequacy of the categorisation and classification of the C&I HMI architecture is discussed within the C&I assessment report (Ref. 47) and hence is outside the scope of my assessment. However, I have assessed the architecture with respect to how it may impact human performance in relation to nuclear safety.

327. The provision of diverse user interfaces provides defence in depth and allows continued monitoring and control for nuclear safety in the event of a failure of the normal computer-based system. However, such technological diversity generally results in a hybrid panel and screen-based HMI, as is the case here between the Class 1 hard-wired controls and the Class 3 screen based PCICS.

328. Delivery of an operable hybrid interface is not without its challenges, particularly with respect to transitioning between soft and hard interfaces, as it is challenging to replicate the look and feel of a soft interface on a panel and vice-versa. Whilst the detailed design is outside the scope for GDA, I would have expected the RP to note such challenges and recognise them as part of demonstrating the competence that it can build the generic UK HPR1000 design in such a way that it can be operated both safely and securely. Such challenges have not been specifically recognised, and as such forms the basis for the Assessment Finding AF-UKHPR1000-0150.

> AF-UKHPR1000-0150 – The licensee shall, in developing its human machine interfaces, implement guidance and a testing methodology to ensure that the deployment of hybrid, soft, and hard-wired interfaces support effective management of safety and reduces human error during normal and fault states to as low as reasonably practicable.

329. I was able to observe a range of recorded MCR Automatic Diagnosis (AD) safety and operability trials (Ref. 48) as a confidence building exercise with respect to viability of AD and the MCR concept. Here I use the evidence gathered to discuss the MCR concept.

330. The trials comprised 9 scenarios, that were selected on a risk importance and scope basis.

Table 4: Trials Scenarios

Scenario Description	Time Available (Minutes)	Time Taken (Minutes)
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

331. In all instances, the MCR crew were able to successfully diagnose that AD had failed, revert to the paper-based procedure fault diagnosis approach, and successfully implement the HBSCs within the times available. Whilst I can draw no confidence from the HMI design as it is not the same as will be fitted to the generic UK HPR1000 design, I can draw confidence that the trials do verify that the controls and instrumentation present do support the successful management of the above faults and give confidence in the RP's ability to develop a functional MCR, and other control location, designs.

332. Although not planned, the simulator suffered a couple of HMI faults during the trials. This was useful in that it showed that the concept design enabled the operators to detect a disparity in data between Class 3 and Class 1 systems, and work around it.

333. Despite clear evidence that AD had failed, it was clear that the crew were reluctant to abandon the full range of functionality offered. Not only does AD provide a diagnosis, the interface displaying the diagnosis result also displays co-located and aggregated data supporting the diagnosis. In the event of failure, I would have expected the next course of action to carry out careful and structured checks to understand the degree and scope of failure, i.e. is necessary to abandon not just AD but PCICS as well due to the scale of the failure. This was not done.

The lack of willingness to abandon AD is a testimony to its potential usefulness, but also a potential problem operationally as it could be a source of human error. This shortfall was the subject of RO-UKHPR1000-0030 (Ref. 49) which the RP successfully resolved for GDA, but it is a topic that will be necessary to revisit during the site-specific stage with respect to developing an adequate safety substantiation for its deployment. It is therefore the subject of the following Assessment Finding. This is particularly important with respect to testing for, and understanding the consequence, of AD failures. I therefore consider the following Assessment Finding is justified.

AF-UKHPR1000-0151 – The licensee shall, as part of detailed design, demonstrate that the testing required for the automatic diagnosis system will provide evidence to demonstrate that human errors resulting from revealed and unrevealed failures are reduced to as low as reasonably practicable.

334. The Remote Shutdown Station (RSS) forms the fall-back operational position if control from the MCR becomes untenable due to either environmental hazards within the MCR or functional failures of the MCR HMI. The RSS is located on the floor below the MCR and in a separate fire area to reduce the risk of the internal hazards affecting both the MCR and RSS room simultaneously. The RSS is equipped with three control switches to transfer operational control from the MCR to the RSS. Two are located outside the two entry points and one is situated on the central RSS Hardwired Control Panel (HCP). [redacted]

335. The RSS comprises sufficient C&I to take the plant from a fault state to a safe shutdown state. It is not designed for continuous normal operation. ONR's assessment of the Categorisation and Classification of the C&I equipment can be found in Ref. 47.

336. The layout of the RSS room is similar to that of the MCR in that it comprises two operator workstations (COWPs – Compact Operator Work Place) for the Nuclear and Conventional Island operators and a supervisor station for the Unit Supervisor which is located behind the Nuclear and Conventional Island operators.

337. They key difference between the RSS and MCR is the omission of the Safety Engineer location and the lack of wide-screen overview panels.

Ref. 46 indicates that in the MCR abandonment that the Safety Engineer (SE) would also relocate to the RSS room. However, there is no description of how the SE integrates into the RSS and there is no discrete location allocated for this role. I therefore raise the AF-UKHPR1000-0152.

AF-UKHPR1000-0152 – The licensee shall, as part of detailed design, substantiate that the Safety Engineer role is adequately supported by the remote shutdown station human machine interface. This should justify the associated claims made in the generic safety case or demonstrate that this role is not needed for the tasks performed at this location.

338. The lack of overview screens in combination with the lack of visibility (identified by the RP in Ref. 46 by the US of the NI and CI operator screens presents a potential supervisory challenge. I was unable to find evidence demonstrating the ability of the US to provide adequate supervision using the currently provided C&I equipment. However, I note that the layout is again similar to other previous designs that have successfully completed GDA, and I consider any impacts likely to resolvable during detailed design.

339. To conclude, I consider that the RP has successfully demonstrated that the design concept for the overall MCR and RSS layouts and staffing recognises the collaborative nature of team working, shared information amongst MCR occupants, and provides interfaces with defence in depth, or fallback positions, to enable continued monitoring and control in normal, or fault operation. Whilst conceptually the design appears sound, there are a number of specific concerns relating to the detailed design. I consider these to be of significance and therefore raise this as an Assessment Finding.

AF-UKHPR1000-0153 – The licensee shall, as part of detailed design, conduct a graded verification and validation of the human factors aspects of the human machine interfaces, up to and including formal integrated system validation trials where appropriate to do so, to demonstrate their safety and operability. The verification and validation approach should resolve the shortfalls identified during GDA including, but not limited to: • All human machine interfaces important for safety, including emergency control centres, and other risk important control locations. • Partial and complete failures (revealed and unrevealed) of the human machine interfaces and their effects on factors such as task duration / time window, situational awareness, error detection and recovery, and cognitive workload. • Migration of command and control between primary and back-up control locations. • Suitable fidelity in the scenarios, including taking account of parallel or competing activities.

4.4.2.6 Assessment of Centralised Control Facilities – Layout

340. The RP has undertaken workspace design reviews on the centralised control facilities (Ref. 46). These comprised: four in the MCR and three others in the RSS and the Technical Support Centre. These reviews were carried out using operational scenarios.

341. My TSC assessed the submissions relating to these workspace design reviews.

342. These spatial reviews comprised: a link analysis, a Field of Vision (FoV) assessment and a workstation leg clearance assessment. My TSC was broadly content that these are appropriate methods to use in developing or demonstrating the adequacy of a layout. However, they noted that that whilst link analysis remains an important component of the analyses, for modern control rooms where extensive information is available from a single control desk, additional methods may be necessary to demonstrate the adequacy of a layout to support effective communications and supervision.

343. The link analysis and the FoV assessments were undertaken by the RP at a workshop session using a 3D Computer-Aided Design (CAD) model assessment that identified the limiting sightlines from different operating positions in the MCR and other closely related monitoring and control facilities. Chinese and USA anthropometric data and some UK specific data drawn from the Target Audience Description (Ref. 30) were used for this review.

344. The link analyses involved working through some basic operational scenarios and considering operator tasks using the relevant CAD model as the basis. During these scenarios the workshop participants would postulate that the operators would undertake interactions, such as face to face verbal communication, control actions, or change their visual focus to another display. These transitions in operator focus to other user interfaces are known as links. These were recorded and then presented graphically as a line between the two locations on a room plan.

345. My TSC found that:

- The analysis did not record the frequency of the links between each item.
- There was no demonstration that the identification and description of tasks was thorough, as is required for link analysis.

346. I therefore consider the RP's link analysis failed to meet modern standards as it did not provide adequate analytical insight to substantiate (or improve) the design. However, I consider this to be mitigated by the fact the general layouts are similar to other past GDA designs, e.g. two reactor operator stations, with supervisory staff sat behind, all supported by elevated overview panels. I consider that specific shortfalls in this area are likely to be at the detailed HMI level and this is outside the scope of GDA. It is also reasonably practicable to address during the site-specific stage. I consider this can be resolved as part of normal business during the site-specific stage.

347. My TSC found that the RP's FoV assessments showed that there was no direct line of sight to all parts of many of the displays, particularly the lower halves of the wall-mounted large screen displays. However, in order to assess the impact of this on task performance it is necessary to have more information about what is shown on those displays, the frequency with which they may be used and whether the data are available elsewhere in direct line of sight. As the detailed HMI design is not available for GDA, it was not possible to assess this aspect. The analysis was also based on upon fixed observation points when the operators are likely to be seated in office chairs with castors, thus was artificial in its constraints. I consider the analysis did not meet RGP. However, I note the design foreclosure risks from this shortfall to be minor. I am therefore content for this to be resolved by the licensee during the site-specific stage as part of the MCR development.

348. My TSC found that the workstation leg-clearance assessment revealed showed that some dimensions would not currently match UK anthropometric requirements. This is unsurprising given the anthropometric difference between the UK and China. I

consider this shortfall to have low design foreclosure risk as the MCR and RSS for the UK HPR1000 generic design are incomplete so there remains opportunity to address HEDs in this area during the site-specific design stage. I am content for this to be managed by the licensee as part of normal business.

349. To conclude, whilst I have identified shortfalls against expectations, I am not concerned that they prejudice the viability of the wider generic UK HPR1000 design. This is because they can be addressed as part of the further design work driven by the need to assess the design against a UK user population, concept and conduct of operations, and develop, trial, and V&V the detailed HMI design and control room concept during the site-specific stage. Whilst I am content for these individual shortfalls to be addressed as part of normal business by the licensee, AF-UKHPR1000-0153 also provides ONR with the opportunity to confirm that they have been resolved prior to the site-specific V&V process.

4.4.2.7 Assessment of Centralised Control Facilities - Design Compliance

350. The RP has undertaken design compliance audit on the MCR, the RSS and the Technical Support Centre which are reported in Ref. 46, together with the RP's reviews of spatial aspects of the designs. These compliance audits were undertaken by the RP deriving checklists from its pre-existing design guidelines. In their documentation, the RP states that these checks have been applied in the context of HBSCs.

351. The RP categorised the outcomes from these design reviews against guidelines in three classifications: compliant, not compliant or design data not available at GDA.

352. My TSC examined the process of translating the HF guidelines into checklists and the results of applying those checklists. This is discussed in more detail in section 4.4 above. They found the HF guidelines to be detailed in content and discursive in nature. This approach is unquestionably helpful for the reader's understanding of the context of the guidelines and the nature of HF requirements or constraints.

353. My TSC found that this has resulted in some loss of information in the translation from guidelines to checklists. This is because the guidelines themselves are comprised of a mixture of discussion and clearly declared points. Some relevant points made discursively are not subsequently clearly declared. My TSC found that some checks are at the level of a goal and lacking clear criteria suitable for a check. For example, "The design of lighting should optimize visual performance at the workplace", or "Alarms should be properly prioritised" can only be reliably applied by those with comprehensive HF knowledge.

354. Notwithstanding this loss of, sometimes potentially important guidance information, the application of the checklist approach has revealed, as described by the RP, design non-compliances and resulting recommendations for changes during the detailed design to resolve these.

355. As the generic UK HPR1000 design is based upon the FCG3 baseline design, which is designed for use by a Chinese population using Chinese NPP work practices, I consider that it is entirely sensible and necessary to apply such a checklist approach to assist in clearly identifying where the baseline design should be modified to meet UK operational population needs, expectations or operating practices.

356. From its analysis, the RP reports that the process revealed that a little over two thirds of the design compliance checks could not be applied because of insufficient design data being available at GDA Step 4. It is welcome that RP has acknowledged these shortfalls as forward work items in its FAP.

357. Between 8% and 10% of the checks have revealed non-compliance with design guidelines for the three facilities. As this ratio is broadly similar between the three control facilities. My TSC concluded that ratio would be likely to remain much the same if it had been possible to apply a more complete population of checklist items.

358. The non-compliances fall generally under the following headings and are non-trivial; although I consider them non prejudicial to the viability of the design.

- Anthropometrics and workstation fit (relevant to my assessment in the preceding section of this report)
- Noise sources, reverberation, noise control, alarms and verbal communication
- Lighting levels and glare
- Thermal environment, thermal gradients, excessive air velocity
- The number of required display screens in an HBSC task exceeding the upper limit of 4

359. The RP has consolidated their findings on non-compliance into a list, each with a corresponding recommendation. This leads to 7 generic recommendations, and ~ 10 for each of the three control facilities.

360. My TSC's findings demonstrates that the RP is identifying shortfalls, even with the limited design detail, and using this analysis to identify solutions to these problems. I am pleased to note that the RP recognises the limited validity of the design compliance checks that have been undertaken to date. From my own observations I note that the validity is further reduced by the information lost in translation between HF guidelines and the RP's applied checklists.

361. It is evident to the RP that further work will be required beyond GDA to ensure built environments/workspaces are habitable, meet claimed task requirements and do not impair levels of human performance below that which can be achieved with reasonable practicability. I am pleased to note that this recognition is capture as a forward work item in the FAP (Ref. 6) for resolution by the licensee during detailed design.

362. To conclude, The RP has established the principle and application of a design compliance review process. The limited results seen to date illustrate that it is an effective mechanism for verifying the application of HF design guidelines to the generic UK HPR1000 design. In implementing such a process, the RP has implicitly recognised the importance of translating the baseline FCG3 design into one applicable to a UK NPP operating population with corresponding expectations and UK NPP operating practices.

363. The design reviews to date have been of limited success with respect to demonstrating an ALARP position for the generic UK HPR1000 design, due to challenges related to design maturity and adequacy of translating HFE RGP into audit material. The RP's audits have also revealed a number of non-trivial shortfalls, as described above. However, I welcome that the process is in place and note that given the lack of design maturity this affords the opportunity to improve the audit process and address these shortfalls during the site-specific stage. Having assessed the recommendations (both those adopted into GDA and those for consideration by the licensee during detailed design), I consider there to be nothing in them that is not reasonably practicable to implement and note that the design changes implied have been readily achievable in an NPP design for many years. I am therefore content for the shortfalls discussed above to be progressed by the licensee as part of normal business.

4.4.2.8 Automatic Diagnosis

364. The generic UK HPR1000 design proposes the use of an Automatic Diagnosis system. This system automatically guides the operator to a suggested diagnosis in the event of a plant fault.

365. As this would be novel for a GB reactor design, I chose to include the AD system within my assessment scope during GDA. Following initial assessment, based upon the RP's submissions during the early stages of GDA, I judged there to be potential regulatory shortfalls associated with the deployment of the AD system on the generic UK HPR1000 design. The RP claimed that the AD system, despite providing actionable diagnostic information important for nuclear safety, and residing on a Class 3 C&I system, was not in fact a safety system and thus was considered as non-classified. I challenged this claim on the basis that the AD system directed fault recovery actions to restore nuclear safety functions and raised RO-UKHPR1000-0030 on this basis.

366. The RO required the RP to do the following:

- Identify the safety function/s that the AD system directly or indirectly supports.
- Based on the safety function/s, assign a suitable safety classification for the AD system.
- Develop a verification and validation plan for the AD system, including both the technology and the human machine interface elements.
- Produce a suitable and sufficient safety justification for the AD system as part of the overall generic UK HPR1000 safety case.

367. The full assessment of this RO can be found in Ref. 49, but in summary:

- The RP provided a suitable and sufficient (for GDA) safety analysis of the safety functions that AD supports. The RP revised the safety classification of AD from unclassified to SFC-3. This now aligns with the safety system that AD forms part of the PCICS. Class 3 is also consistent with other reactor design's screen-based computer-based control systems.
- The RP provided video evidence of AD being tested in the MCR simulator, which demonstrated that there is sufficient diverse instrumentation provided to perform diverse checks to confirm the functionality of AD. Thus, proving that conceptually AD failure could be detected.
- Should either the reliability or operability of AD be subsequently found to not meet the claims for it during GDA, it could be removed, and the concept of operations revised to one of using paper-based (or electronic) procedures to carry out fault diagnosis. This approach is the one used on currently operational reactor designs. Hence there is little design risk posed by including this system in the generic design.

368. Whilst the RP has provided sufficient evidence to conceptually demonstrate the feasibility of AD, the video evidence shown for confidence building also showed some implementation problems. For example, I noted (Ref. 48) a reluctance to turn off the AD when it was known to be in a faulted state, as the AD HMI aggregated diagnostic data considered useful by the MCR crew.

369. AF-UKHPR1000-0151 raised above can be used to ensure that the licensee demonstrates the usability of AD system.

370. To conclude, I consider that the RP has provided sufficient evidence to demonstrate the conceptual validity of the AD system. I welcome, the recognition that it does indeed play a safety role, and subsequent change from non-classified to Class 3. However, I

also note that additional evidence will be required to fully substantiate its deployment on the generic UK HPR1000 design, and therefore raise AF-UKHPR1000-0151.

4.4.2.9 Management of Human Factors Engineering Deficiencies

371. ONR expects (Ref. 4) that duty holders have in place suitable and sufficient arrangements for the capture, management and sentencing of HEDs.

372. In determining the adequacy of the RP's management of HEDs, my TSC assessed the following sources for the identification of emergent HEDs and consequent HF recommendations for change upon which the RP relies. These sources were:

- HBSCs List (Ref. 51)
- HF Assessment of General Layout of Typical SSCs (Ref. 37)
- HF Verification of HMI and Workspaces Related to Risk Significant HBSCs based on FCG3 (Ref. 34)
- Target Audience Description – in particular, the identifications of SSC designs Identified from analyses informed by their TAD (Ref. 30)
- ALARP Demonstration Report of PCSR Chapter 15 (Ref. 51)
- HRA Summary Report (Ref. 10)

373. It is clear from my TSC's assessment that recommendations to address HEDs have arisen from all these different sources. There is also evidence that these recommendations are being appropriately sentenced. The list of recommendations adopted into GDA can be found in Annexe 2. For example, I note that a significant HED identified was the inability of an operator to respond in time to re-energise the necessary valves to support in-vessel retention function following a loss of coolant accident. This HED lead to a design change to change the AoF from local manual to remote manual.

374. I note that, the predominant source of recommendations has been the HRA and the HF design reviews. The RP's FAP (Ref.6) reports that in total 278 shortfalls and related recommendations have been raised during GDA.

375. The RP's sentencing of these recommendations has resulted in four types of sentencing decision.

- Design modifications included in the design reference - #16
- Out of GDA scope/site commitment - #155
- Safety case document clarification - # 7
- Safety Case clarification and modification - #85

376. The small number of design modifications may reflect the detail of the generic design information available to those seeking to apply checklists/guidelines to the design. I have noted earlier in this assessment that in HF studies of centralised control facilities the RP was unable to apply more than 1/3 of the HF guidelines/checklists to the design which provides another explanation.

377. Circa 56% of the recommendations have been judged by the RP to be out of GDA scope and by classifying them as a site commitment for the licensee. This means that a considerable degree of, possibly additional, design assessment must occur in the site-specific phase.

378. I am encouraged to note that 112 recommendations have been made to influence improvements in the safety case at both an editorial and at a more functional and structural level for the detailed design.

379. To conclude, many HEDs are emergent and cannot be solely addressed by the application of international, local or site-specific standards and guidelines. Therefore, I am pleased to note that the processes collectively described by the RP as HF risk assessment processes (Ref. 30) are delivering HF recommendations for improvement. However, such processes by themselves, when aimed at error quantification focus on substantiation rather than improvement. The necessary substantiation mindset is unlikely to identify as many improvements as a focussed design review. Thus, it only goes part way to demonstrating ALARP. I am pleased to note that the RP has defined FAP actions in this area which will increase the scope of the HFE design reviews to address this. I am content for these shortfalls to be addressed as a combination of normal business and the Assessment Findings already raised.

4.4.2.10 HFE In SSC Procurement

380. It is difficult for the full scope of HFI to be delivered solely by the designer in collaboration with the Licensee for a nuclear power plant. Typically, this means the supply chain is leveraged to provide additional HF support during the procurement of SSCs. Usually, this is managed via the flow-down of HFE requirements into the design specifications and subsequent procurement contracts.

381. The RP expects the licensee to adopt this approach during the site-specific stage, so my TSC sampled 20 of the RP's Equipment Specifications / 'Technical Specifications to test the suitability and sufficiency of these specifications. The sample comprised a range of equipment including diesel generators, heat exchangers, pumps, switch gear, C&I equipment, fuel route lifting equipment, and motors:

382. Where HFE has been specified, my TSC found variability in what has been included and in eight cases, HF is not mentioned at all. It would be disproportionate to assess each of these documents in detail. For GDA, however, it is appropriate to consider and draw together common elements that should be in all SSC specifications issued during the site-specific phase.

383. The different authors of the specifications have sought to identify different forms of HFE requirements, which is positive in terms of the wider recognition of HF within the RP. These types comprise:

- Requests for the supplier to provide an HFI Plan (HFIP).
- The specification of a proportionate HF process determined by listed criteria.
- The outline of the overall objective for effective human performance and error minimisation.
- A requirement to follow specified HF design guidelines.
- The broad description of an overall HFE process e.g. involving the application of guidelines, with subsequent verification and validation using simulators.
- The specification of particular design features to support maintenance.
- The specification of particular HF objectives to support operation.
- The identification and outline description of specific task requirements.

384. I consider that, in practice, all of the bulleted elements outlined above should be included in equipment specifications to an appropriate level of detail.

385. At the close of GDA the RP does not have a systematically developed approach to the specification of HF interface and integration processes nor HF methods to be applied to design that suppliers will need to meet if the HFE mission is to succeed.

386. The RP does not consistently require:

- The provision of an HFIP.

- Design verification and validation activities.
- The application of specified and harmonised HF guidelines.

387. In addition, the RP does not appear to recognise that the HFE mission can only succeed if it:

- Describes in some detail the safety case claims and requirements for good levels of human performance and minimise human error if the safety case assumptions are to be met.
- Describes in some detail the consequent human operational and maintenance tasks that need to be undertaken with the suppliers' and other interfacing suppliers' systems if the HFE mission is to be met.
- Provide managed processes and a forum whereby:
  - Design and HF analysis interfaces between procurers, suppliers and the designer occur effectively to manage the delivery of HFE missions across supplier boundaries.
  - Identify and resolve the inevitable emergent HEDs arising across such boundaries.

388. I have also seen little evidence to suggest that the RP fully understands what is required to manage HFI across supplier boundaries.

389. However, I am content that the licensee can address these gaps, and I welcome the clear intent shown by the RP to ensure that HF requirements are cascaded down into the supply chain, and I particularly welcome the fact that this is understood not just by the HF team but also by the wider engineering function of the RP, and most importantly that this is understood during GDA.

390. To conclude, despite the minor gaps in the HFI requirement included in SSC specifications, the fact that the specifications include this requirement at the GDA stage, I consider sends a clear message of intent that the RP understands the importance of HFE in design. I consider the degree of HFE expectations established within the specifications are suitable for GDA. However, I would expect further development by the licensee with respect to detail and consistency, to mitigate the variability and inconsistency in the international supply chain when it comes to HFE and HFI. I consider that this matter can be addressed as part of normal business.

4.4.3 Strengths

391. The HFE guidance strengths comprise the following.

- The RP has provided a suitable justification for the selection and use of HF RGP to the design of the generic UK HPR1000.
- The guidance developed by the RP is generally attributable and aligned with identified sources of RGP.
- The guidelines have a suitable and sufficient coverage of HF topics for GDA that recognise the extent of HF influence necessary within NPP design.
- The broadly comprehensive nature of guidance in addressing HF topics pertinent to NPP design should mean that, by inference, all safety significant topics are covered.
- The RP has provided a clear and evident CAE structure that explains the purpose and status of the HFE guidelines documents
- Although detail discrepancies exist there is an overriding process apparent for the integration of HF guidance into the design of the generic UK HPR1000
- The RP has clearly defined its expectations for the users of the guidelines.
- The RP has demonstrated that it can develop sufficient HF capability to integrate HFE into the design process.

- The RP has demonstrated that it has up-skilled HF capability outside of the core HF team via targeted training.
- The qualitative HRA does not identify or suggest that there are any design shortfalls that might impinge upon task performance.
- The RP has suitably demonstrated that the HFI programme has been effective in driving design improvements towards an ALARP position.
- The outcomes from design programme for FCG3, as seen in the inspection videos, show that operational and EMIT considerations have been taken account of in the design.
- The RP recognises the importance of HFI within the supply chain and there is evidence, even during GDA, that HF requirements are being captured in the supply chain specifications for SSCs.

4.4.4 Outcomes

392. The HFE guidance findings comprise the following.

- There are discrepancies apparent in the application of anthropometric data.
- There are some shortfalls with respect to the traceability of the source of material cited in the guidance.
- The guidance provides insufficient hooks to ensure that it is applied within the context of the task, as opposed to the current criteria compliance approach.
- There is insufficient guidance presented in relation to supporting cognition. The current focus is on physical ergonomics.
- There are examples where the guidance fails to provide sufficient specificity to support design verification activities as it is presented as narrative text as opposed to specific objective criteria.
- The RP should ensure that all data used within the guidance is demonstrably relevant to a UK NPP application.
- The RP's processes for the application of HF design guidelines are disjointed depending on the topic area under consideration.
- The RP's processes for the application of HF design guidelines only include HF SQEP in a "review" capacity.
- The ability to apply the HFE checklists for audit purposes have been limited by a lack of design maturity.
- The HFE work to date has focussed mainly on design-verification (a standards in design approach). Outside of the HRA work, there is no evidence of task-verification work performed to validate the design.
- The evidence provided by the RP to demonstrate compliance with HF RGP is variable in quality – in several instances offering subjective statements against insufficiently specific criteria. However, this generally applies at the component level like lighting so is resolvable during the site-specific stage.
- I have raised 7 assessments findings in my assessment of the RP's HFE.

4.4.5 Conclusion

393. Based on my TSC's sample assessment of the generic UK HPR1000 design HF guidelines documents and associated ancillary material, and my own assessment work over the course of GDA, I am satisfied that the RP has established a suitable (for GDA) suite of guidance material. Further development will be needed, but I consider these resolvable by the licensee in the site-specific stage. The generic design facilitates the continued development of this guidance, and also affords the opportunity to directly integrate it into the design process. The RP recognises the need for a more pro-active HFE design approach during the site-specific stage.

394. The application of the design guidance has generally been retrospectively applied rather than used more proactively by the HF team. Evidence provided by the RP

demonstrating compliance with HF RGP has been variable, although I have observed an upward trend in quality throughout GDA. Considering other work including the AoF analysis and the HRA, I judge that the RP has sufficiently demonstrated the viability of the design such that it could be built and operated safely and securely within GB.

395. I have found no evidence of task-verification outside of the HRA work to date, although concede the difficulties in conducting such analysis with a generic design at the component level so I am content for this to be performed during the site-specific stage. The licensee will need to programme its HFI work accordingly so that it aligns with the design procurement programme and avoids risks of foreclosing the design options without appropriate task verification.

396. I am pleased to note that the RP has demonstrated that despite some of the shortfalls in guidance and application cited above, the HFE work has raised a number of recommendations, which, when scrutinised, provide confidence that the RP is working towards a design that is ALARP.

397. Overall, I am content that the RP has provided sufficient HFE evidence (when considered in concert with the evidence provided by the other HF workstreams) to demonstrate that the generic UK HPR1000 design can be built and operated safely and securely in GB.

4.5 Identification, Analysis and Substantiation of HBSCs

398. ONR SAPs EHF.3 Identification of actions impacting safety and EHF.10 Human Reliability Analysis (HRA), establish the expectations for a modern standards HRA. They respectively guide that: “A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents, and Human Reliability Analysis should identify and analyse all human actions and administrative controls that are necessary for safety”.

399. It is against these that I have based my assessment of the RP’s HRA. It is important to note that HRA is also assessed in part within the PSA assessment report, (Ref. 52). I have worked closely with my PSA colleagues in this assessment. I have also used TSCs to perform independent assessments of the RP’s HRA to inform my judgement.

400. I have structured my assessment of the RP’s identification and substantiation of HBSCs in three inter-related parts:

- **Identification and management of HBSCs** – In this section I assess the RP’s approach to the identification and management of HBSCs.
- **The qualitative analysis and substantiation of HBSCs** – In this section I assess the qualitative aspects of the submitted HRA, including the data and information sources, the qualitative methods, links to design activities, and verification and validation. The purpose of this part of the assessment is to judge the level of understanding of the human contribution to risk and how it has been managed and reduced. The outputs from the RP’s qualitative analyses will inform their quantitative analyses, such as by supporting the identification of PSFs and the assessment of their effect, and hence my assessment of the qualitative aspects informed my assessment of the quantitative analyses.
- **The quantitative analysis and substantiation of HBSCs** – In this section I assess quantitative aspects of the HRA, including the scope of the analyses, the identification of HBSCs, the quantification methods, the treatment of dependency. The purpose of this part of my assessment is to judge the acceptability of the level of risk associated with human performance.

4.5.1 Identification and Management of Human Based Safety Claims

401. The identification and management of HBSCs is captured within Ref. 50. This submission has been used as the vehicle to provide a single source of HBSCs for the GDA project, and it is anticipated that it will continue to do so by the licensee as the safety case evolves through the site-specific phases.

402. A significant challenge for HF is understanding what risk important operator claims are being made and where to find them. This is key to suitable and sufficient substantiation. I consider the fact that at GDA, there is a central repository for all HBSCs to be a positive step by the RP.

403. I consider the HBSC list to be sufficiently comprehensive for GDA. It draws from a wide range of sources, including the internal and external hazards PSAs and fault and hazard schedules.

404. It depends on the specific source of the HBSC, but typically the information presented includes a source reference, the HBSCs relation to the safety function, HBSC classification (as within the fault schedule) and relevant probabilistic importance measures, e.g. Fussell Vesely (FV) and Risk Achievement Worth (RAW). These importance data have been used to derive the RP's GDA scope of HBSC analysis.

405. The only areas where a minor shortfall was identified and later closed during the GDA assessment was in the identification of HBSCs within both the external and internal hazard schedules. This shortfall was progressed jointly with ONR's internal and external hazard assessors, and is discussed in their respective reports: References 53 and 54.

406. Collectively, ~ 1200 HBSCs are presented in the HBSC list report (Ref. 50).

407. To conclude, I consider this collated and risk informed database of HBSCs establishes a sound basis to develop the forward programme of HRA and HFE during the site-specific stage as, in the format presented, it is a very powerful tool for the licensee to inform its future HFI programme.

4.5.2 Qualitative Assessment and Substantiation of HBSCs

408. The present section presents my assessment of the qualitative aspects of the RP's HRA. It is presented under the following sub-headings:

- Suitability of data (including OPEX)
- Task and error analysis approach
- Dependency
- Analysis of Type A failures
- Analysis of Type B failures
- Analysis of Type C failures

4.5.2.1 Suitability of Data (Including OPEX)

409. This section describes my assessment of the data sources that underpin the qualitative analyses, including their coverage and relevance. I have used an independent TSC assessment to inform my regulatory judgements on this topic. I refer forward where relevant to the specific analyses of different failure types to discuss the implications for the validity of the analyses of how the data have been applied.

410. The HPR1000 design is an evolution of existing plant, and hence it is expected that an input to the HFE and HRA should be data collected from operating experience drawn

from existing plant; both to underpin claimed human performance, and to provide evidence in support of improvements incorporated into the new design.

411. ONR expects (Ref. 2) the appropriate use of OPEX (historical data from operating plant and from international experience) be used to support human performance claims, and to identify credible errors.

412. When assessing specific HRAs, my TSC did not find evidence of the comprehensive use of OPEX to inform judgements of human error and human reliability. This was particularly apparent with the 'generic' assessments of potential Type A errors, e.g. 'Human Reliability Assessment Report for Instrumentation Calibration Activity' (Ref. 55). In this report, there is no stated OPEX used to inform the identification of potential errors, nor their quantification. Whilst SMEs in operations and maintenance were involved in the HRA process, I find the lack of cited OPEX notable.

413. My TSC also noted the limited use of OPEX in Type B HRAs, such as in 'Human Reliability Assessment Report for Fuel Handling Operations' (Ref. 56), where only three items of OPEX are cited.

414. In the HRAs for Type C errors, the use of OPEX is also limited. In 'Human Reliability Assessment for manual water injection to SG by ASG (OP_L2_FW)' (Ref. 57) it is stated that 'No Operating Experience (OPEX) identified'. It is unclear to what extent attempts have been made to examine OPEX generated from simulator exercises, training experience, and other secondary sources of OPEX to inform error identification and reliability estimates. My TSC noted limited use of simulators to validate certain task timing assumptions. However, I welcome that the RP cites the need for the licensee to gather further OPEX data, including from simulators, in the FAP (Ref. 6).

415. Because of these uncertainties in my ongoing assessment, I raised RQ-UKHPR1000-1438 Use of OPEX. The RP's response to this RQ confirmed that their OPEX database does include lessons learned, good practice, and experience summaries. It also confirms that thematic experience feedback on similar events is included. The response also provides further information concerning the structure of the CGN OPEX database and the search functions. My TSC's assessment of the RQ response provided sufficient confidence for me to be satisfied that the database provides a useful tool for searching OPEX data that have been collated. I am also satisfied that the RP understands the importance of the keywords to aid search within their OPEX database.

416. However, the tool appears to be structured principally to support design decisions, and hence I note that the tool has not been used sufficiently rigorously to identify credible error modes and to support quantification. I would expect greater use of OPEX to be apparent when updating the HRAs to better inform the emerging design, following GDA.

417. Little formal OPEX is cited for the majority of HRAs that my TSC's assessed. Whilst this is likely to be correct with respect to the specific transient and post-fault actions that have been modelled, it suggests a potentially narrow search process. I would expect to see some evidence of OPEX relating to the generic activities that underpin the tasks. Elements of such OPEX will have been accessible through the presence of operations SMEs at the RP's data collection workshops, but I am unable to judge the adequacy of the data collection arrangements in this respect.

418. My TSC found that little explicit use of simulator data has been cited other than to inform the identification of key HMIs. There is some evidence of use of simulator data to inform assessments of task success, such as for 'Isolating Impaired SG' (Ref. 58), where a simulator trial was used to validate task time. However, my TSC was unable

to identify sufficient evidence of simulator data being used to inform identification of operator errors and behaviour, in the absence of OPEX relating to failures on operational plant.

419. Some HRAs do cite extended OPEX. In particular, the HRA for 'Isolating Impaired SG' (Ref. 58) does describe extensive OPEX from other plant, given that Steam Generator Tube Rupture (SGTR) is a notable PWR fault, although much of the cited OPEX is comparatively old. However, in this example, the use of OPEX has tended to be restricted to validating timeline analysis, rather than informing the error identification element of the HRA. I consider that this has reduced the value of the HRA process for the RP, in respect of enhancing their understanding of human performance.

420. I note that the absence of a clear description of how OPEX has been collected creates uncertainty about whether the OPEX search process is sufficiently comprehensive. A number of the HRA reports state that no relevant OPEX has been identified. Those reports would benefit from a clear description of how OPEX has been sampled and what sources were searched. My TSC identified a number of items of OPEX that I consider exemplify the wider benefits of a more comprehensive examination of extant OPEX.

421. For example, the 'HRA for Bleed and Feed' (Ref. 59) does not make reference to any OPEX. There is international OPEX for Feed and Bleed, such as the Davis Besse Loss of All Feedwater Event (NUREG 0933 Issue 122). Whilst this OPEX does not have strong recommendations with respect to HRA, it presents extensive information concerning the performance of the operating team, including the potential for delayed action. I would have expected OPEX such as this to be referenced. Similarly, NUREG 0933 Issue 70 describes an problem with PORV and Block Valve reliability, which identifies a potential accident scenario including where failure of an operator to close the Block Valve would increase the likelihood of a small break LOCA through the PORV flow-path.

422. There is a range of OPEX that I consider should be acknowledged, both with respect to HRA and to design of the system, including design of procedures and training. Other examples include, but are not limited to, Dampierre (Ref. 60), uninterruptible power systems (UPS) failures (Ref. 61) Callaway Plant (Ref. 62).

423. The RP recognises that OPEX could have been used to greater effect during GDA and has added an item to its FAP to capture this for future resolution by the licensee during detailed design. (Ref. 6).

424. I consider there is sufficient OPEX material developed by the RP during GDA in the HF area to provide the licensee with a starting baseline to develop further its HF related OPEX database. The RP has provided sufficient material within its FAP to give clarity what additional work will be required in the site-specific stage. I consider the matters identified during GDA can be resolved as part of addressing AF-UKHPR1000-0085, raised earlier.

4.5.2.2 Task and Error Analysis Approach

425. This section presents my assessment of the analytical methods that underpin the qualitative analyses. I have used an independent TSC assessment to inform my regulatory judgements on this topic. I refer forward to the specific analyses of different failure types to discuss the implications for the qualitative insights that arise from how the methods have been applied.

426. SAP EHF.5 guides that: proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute. It is a key input in a suitable and sufficient risk assessment.

427. I expect the RP to undertake analysis, that is proportionate to the information available at GDA, of those human actions necessary for safety, in order to determine that the human contribution to risk is understood, and that the risk is (or capable of being) reduced to levels that are ALARP.

428. A critical part of that programme of work is the Task and Error Analysis, that provides a basis both for demonstrating a sufficient understanding of the task demands and how they are managed and controlled, and also to provide input to the quantification processes that support the determination of human error probabilities to be applied to the PSA.

429. My expectations with respect to the approach to task and error analysis take account of generic nature of the design, and from the manner in which human performance is affected by the suitability of organisational and administrative arrangements that are not part of the GDA scope.

430. My assessment (and that of my TSC's) was therefore based on the following expectations, for each task and error analysis, as per ONR's TAG on HRA (Ref. 4):

- A clear description of the task based on a structured process of task analysis.
- The task analysis is informed by relevant data sources, including formal descriptions of similar tasks applied to current plant, contributions from relevant SMEs (including operators), training and simulator data, plant descriptions for the proposed design, reviews of expected PSFs.
- A structured process for error identification is applied, including errors of omission and commission, and cognitive errors.
- A structured process for consideration of operator workload.
- A structured process for consideration of task timings, and, where appropriate, communication demands.

431. I expected the way each of these were undertaken to be proportionate to the specific task, the level of risk associated with task failure, and the maturity of the design in respect of the task. I also expected to see clarity concerning the way the outputs from these methods have informed the HRAs, and also how the outputs will be used to inform detailed design and the development of the licensee organisation and arrangements.

Task Analysis

432. The RP's approach to task and error analysis is set out in the 'Task Analysis Methodology' report (Ref. 63), which provides further explanation of the approach described in the 'Treatment of Human Actions Implementation Plan' (Ref. 64). The Implementation Plan states that during GDA, HBSCs will be subject to proportionate HF assessment using Task Analysis and Human Reliability Quantification informed by the nature and severity of the potential consequence.

433. It further states that a representative set of such assessments will be completed for GDA. I am content that the RP has recognized that the set of assessments presented at GDA is not complete, and that it has selected a sample based both on risk significance and other factors such as the challenging nature of certain tasks as informed by operational subject matter experts.

434. The RP has recognized that the set of HBSC assessments presented at GDA will also require re-assessment during the site-specific stage, once further understanding is available concerning the detailed design and organizational and administrative arrangements. The FAP identifies several areas where further work will be required during the site-specific stage.

435. The FAP does not specifically note the need to revisit the existing HRAs to address the shortfalls noted in my assessment, but I consider these can be managed via normal business.

436. The 'Task Analysis Methodology' document (Ref. 63) sets out further information concerning the methodology applied. My TSC found that the importance of OPEX is clearly noted, although as I discuss below, in the context of the specific Type A, B and C assessments, it is unclear whether sufficient use of OPEX has been made.

437. The RP has used Hierarchical Task Analysis (HTA), Tabular Task Analysis (TTA) and Time-Line Analysis (TLA) methods, which I recognise as RGP and appropriate for a generic design. I would expect to see selective use of other methods, dependent on the nature of the task under consideration, such as Link Analysis and Communications Analysis, but I also recognize that the HEDs that would be revealed by such methods can also be recorded within an HTA or TTA.

438. The 'Task Analysis Methodology' document (Ref. 63) presents the template assessment for TTAs and uses the following headings:

- Task No.
- Task Title
- When and where
- Equipment Indications
- Job factors (e.g. training)
- Technology factors (e.g. HMI)
- Environmental factors (e.g. noise)
- Organisational factors (e.g. culture)
- Situational awareness and cognitive workload
- Error/Violation Mode
- Error/Violation Description
- Error/Violation Consequence
- Error/Violation Recovery
- Note

439. This set of headings supports the recording of sufficient information to meet RGP in this area, although it does not fully support a clear description of the links between identified errors and PSFs, and hence assessment of the strength of affect arising from identified PSFs.

440. My TSC found that that the TTA structure contained small inconsistencies. For example, whereas the TTA presented in 'HRA for Typical Valve' (Ref. 65) broadly follows this structure, it does add in further headings or additional information such as 'Person', 'Information needed and presented'. Conversely, the TTA presented in 'HRA for manual water injection to SG by ASG (OP_L2_FW)' (Ref. 57) and the TTA presented in 'HRA for restarting RHR pump manually (OP_RHR_S1)' (Ref. 66) adds in a heading for "duration".

441. I consider these inconsistencies a reflection of the continuous improvement observed during the GDA with respect to establishing a fit for purpose HRA approach. I am content that the quality of the HRA submissions are adequate for GDA.

Error Identification

442. ONR expects (Ref.4) that a: "…structured and systematic human error identification process has been used to identify and define all safety important human tasks, sub-tasks and associated errors." Identification of potential errors is a key element of the qualitative analyses that supports HRA.

443. The language used in Ref. 64 appears to use the terms HBSC and Errors interchangeably (e.g. Section 3). This may restrict the way the RP has sought to identify human failure events that could lead to a challenge to the HBSC. Later sections of Ref. 64 indicate that a structured approach to error identification is applied, drawing on a range of sources such as OPEX, data collection from simulators, and structured task analysis. However, the categorization of error modes presented in Section 5 of Ref. 64 appears to be limited. The categories considered are Slips, Lapses, Mistakes and Violations. It is not clear, from this information, to what extent a rigorous and comprehensive process of error identification has been applied, covering errors of omission, commission, and cognitive errors. It is not clear that there is sufficient treatment of psychological error mechanisms such that the links between tasks, demands, and PSFs can be suitably understood and assessed. Furthermore, as discussed above with respect to OPEX, my TSC noted that the data sources that have been collated did not present sufficient evidence of a structured approach to error identification.

444. There is an absence of any formal error identification methods described within the HRA method document (Ref. 67), such as Systematic Human Error Reduction and Prediction Approach (SHERPA) or Technique for Retrospective Analysis of Cognitive Error (TRACER). However, SHERPA is cited within some of the HRAs, but the decision to use this method is not explained (although I have no objections to its use as it is a common method employed I consider it to be RGP) and whether it is expected to be a routine part of future HRAs.

445. The submitted HRAs report the use of an error taxonomy that appears to be a modified form of SHERPA. The taxonomy predominantly uses a set of surface forms of error (e.g. action too early… wrong check… critical data not obtained… etc). Whilst the cited taxonomy does include a set of error modes associated with the plant status Assessment, I would expect to see a more rigorous treatment of cognitive errors (as is provided by such methods as TRACER), particularly in the context of fault diagnosis. The taxonomy used, being based on the surface forms of the errors, does allow identification of errors of commission. However, the absence of formal methods to consider cognitive errors during diagnosis limits the scope of error identification, particularly in respect of improving the design. It also reduces the value of the analyses with respect to providing a more detailed understanding of human performance and how it may be influenced by HMI, task design and organisational arrangements. Furthermore, the absence of explicit discussion of internal/psychological error modes reduces my confidence in the way the strength of PSFs has been assessed and incorporated into the quantification process.

446. However, this shortfall needs to be considered against the limited set of relevant information available at GDA (particularly HMI), and hence I consider that the error analysis provided is sufficient, subject to my expectation that a more rigorous error identification process will be undertaken during detailed, as the task design, HMI and procedures are developed and refined. The RP recognises the need for further work by the licensee in this area and it is captured in the FAP (Ref. 6). I consider it appropriate for the licensee to address this matter as part of normal business.

447. The current level of error identification is sufficient to demonstrate that the claimed actions are not excessively sensitive to human error, but does not assure the level of

understanding of human performance that will lead to an optimized, ALARP, design following detailed design. It may also lead to some optimism in the assessment of the strength of PSFs for use in quantification, but this is mitigated by the sensitivity analysis performed by the RP.

448. I also note the absence of any formal Workload Analysis methods, although workload and situation awareness are considered within the assessments. I discuss this shortfall further below.

Error Recovery

449. ONR expects (Ref. 4) that: “The duty-holder has examined the opportunities and options for error recovery and the potential for further human error, which could exacerbate a fault.”

450. My TSC found that the RP’s HRA submissions are predominantly success-oriented, with relatively little consideration of recovery demands presented in the analyses. Error recovery opportunities are noted within the TTA, aligned with the identified errors. However, there is little discussion of the impact of errors on the development of mental models concerning the behaviour of plant, and hence the impact of the error recovery actions and the need to repeat/revisit actions and decisions on the likely behaviours of personnel.

451. RQ-UKHPR1000-1700 and RQ-UKHPR1000-1734 (Refs 68 and 69) were raised to better understand the RP’s position on this topic.

452. The RQ responses and the later submitted HRA Summary Report (Ref. 10) provide additional expository information on the RP’s approach.

453. The RP’s approach to consideration of recovery was focused primarily on recovery from incorrect plant states, and recovery from identified failures such as the failure of a task by implementing a new task.

454. For example, Section 6.3.9 of Ref.10 states that “the reliability derived for the HBSC describes the likelihood of the potential error manifesting and leading to failure of the HBSC. The potential errors do not occur if the HBSC is a success. Therefore, the time taken to complete the success path for a HBSC is not affected by the potential errors that are identified.” It does not fully address recovery from human error as part of the overall task.

455. Section 6.3.8 of Ref. 10 discusses the potential effect of predictable failures but does so only in the context of a broad consideration of workload.

456. The approach used to date is adequate to assess the impact of an error and its recovery on the performance of the personal involved in the task. It does not fully address the potential impact of those errors on subsequent human performance.

457. However, I consider the further discussion on modelling recovery within the HRA summary report demonstrates a more thorough understanding of the importance of error recovery not shown in the HRAs and therefore provides a basis for a more detailed treatment of recovery, as appropriate, within each of the HRAs as they are developed during detailed design.

Timeline Analysis

458. ONR expects (Ref.4) that: “The Duty-holder’s task analysis demonstrates that operators can reliably perform and sustain claimed actions over timescales assumed in the safety case and under the prevailing conditions that may exist.” In addition to

providing a sufficient understanding of the task demands such that reliable performance can be substantiated, the HRA process should confirm that the tasks can be undertaken within the time available during the evolution of the transient.

459. The RP has carried out a formal process of Timeline analysis, and these are present in the submitted HRAs where necessary.

460. The qualitative assessment of time required to complete claimed actions is supported by 'Task Step Duration Data' to aid consistency between assessments and estimates of time required are usually provided for individual tasks steps. Some individual task time data have been collected from, and validated through, simulator studies, and certain overall task timings have been validated on simulators. Within each assessment, a TLA is produced to support evaluation against time required and determination of an appropriate PSF Level.

461. The way task timings have been assessed is broadly consistent with RGP. However, my TSC found several aspects of the approach that may lead to insufficient assessments. These relate to the adequacy of modelling recovery and thus providing a best estimate of task performance time and are discussed in the following section.

462. It is apparent that the presented timelines are predominantly success-oriented. My TSC did not find evidence of the routine explicit treatment of recovery actions within the timelines, even where recovery actions are claimed for certain predicted human errors. For example, the 'HRA for Isolating Impaired SG' (Ref. 58) notes that mis-identification of the affected SG is credible. An error recovery route is identified and described, involving the SE. The assessment states that the error can only be revealed after initial isolation of the mis-identified SG and hence a section of the task must be repeated. However, the timeline analysis does not model this explicitly, even though the recovery is claimed within the quantification of this HEP. Instead, the approach to determining the ability to complete the task within the time available has been to incorporate conservatisms into the assessed available time.

463. Whilst such an approach is appropriate for the inherent error recoveries that are implicit in a well-designed task (e.g. self-checking, correction of errors in control selection and operation, etc), I do not consider it sufficiently robust for those recoveries that are explicitly claimed within fault trees, such as correction by the Safety Engineer of mis-diagnosis by Operators.

464. RQ-UKHPR1000-1437 (Ref 70) was raised to seek clarification concerning the treatment of error recovery. Whilst the response provided a clearer description of how the impact of error recovery on workload is addressed, and how task timings had been derived, it did not adequately address the concern that claimed human error recovery paths should be considered when deriving overall task timings. The RQ response focused on recovery of safety functions, rather than recovery from human error. An example of the latter is where the SE identified mis-diagnosis by the MCR operators, alerted them to the error, and assisted to repeat the necessary elements of the task. The overall result was task success, but at the expense of additional actions, and task time. Further discussion of the approach to TLA has been provided in the 'HRA Summary Report' (Ref. 10). This additional information clarified the approach.

465. Some of the submitted TLAs revealed that HBSC task time exceeded available time, demonstrating that the task could not be demonstrated to be reliably completed. For example, the analysis of SGTR (Ref. 58) presented a derived timeline that exceeds the available time (and this excludes consideration of recovery from isolation of an incorrect SG). The analysis notes that this may be due to significant conservatism, and that simulator studies have indicated a shorter response. A recommendation to

address this is noted in the HRA report. I therefore consider that this is not an insurmountable challenge to the claim, but the way it will be addressed is unclear.

466. In other instances, my TSC noted that uncertainties within the timeline analysis were recognised, and a requirement for further validation of assumed timings was identified. However, these were recorded as assumptions rather than explicit recommendations for further assessment. For example, in OP_L2_FW (Ref. 57), within the assessment a need to determine the time required to open SADVs was noted, but this is recorded in the assumptions list as an assumed most onerous time constraint. Consequently, it is not clear that the expectation that the task duration will be more accurately determined will be carried forward. Whilst there is an overall recommendation to 'validate all assumptions', I consider this lack of clarity to require attention, and I discuss this further, below, against Assumptions.

467. The lack of precision in the timeline analysis was recognised by the RP, and its declared approach to address this was to identify the sensitivity of the task. This approach was not fully described in any of the methodology statements, but was later described in the 'HRA Summary Document' (Ref. 10). Sensitivity comprises a combination of the margin (absolute and relative) between required time and available time, and an assessment of the significance of any assumptions made when deriving the task times.

468. Consequently, 'sensitivity' refers to the extent to which the conclusions from the Timeline Analysis are sensitive to the accuracy of the calculated task duration and/or an increase in the overall task duration arising from additional events, tasks and/or PSFs that are not explicitly modelled in the HBSC's fault scenario. I consider this to be a proportionate response within GDA. I welcome that the RP acknowledges this shortfall and has captured it for the licensee to address during the site-specific stage.

469. The submitted HRAs tend to consider tasks in isolation and focus on the immediate responses to the transient being modelled. There is discussion of the overall scenario and hence the context in which the tasks are being undertaken. This was used to inform judgements concerning workload and concurrent task demands. Workload was predominantly discussed in terms of the impact of concurrent tasks and task complexity on overall task duration. However, my TSC did not see evidence of an explicit treatment of workload and complexity on the duration of individual task steps, or on the potential for errors and hence a need to allow additional time for error recovery. For example, as noted above in respect of Ref. 58, a bounding scenario was identified that excluded SBO as a concurrent demand. Whilst the response to SBO in this specific instance may be excluded for other reasons, it is apparent that situations such as SBO may have a significant impact on both individual task-step timings and also on the overall time to complete a task. Whilst this forms an analytical shortfall, I consider it mitigated by the wider HRA sensitivity analysis which bounds this shortfall. I am content for this to be addressed as part of normal business.

470. To conclude, given the status of the design at GDA, the additional design and operational detail being provided during the site-specific stage, and the limitations that this imposes on the HRA process, I consider that the RP's approach for TLA is acceptable at GDA given the conservatisms incorporated into the timelines.

471. In most instances, the sample assessment of TLAs that my TSC conducted shows that task success is achievable within the time available. Where time taken exceeds time available, the RP has identified this and provided additional expository discussion in relation to whether this can be explained by excessive conservatisms or genuine weaknesses in the design. Where a genuine weakness is identified, there is evidence of design changes to address it. For example, HF analysis carried out in support of the in-vessel retention safety case identified that the operator did not have sufficient time

to manually energise the valves required for the safety system activation locally. The design change changed the mode of activation from local-manual to remote-manual bringing the task time below time available.

472. Whilst the TLAs are fit for purpose for GDA, they will require more rigorous re-assessment as the detailed design of the tasks and interfaces continues during detailed design. As the RP has adequately demonstrated that it understands the importance of TLA, and has identified the need for further work in this area during the detailed design under FAP item HF- HRA -20 (Revisit the timeline analysis during the site license phase according to the design of license phase.) I consider this can be addressed as part of normal business by the licensee.

Treatment of Workload, Situation Awareness and Violations

473. "The workload of personnel required to undertake these actions and controls should be analysed and demonstrated to be reasonably achievable." (Ref. 2). The shortfalls in the TLAs, and the treatment of concurrent tasks, were also noted in the overall treatment of workload and situational awareness within the HRA submissions.

474. The RP has assessed cognitive workload by considering the impact of simultaneous task steps, memory demands, and related PSFs such as stress, time pressure, unfamiliarity and complexity. Whilst my TSC found appropriate workload factors have been captured, there was little evidence of a structured and consistent approach, and variability across the submissions.

475. The predominant analysis of workload was conducted as part of the timeline analyses; the implication being that high cognitive workload leads to increased task duration. I do not consider that this offers sufficient insight into workload impact on HBSCs. Workload is significant PSF when applied to human reliability and my TSC found that this link is not clear in the qualitative HRAs. I acknowledge that the high-medium-low PSFs for workload do feature in the HEP calculations.

476. I recognise that the extent to which workload can be assessed using such methods is limited at GDA, given that many of the factors that affect workload are not yet fully determined at this stage of the design. For example, elements of the HMI that might affect cognitive workload are not yet determined. It is positive that the RP recognises this.

477. Formal validated methods of Cognitive Workload Analysis, such as secondary task measures or Multiple Resource Questionnaires, or broader methods of workload analysis such as NASA-TLX are not appropriate for use at GDA without a high level of design maturity. However, I would expect to see a simplified approach, clearly described to ensure consistency of application, with clear links between the qualitative and quantitative HRA.

478. Without adequate guidance, workload analyses become heavily dependent on the RP's expertise in this area and may deliver inconsistent analysis quality. As workload is an emergent property, the value of analysis of workload derives from the enhanced understanding of the extent to which the factors affecting workload contribute to reduced task reliability. Without the enhanced understanding of these factors, it becomes difficult to demonstrate an ALARP design.

479. To confirm the significance of the variability in approach, my TSC sampled several the TTAs and found that many of the factors that affect workload that I would expect to see addressed were noted. For example, in HRA for Manual Water Injection to SG by ASG (OP_L2_FW) (Ref. 57), the discussion of workload notes the need to:

- coordinate multiple teams
- consequent communications demands
- the potential requirement to simultaneously conduct operations
- to determine a strategy using information from multiple sources
- and to calculate the SG injection limit which is dependent on multiple factors and which, if incorrect, could lead to water hammer

480. However, it is unclear, without repeating the assessment (which is not practical) whether this is a comprehensive list.

481. My TSC found that assessments generally appear to be suitably conservative, and the factors affecting workload are, generally, amenable to improvement post-GDA if required. However, they were unclear whether the level of conservatism is appropriate, nor the level of uncertainty. I therefore welcome the later sensitivity analysis (Ref. 10) performed by the RP to mitigate many of my TSC findings with respect to possible optimisms in the HRA.

482. My TSC found that a demonstration of: "…sufficient, unambiguous information for the operator to maintain situational awareness in all operating modes and in fault and accident conditions (e.g. the behaviour and status of the automated plant control systems)." is provided. (Ref. 2). SA is recognized by the RP as an important factor in task performance. The RP recognises (Section 3.2.3 of Ref. 57) that the assessment of SA in GDA is limited, as it is reliant heavily on HMI design and conduct of operations – both of which are out of scope for GDA.

483. My TSC found that within the TTAs, task cues and required information are captured, which I consider adequate for GDA as it establishes a basis for later task-verification exercises during the detailed. However, my TSC did note a lack of consistency between HRAs in which such information requirements was identified which will need addressing to be resolved by the licensee if it is support task-verification.

484. In addition, my TSC found that the implicit assumptions concerning the presentation of such information were not always recorded sufficiently clearly to ensure that they are carried forward into the detailed design. In some instances the key cues used for certain tasks are recorded in the Assumptions list (e.g. Ref. 57), whereas in other instances the necessary cues are noted in the TTA but not recorded in the Assumptions list (e.g. Ref. 58).

485. I consider this reduces the value of the HRAs undertaken at GDA. The need to review all HRAs for implicit assumptions during detailed design is included in the FAP (Ref. 10) and is welcomed and will be an ideal opportunity to address the consistency shortfall noted here.

486. ONR expects that violations be "qualitatively identified" along with a demonstration that the design "minimises violation producing conditions". (Ref. 4). I can confirm potential for violations has been considered by the RP. The RP states that assessment of the control of violations is not viable at GDA, which I concur with, but has sought to identify opportunities for violation to identify measures for reducing those opportunities, such as engineered defences and physical barriers, and to assess the extent to which it is reasonable to claim the use of administrative controls that are to be developed during the site-specific stage. I consider this approach adequate given the limitations of GDA. However, I would expect the outputs from such violations assessments to be collated as part of the implicit assumptions review noted above.

487. To conclude, on the basis that the suite of HRAs substantiate[†] – or where this is not the case, design improvements have emerged from the HRA – I am content that the RP's approach to analysing Workload, Situation Awareness and Violations is adequate for GDA. I consider the development of the violation assessment to be part of normal business.

4.5.2.3 Dependency

488. This section presents my assessment of the RP's analyses of inter and intra HBSC dependency. I have used TSCs and their assessment of HRAs to inform my regulatory judgements on this topic.

489. The HRA TAG guides that: "…dependencies between human actions must be accounted for to avoid underestimation of risk. The potential impact of dependency between separate activities (either by the same or by different persons) should be assessed. The HRA should qualitatively consider the effect of dependency on reliable human performance. Dependency should also be "factored…into their HEP estimates."

490. Requirements for the assessment of dependence between human errors comprising a Human Failure Event (HFE) are well established in regulatory guidance on HRA. ONR's TAG on PSA (Ref. 4) establishes the expectation that "Dependencies between HFEs appearing in the same accident sequence are identified and accounted for". It sets further expectations that:

- The process by which the candidates for dependency were identified is transparent.
- Any assumptions made in the dependency analysis are described and justified.
- The determination of the degree of dependency is transparent and justified.
- The method by which the conditional probabilities of dependent HFEs are calculated is clear.

491. These expectations are consistent with those expressed in ONR TAG 063 on HRA (Ref. 4) and they also reflect guidance provided by IAEA in its Specific Safety Guide on Level 1 PSA (Ref. 71) which emphasises that dependencies among HFEs in the same sequence can significantly increase human error probability, and the interdependencies should therefore be identified and quantified within the analysis, adding -

492. "All measurable cut-sets involving multiple human failure events should be identified. Such cut-sets can be identified by setting the human error probabilities to a high value (e.g. 0.9) and recalculating the core damage frequency; the cut-sets involving multiple human failure events will then appear at the top of the list of cut-sets. The set of human failure events that are combined in the same cut-set should be reviewed to determine the degree of dependency between them; the human error probabilities used in the quantification of the model should reflect this degree of dependency."

493. Within the context of the qualitative assessments presented in the HRA reports, I would expect to see a clear discussion of dependency within and between HBSCs, i.e., between members of the operating teams, and within the tasks undertaken by a single person.

494. A qualitative assessment of dependency underpins the assessment of the HBSC. It is necessary to both, determine the strength of identified dependencies to inform the HRA, and to provide insight into opportunities to reduce the potential for dependency, to support the ALARP position. The quantitative treatment of dependency within the PSA, i.e. across separate branches of the modelled fault trees is discussed further in

[†] *– To the degree possible within the scope of GDA*

Section 4.5.3 when considering the methods for quantitative assessment. It is also subject to wider assessment within the PSA Assessment Report (Ref. 52)

495. The RP's method for identifying and assessing potential human error dependencies is described in Revision B of its 'HRA Methodology' document (Ref. 67). Potential dependencies have been identified by setting all HEPs to 0.1 and then reviewing the minimum cut-sets. Where two or more HBSCs are present in a cut-set, the HBSCs are selected for dependency analysis. This is consistent with the approach adopted in other GDAs.

496. The RP's consideration of Dependency is discussed in Ref. 64. The approach described is restricted to the dependency considered numerically within the PSA. Mt TSC noted a lack of clarity in the RP's submissions with respect to its qualitative treatment of dependency.

497. The text within the 'HRA Summary Report' (Ref. 10) failed to provide the necessary confidence that the qualitative insights from its approach were both suitable and sufficient. The description appears primarily to focus on dependency between HBSCs, as stated in Section 5.4.1 of Ref. 10 and does not discuss in detail dependency between actions that deliver a single HBSC. It does note, within Section 5.4.2 of (Ref. 10), that there is potential for dependency between various combinations of errors including those in pre-initiating activities, initiating events, and post-initiating event activities. However, it does not clearly acknowledge the potential for dependency between different post-initiating event activities, i.e. between the various actions that might be demanded in response to an event.

498. I would expect to see further qualitative consideration of dependency, particularly with respect to dependencies that might arise within a fault sequence, such as where recovery actions are claimed, by the licensee during detailed design. Dependency will need to be revisited as a topic during detailed design as drivers such as task design and organisational structure are not defined during GDA. I am content for this be followed up during normal business.

499. Within each HRA, there is a discussion of dependency. A simple model is presented, comprising an evaluation of the extent to which the factors that affect dependency are present, i.e. same/different person/team; same/different time; same/different location; same/different task/cues. I consider that the approach is appropriate for GDA, in principle, but it has not been executed in a manner that is sufficiently conservative. However, the RP has conducted a wide sensitivity analysis across the HBSCs within the PSA using HEP failure rates from .1 in order of magnitude steps to determine whether there are any HBSCs that are particularly important in plant risk terms. I consider this bounds the lack the potential for optimism numerical terms, but does not when it comes to insight into the design of SSC and task design.

500. By the nature of dependency, there are many opportunities that are available during detailed design for further reducing the potential for dependency. I therefore would expect to see a conservative approach to the identification of dependency, in order to guide attention during detailed design, i.e. to identify sensitivity to dependency.

501. In my TSC's assessment of the HRAs they noted a number of instances where low dependency is claimed as a consequence of 'changes in crew' (e.g. Ref. 66 and Ref. 72). The changes are often restricted to a different person operating within the same MCR. In other instances, low dependency is claimed due to 'different location' or 'different time' (e.g. (Ref. 72) whereas both persons are in the same MCR and responding to the same transient. I therefore consider that the opportunity to further reduce dependency has not been fully determined by the RP, and that the significance

of some of the implicit claims (e.g. concerning use of different procedures by different personnel) may not be fully recognised.

502. Some HRAs also consider dependency inadequately. For example, Ref. 58 declares that no potential dependency has been identified. It concludes this on the basis of consideration of inter-claim dependency (i.e. there are no preceding HBSCs within the fault sequence). It does not explicitly consider the potential for intra-task dependencies other than where there is complete dependency (i.e. failure of a preceding task will defeat the claim).

503. Whilst the RP's methodology document acknowledges that there is potential for dependency to occur between Type B and Type C HFEs, no Type B – Type C dependency pairings are identified and evaluated within the RP submissions reviewed. This means that within the HRA, dependency has only been considered for human errors that occur during post fault tasks. I do however acknowledge that the limitations that design detail and the lack of a developed maintenance regime, can make it difficult to perform a meaningful assessment of some potential coupling mechanisms.

504. For GDA, the RP has assumed zero dependency between Type A failures. I consider this to be an in-valid assumption. The RP should have recognised that this may be a false assumption as it has itself noted the likelihood that the same item is present in redundant trains and could be maintained by the same team. Furthermore, the claim of zero dependency between Type A HFEs reduces the value of the HRA programme for informing the detailed design and the development of licensee arrangements, as it will not identify the sensitivity of EMIT arrangements that might increase the potential for dependency.

505. However, at the end of GDA, the RP has recognised that further work will be needed in this area during detailed design, and notes this in the HRA Summary Report. The RP also cites the need for the licensee to re-assess Type A dependency in the FAP (Ref. 10).

506. The RP's methodology document (Ref. 67) states that potential dependencies among different combinations of Type A, Type B and Type C HFEs will be examined, however in the 'HRA Summary Report' (Ref. 10), only dependencies between Type C HFEs are considered.

507. A further source of dependency that I do not consider has not been adequately addressed is the Auto Diagnosis feature. Claims are made concerning the ability of the operators both to monitor the performance of the AD, and to respond to AD failures. I consider this gap acceptable for GDA as the development of the AD, its HMI, and the supporting conduct of operations will be developed by the licensee. I am content for this to be addressed during detailed design as part of normal business. Evidence could also be gathered as part of the resolution of AF-UKHPR1000-0151.

508. To conclude, whilst I did identify several shortfalls in the RP's treatment of dependency during GDA, they are minor (bounded by the wider HBSC risk sensitivity work carried out by the RP), and significant further work on dependency will be carried out during detailed design, as design and operational detail and maturity increases. I therefore consider the treatment of dependency within GDA to be suitable and sufficient and am content for these shortfalls to be resolved as part of normal business.

4.5.2.4 Qualitative Analysis of Type A Failures

509. This section presents my assessment of the RP's analysis of pre-initiator failures. It is based upon independent assessment work performed by my TSC. It considers the use of generic tasks for the assessment of Type A failures.

510. ONR expects (Ref. 2) that: “The human reliability analysis should include: pre-fault human actions during maintenance, calibration or testing activities where error could result in the non-availability of equipment or systems important to safety…”.

511. Type A Failures are those that occur prior to the initiation of a fault sequence. Typically they arise as a consequence of maintenance activities, and might be expressed as a calibration error, or a safety system not being made available, such that the claimed performance of the SSC cannot be delivered. They can also include the operator directly hazarding the plant, which should not be the case for reactor operations if it complies with the engineering hierarchy, but may be possible in other areas of the design such as within the fuel route, e.g. crane operations.

512. The approach to the identification of Type A failures is set out in Ref. 67. This presents a high-level description of the approach and the data sources used.

513. The intention by the RP is to eliminate opportunities for Type A failures where reasonably practicable, prior to substantiation. Where this was not possible, the RP elected to submit a suite of bounding assessments relating to a range of risk important SSCs. Given the multiplicity of potential forms of a Type A failure, I would expect to see assessment of generic activities, such as Valve Maintenance, Instrument Calibration, etc. Given that such activities are both normal practice in any system, and also well-understood, I am content with such an approach.

514. My TSC sampled two of the generic Type A assessments:

- Human Reliability Assessment Report for Instrument Calibration Activity (Ref. 55), as a representative example of a generic task.
- Human Reliability Assessment for Safety Valve Maintenance Activity (Ref. 44) as an example of a more focused Type A activity.

515. When undertaking a generic Type A assessment, I would expect to see a clear definition of the scope of the task, a clear description of the data sources used to model the generic task, ideally based on examples drawn from relevant existing systems and plant, and a structured approach to task description, error identification, and error recovery. I would also expect to see representation by relevant subject matter experts (both engineering, safety analysis and HF).

516. My TSC confirmed that this is the approach that the RP has followed.

517. A suitable and sufficient assessment in this area should provide confirmation that the design has taken account of operating experience to optimize these activities and avoid repeating design deficiencies, and in doing so demonstrate that the tasks can be substantiated. They should also provide guidance for the licensee when considering the organisational and administrative arrangement assumptions made that will deliver reliable performance.

518. The two submissions assessed by my TSC follow a broadly similar structure but show differences in the levels of detail. This can be explained by the evolution of the RP’s HRA method, differences in analysts undertaking the work, and possible differences in design maturity. Neither assessment explains how formal OPEX has been used to inform the assessment, although it could be argued that using suitable SMEs with experience of the SSCs of interest will bring a degree of informal OPEX learning to the assessment.

519. Whilst the attendees at the analysis workshops are described for the Valve Maintenance HRA, and those attendees include SMEs with valve maintenance

experience, the Instrument Calibration HRA only refers to a maintenance SME without clarifying their experience. No other sources of OPEX are cited.

520. I consider this to be a deficiency, as there should be operating experience data concerning types of errors, frequency of errors, and the performance of error reduction and recovery arrangements. I consider that such data are of particular importance for generic Type A assessments and their omission reduces the validity of the assessment. However, given that these maintenance tasks are both well-understood and familiar, I consider that the conclusions are broadly reasonable and appropriate and consistent with what I would expect.

521. The RP notes in its FAP (Ref. 6), that that further work will be required by the licensee during detailed design as the engineering and task design detail is developed.

522. My TSC noted that the valve maintenance assessment (Ref. 44) provides a description of the use of SHERPA for error identification. As noted above, this is not a method that appears in the declared methodology, although I consider it to be appropriate. It is not clear how error identification was undertaken for Instrument Calibration. However, my TSC examined the TTA for Instrument Calibration and considered that the identified errors are broadly appropriate with respect to an analysis undertaken at GDA.

523. Both reports present a set of assumptions and a set of recommendations. For Instrument Calibration, the set of assumptions is detailed, and provides guidance for the development of task design and procedures. For example, Assumption A7 notes specific information to be included in Procedures. The Safety Valve Maintenance assessment does not provide the same level of detail within the Assumptions List.

524. This difference in outputs reduces the confidence that the value of the various HRAs undertaken during GDA will be maximized during the detailed design, nor that the opportunity to identify risk reduction opportunities has been fully realized. As this work will, by the necessity of taking account of further design and operational details, be updated during detailed design, the identified shortfalls should be ameliorated as part of normal business. Updating the suite of HRAs to take account of design maturity and UK specific operational requirements / decisions is also declared on the FAP for resolution by the licensee.

525. Within the ‘HRA Summary Report’ (Ref. 10) it is stated that there is zero dependency between Type A failures. Whilst this assertion is incorrect, I do not consider it reflects a lack of understanding by the RP, as I note the intention to consider Type A dependency during the detailed design which will be an opportunity to address this shortfall.

526. To conclude, I consider that the approach to the assessment of Type A failures is broadly appropriate and consistent with RGP. However, I have noted some aspects of the two assessments that fall short of what I would expect. I do not consider that the shortfalls materially affect the validity of the Type A failure assessments at GDA, but they will need to be addressed as the HRAs are updated during detailed design either as part of normal business or in the resolution of AF-UKHPR1000-0153.

4.5.2.5 Qualitative Analysis of Type B Failures

527. This section presents my assessment of the RP’s analysis of initiating failures. It is informed by independent assessment by my TSC.

528. ONR expects (Ref. 2) that: “The human reliability analysis should include:…actions that contribute to initiating events…”.

529. Type B Failures are those that directly initiate or contribute to faults. I would not expect a modern PWR design to be susceptible to significant numbers of Type B failures during reactor operations. My TSC confirmed that the RP's design meets this expectation; there are no high-risk contribution Type B errors within the internal events L1 or L2 PSAs.

530. The set of HBSCs presented by the RP indicates that the principal Type B failures arise within the Fuel Route, and hence my TSC's scope of assessment focussed on this area. They sampled the Human Reliability Assessment Report for Fuel Handling Operations (Ref. 56) to assess the qualitative analysis of Type B failures as this has the highest potential and contribution when it comes to Type B risk.

531. When undertaking a Type B assessment of a new design I would expect to see a clear definition of the scope of the tasks, a clear description of the data sources used to model the tasks (ideally drawing on relevant analogues from existing SSCs) and a structured approach to task description, error identification, and error recovery. The RP's approach for Type B analysis is set out in Ref. 64, and the approach and data sources used aligns with my expectations for GDA. I also take confidence from the indication in the FAP (Ref. 6) for the licensee to undertake further HBSC identification during detailed design.

532. The Fuel Handling Operations report states that the development of the Fuel Route HRA is an iterative process, reflecting the design development process. The report indicates that the HRA process feeds into the design development, which I consider appropriate.

533. The assessment reported in (Ref. 56) appears to be based primarily on workshops and a visit to a training facility (Daya Bay) with a full-size representative fuel route. Training personnel and fuel route operator SMEs were represented during the data collection.

534. Three items of OPEX are cited in the report, two of which appear to be drawn from the operation of plant similar to the generic UK HPR1000 design and one drawn from a French NPP. Two of the items refer to operator failures and one refers to task complexity that is considered undesirable. I consider this to be a limited set of OPEX. Whilst other OPEX may have been drawn upon through the experience of participants at the workshops, there are no auditable record of these inputs. The report distinguishes 11 groups of activities to represent the process of fuel handling from receipt to loading into the reactor. Using these sub-tasks as the basis to search for other relevant OPEX may have identified additional useful data. For example, lifting activities that are not fuel route related.

535. I am therefore not confident that the full benefit of this assessment has been realized, with respect to informing design improvements, or to informing the quantification of error probabilities. However, the RP has identified within the FAP the need to update the OPEX reviews, along with updating the HRA as the design and operational details of the fuel route are developed further.

536. Ref. 56, notes that a human error analysis was undertaken using an agreed set of error modes. The report does not provide a description of how this was undertaken, or what the set of error modes comprises. It is therefore not possible to confirm that the set of errors presented in the TTA is complete. However, having assessed the TTAs, and the identified errors, my TSC concluded that they appear to be reasonable, including errors of omission and commission, and those affected by design of tasks and interfaces.

537. The assessment has excluded consideration of Type A and Type C failures. The assessment notes at various points that other errors could occur when performing the

tasks (e.g. Section 6.11) which 'would be Type A latent errors'. They are not noted or discussed further. My TSC noted that it was therefore unclear where and when such failures will be assessed for UK HPR1000. I consider this to be an omission, although I do not consider it to undermine the Fuel Route assessment, given that further significant regulatory assessment will be undertaken during the detailed design and the generic fuel route is subject to significant design change as a result of RO-UKHPR1000-0014 and RO-UKHPR1000-0056.

538. Given the iterative nature of the assessment, and the current level of design maturity, assumptions have been made for areas where no detail yet exists. However, these are noted against the individual THERP data sheets rather than being drawn together in a coherent assumptions list, and my TSC reported that it was not clear how these were recorded and fed forward into the ongoing design process. The fuel route assessment was one of the earlier ones and I note that the RP has got better at capturing assumptions as the GDA has progressed.

539. To conclude, I consider that the approach to the identification and assessment of Type B failures is broadly consistent with RGP and appropriate to a design undergoing GDA. However, I do not consider the presented assessment of the Fuel Handling Operations is sufficiently rigorous in terms of the methodology for data sources and error identification to fully substantiate fuel route activities. I consider this acceptable for GDA given the significant further assessment work which will underpin the fuel route design changes born out of GDA. These shortfalls can be addressed as part of the ongoing design programme. The licensee will need to take cognisance of the assessment presented in this report and improve the assessment process. I consider this to be normal business.

4.5.2.6 Qualitative Analysis of Type C Failures

540. This section presents my assessment of the RP's analyses of post-fault human actions. It was supported by independent assessment work by my TSC. The scope of the Type C failure analysis represents the bulk of the RP's submission and also provides further detail of the implications for the analysis of workload, dependency and cognitive errors of the methods and data used by the RP.

541. SAP EHF.10 guides that: "The human reliability analysis should include…post-fault human actions and long-term recovery actions in severe accidents.".

542. Type C failures are those that can aggravate an initiated fault sequence or act to defeat or impair claimed defences. I expect the RP's assessment to focus on substantiating the claims associated with minimising significant Type C failures.

543. The approach to the identification of Type C failures is set out in Ref. 63. This presents a high-level description of the approach, the data sources used, and aligns with my expectations. I welcome the intention to eliminate opportunities for Type C failures where possible, prior to substantiation.

544. The substantiation of Type C failures comprises the most detailed and comprehensive suite of HRA undertaken by the RP as it underpins many of the risk-significant HBSCs.

545. As part of my assessment, my TSC sampled the HRA reports listed below. Their sample was selected to represent a range of fault sequences and activities, including fault diagnosis and MCR response, and error recovery activities.

- Human Reliability Assessment for manual water injection to SG by ASG (OP_L2_FW) (Ref. 57) (severe accident)
- HBSC Reliability Assessment for restarting RHR pump manually (OP_RHR_S1) (Ref. 66) (action required to achieve safe state)

- Human Reliability Assessment Report for Isolating Impaired SG Manually (OP_ISO_SGTR) (Ref. 58) (diagnostic demands)
- HBSC Reliability Assessment for isolating break by operator manually (OP_ISO_LOCA) (Ref. 73) (coordination of tasks)
- Human Reliability Assessment for Performing Low Head Safety Injection (cold leg and hot leg) (OP_LHSI_HC1) (Ref. 74) (re-orientation of procedures)
- Human Reliability Assessment for Isolating the Source of Dilution (Ref. 75) (task timings)

546. For GDA I would expect the HRA for Type C errors to:

- Present a risk informed and proportionate substantiation of the totality of the identified HBSCs.
- Present a clear description of the safety function, and the fault sequence within which it is claimed.
- Include a summary of the fault sequence in the context of the reactor state and operations being undertaken when the sequence was initiated, in order to provide a description of the environment and context in which the claimed human actions are being undertaken.
- Present a clear and justified description of the assumptions that underpin the assessments and demonstration of a proper understanding of human performance and the factors that will affect reliable delivery of the claims.
- Present a clear linkage between the outputs from the assessments (including the assumptions) and the more detailed assessment, validation and verification to be undertaken during detailed design and the site-specific stage.
- Show clear links between the qualitative analyses of human performance and the judgements concerning the strength of identified PSFs that is then used within the quantitative analyses.

547. Each of the assessed submissions follows a broadly similar structure, although they are not fully consistent. This is explicable by the continuous improvement efforts demonstrated by the RP throughout GDA.

548. The submissions generally present:

- The scope of the report.
- The fault sequence.
- Relevant OPEX.
- Description of the analysis applied.
- Commentary on situational awareness.
- Commentary on cognitive workload.
- Commentary on violation.
- The qualitative assessment undertaken.
- The quantitative assessment, derived from the qualitative analysis.
- An overall judgement on demonstration.
- Assumptions made during the analysis.
- Shortfalls and recommendations.
- Conclusions.

549. Based on my TSC's assessment, I consider this broadly meets my expectations for GDA.

550. The descriptions of the fault sequence focus on the evolution of the transient. They do not present a clear description of the expected state of the plant immediately prior to the transient, and hence the likely global PSF that may be present at the point of fault initiation.

551. Subsequent qualitative assessments seek to assess factors such as stress or workload, etc. only as an overarching factor, i.e. they do not consider these might affect specific errors and actions.

552. The assessments present the bounding conditions that have influenced the selection of the transient for analysis. Whilst these are based on risk, and derived from the PSA, they may not fully represent the most onerous task conditions from an HF perspective.

553. The 'HRA Summary Report' (Ref. 10) presents further description of how the bounding conditions have been identified, and claims that this process includes consideration of available task time, complexity of action and consequence. However, the extent to which this approach has been consistently applied is not clearly articulated in the RP's submissions. For example, OP_L2_FW (Ref. 57) considers Anticipated Transient Without Trip (ATWT) as the most onerous condition. It excludes SBO. SBO may, however, provide a more challenging set of conditions for staff within the MCR. I would expect further analyses undertaken during detailed design to consider alternative operating conditions and transient evolutions, and note that the scope of the HRA will be need to be increased during the site-specific stage. I consider this normal business. The need for the HRA scope to increase is also identified by the RP in the FAP for the licensee to address.

554. Use has been made of both HTA and TTA to model the tasks under assessment. This is aligned with RGP. My TSC found that the level of modelling is proportionate to the development of the design represented during GDA – noting the previously discussed methodological shortfalls in section 4.5.2.2.

555. To conclude, I consider that the approach to the identification and assessment of Type C failures is broadly consistent with my expectations for GDA. It provides confidence that there are no tasks associated with Type C HBSCs that are likely to be incapable of substantiation during detailed design. However, I have noted a number of aspects of the analyses where I consider that a more rigorous and complete assessment could have been undertaken, and where it has therefore placed a greater demand on the detailed design and substantiation work still to be undertaken:

- Further analyses will be required during detailed design to consider alternative operating conditions and transient evolutions within the treatment of bounding scenarios and task complexity.
- The use of OPEX for Type C failures will need to be improved for the detailed design.
- A more rigorous error identification process for Type C failures will need to be undertaken post-GDA, as the task design, HMI and procedures are developed and refined. I also consider that a more detailed treatment of error recovery will be required within each of the HRAs as they are updated during the site-specific stage.
- Further analysis of operator action task timings will required during the detailed design.
- Improvements to the analysis of workload, situation awareness and violations analysis will be required during the detailed design.
- Improvements to the post-fault action dependency analysis will be required during the detailed design.

556. Collectively, this suggests that the RP's understanding of human performance, and the relevant PSF, may not yet be at a level that fully supports detailed design and the development of the licensee organization and arrangements. However, I am pleased to note that the RP notes in its FAP that significant further work will be required by the licensee. This work is summarised in 4 FAP items associated with the expansion and

improvement in the quality of the HRA. I consider these shortfalls are suitably captured by AF-UKHPR1000-0154.

4.5.3 Quantitative Human Reliability Assessment

557. This section presents my assessment of the quantitative aspects of the RP's HRA. It is split into the following sub-sections:

- Assessment of GDA HRA Scope
- Assessment of Screening and Bounding of HBSCs.
- Assessment of Quantitative Human Reliability Methods
- Assessment of Quantification of Human Error Probability (HEP)
- Assessment of Overall Human Contribution to Risk

558. It is important to note that this area of my assessment focusses mainly on the numerical risk modelled in the HF derived HRA submissions. The reader is directed to the PSA assessment report (Ref.52) for the overall acceptability of the HRA architecture within the PSA.

4.5.3.1 Assessment of GDA HRA Scope

559. This section presents my assessment of the RP's approach to the inclusion of HEPs for human actions in the various risk models and fault schedules. It was supported by independent assessment by my TSC.

560. The totality of the HRA for the generic UK HPR1000 design is presented across approximately 30 separate documents, with 4 documents addressing aspects of HRA methodology and the other documents presenting qualitative and quantitative assessment of selected HBSCs.

561. My TSC noted that the 'HBSC list' report (Ref. 50) includes details on HBSC identification but provided insufficient detail on:

- The process of bounding scenario selection.
- The results of completed analysis.
- Collated HBSC data (e.g., actual HEP values and risk insights).

562. Furthermore, they found a lack of clear 'sign-posting' to highlight links between the HRA documentation meant that it was difficult to conclude that the case as a whole is coherent.

563. In response to regulatory feedback in this area, the RP produced the 'HRA Summary Report' (Ref. 10). This submission provides an improvement in the coherency of the HRA. It provides details of HRA scope and method development through GDA, describes HRA integration with wider project design development and safety justification activities, and presents analysis results with discussion of risk insights, which I refer to below where relevant. It also includes the latest HBSC data for each of the PSA models (Ref. 10 – Appendix H) provided in response to RQ-UKHPR1000-1734 Collated HBSC Data (Ref. 50), which I refer to as I discuss the distribution of HBSCs throughout the PSA Type A HBSCs.

Scope of HRA - Type A HBSCs

564. Type A errors are identified across the PSA models. Whilst generic UK HPR1000 design is evolutionary based on operational plant, the approach to assessment reflects the current level of design detail and the lack of a developed maintenance regime for the this design. Type A errors are grouped into three basic error types, which have been assessed at the genetic task level:

- Mis-alignment of manual valves.
- Mis-calibration of safety valves (i.e. Pressure Relief Valves).
- Mis-calibration of flow / level transmitters.

565. These were subject to generic task analysis and subsequently quantified to provide conservative screening data for use in the PSA. My TSC concluded that the RP has taken a proportionate approach to assessing Type A errors, which aligns with my expectations for GDA as many of the factors significantly affecting task performance, such as job design, training and procedures, are not available during GDA.

566. I also note that the identification of Type A HBSCs is not limited to those listed within the PSA models, and that four discrete EMIT tasks were identified for assessment that do not fit the generic tasks identified above. Specific analysis was undertaken in each case. These additional Type A tasks comprised:

- Maintenance of the Pressuriser, specifically – replacement of the heater.
- Maintenance / replacement of the Low Head Safety Injection pump.
- Steam Generator Access and Inspection.
- Reactor Pressure Vessel Head Assembly Lifting

567. My TSC examined the Type A HBSC listing across the various PSA models as presented in the response (and duplicated in Appendix H of the HRA Summary Report) to gain insight into the distribution of risk significant Type A HBSCs amongst the total population. The distribution for the IEAP Level 1 PSA is presented in Table 5 below.

Table 5: Type A HBSCs within the IEAP Level 1 PSA

Generic Error Grouping	Risk Significant HBSCs	Low Risk HBSCs	Total
Mis-alignment of manual valves	19	42	61
Mis-calibration of safety valves	0	8	8
Mis-calibration of flow / level transmitters	6	13	19
Totals	25	63	88

568. When assessing HRA Summary Report regarding the proportionate assessment sample for Type A HBSCs, my TSC found some discrepancies.

569. The HRA Summary Report identifies a total number of 118 Type A HBSCs within the latest 'Internal Events Level 1 PSA' (Ref. 69), 40 of which were risk significant and are presented in its Appendix F. It does not clarify what revision of the PSA model or supporting document is being referred to as the 'latest' version.

570. There were further discrepancies as the FV values for the same risk significant Type A HBSCs, were different in Appendix F than in Appendix H. My TSC was unable to ascertain whether this discrepancy was the due to the inclusion of superseded data

from a previous iteration of the PSA model, or whether the datasets in each appendix had been subject to different treatment within the latest PSA model.

571. The HBSC listing provided in response to RQ-UKHPR1000-1734 Collated HBSC Data includes a total of 1065 HBSCs across 11 PSA models.

572. Of these HBSCs, 700 entries are Type A errors. On examination, the bulk of these are multiple repeated entries for the same HBSCs, throughout multiple PSA models. As Type A errors are 'pre-initiator', the fault or hazard context has no impact on the task performed or human error likelihood, so my TSC interrogated the data to identify unique HBSC entries, of which there were 170. They noted discrepancies in the 'HRA Summary Report' (Ref. 10), which does not discuss high risk Type A HBSCs beyond the scope of the *Internal Events Level 1 PSA* and explicitly states that "from the latest Internal Events Level 2 PSA, no high-risk Type A HBSCs is found. No type A HBSCs are chosen from the Internal Events Level 2 PSA". My TSC identified several risk significant HBSCs in the Level 2 PSA, including some that are only risk significant in the Level 2 PSA as illustrated in Table 6 below. My TSC also identified risk significant Type A HBSCs that are unique to other PSAs including models for the Spent Fuel Pool, and several the internal and external hazards PSAs.

Table 6: Example of Risk Significant Type A HBSCs within the Internal Events Level 2 PSA

PSA Model	HBSC ID	HBSC Description	FV	RAW
Internal Events Level 2 PSA	EHR1102VPM_EC	Error closure of manual valve EHR1102VP at the suction of EHR1101PO	2.45E-03	4.06E+00
Internal Events Level 1 PSA	EHR1102VPM_EC	Error closure of manual valve EHR1102VP at the suction of EHR1101PO	3.66E-04	1.46E+00
Internal Events Level 2 PSA	EHR1103VPM_EC	Error closure of manual valve EHR1103VP at the discharge of EHR1101PO	2.45E-03	4.06E+00
Internal Events Level 1 PSA	EHR1103VPM_EC	Error closure of manual valve EHR1103VP at the discharge of EHR1101PO	3.66E-04	1.46E+00
Internal Events Level 2 PSA	EHR1810VPM_EC	Error closure of manual valve EHR1810VP at the discharge of EHR1101EX	2.45E-03	4.06E+00
Internal Events Level 1 PSA	EHR1810VPM_EC	Error closure of manual valve EHR1810VP at the discharge of EHR1101EX	3.66E-04	1.46E+00

PSA Model	HBSC ID	HBSC Description	FV	RAW
Internal Events Level 2 PSA	EHR2102VPM_EC	Error closure of manual valve EHR2102VP at the suction of EHR2101PO	2.38E-03	3.97E+00

573. Whilst the inconsistencies in the data presented in the HRA summary report slightly undermine confidence that a coherent and complete assessment of human errors has been presented, my TSC did not consider this to be significant as the discrepancies are small overall.

574. I explored the cause of these discrepancies with my PSA colleagues and with the RP. They can be attributed to two parallel, but not sufficiently integrated, HRA work streams. One derived by the HF team and one derived PSA team. The lack of integration appears to be caused by the significant amount of HRA work done at pace in the later stages of GDA. I consider it sufficiently mitigated by the sensitivity analysis performed.

575. However, this shortfall does not meet ONR's expectation that qualitative modelling should be used to substantiate any HBSCs and that this be used to inform the associated quantitative human error modelling. Without these links the HRA risks missing factors that may be important to error and ultimately safety. It is this holistic task analytical process that ONR understands by the term HRA. I am pleased to note that the RP recognises this shortfall and has captured this for the Licensee to address during detailed design in its FAP.

576. Given the importance to the safety case of a suitably integrated approach to HRA I therefore raise AF-UKHPR1000-0154 to ensure sufficient regulatory oversight during the site-specific stage.

AF-UKHPR1000-0154 – The licensee shall, as part of detailed design, ensure that an integrated and holistic approach is adopted to develop the human reliability analysis. This should ensure that:

- The qualitative Human Factors analysis informs the quantification of the human errors in the Probabilistic Safety Analysis (PSA).
- The PSA considers the outputs from the HF engineering programme, where appropriate.

577. From my TSC's review of the 170 unique Type A HBSCs identified in the PSA models, I am confident that there is sufficient alignment with one of the three generic bounding cases identified for detailed analysis. I discuss this further when I address bounding cases below.

Scope of HRA - Type B HBSCs

578. A small number of Type B errors are identified within the PSA models (see table 7). These are duplicated across several of the PSA models.

579. Type B errors are expected to be essentially designed out by good engineering practice on modern reactor plant during normal at-power operations. This is because considerable international effort has been expended upon developing reactor

protections systems that provide protection against human errors that pose single failure weaknesses in the design.

580. My TSC identified disparities in the HRA data presented by the RP. The 'HRA Summary Report' (Ref. 10) states that no risk significant Type B HBSCs have been identified from the PSA and therefore none are analysed in detail (Ref. 10: Section 4.2), which contradicts the data presented in RQ-UKHPR1000-1734 Collated HBSC Data (summarized in Table 7), and also Appendixes F and H of the summary report where the risk significant Type B HBSCs below are also identified. I believe this is further evidence of misalignment between the PSA and the HRA work as they have each developed iteratively. Whilst I consider this acceptable for GDA due to sensitivity analysis work performed by the RP, a more robust integrated approach, will be required for the detailed design. This is captured by AF-UKHPR1000-0154.

Table 7: Example of Risk Significant Type B HBSCs within the Internal Events Level 1 PSA

PSA Model	HBSC ID	HBSC Description	FV	RAW
Internal Events Level 1 PSA	OPB_DVLRAE_MC	Recover the function of DVL damper	3.86E-02	1.35E+00
Internal Events Level 1 PSA	OPB_ISO_MSSV	Reclose MSSV manually	5.83E-03	1.22E+00
Internal Events Level 1 PSA	OPB_RHR_TR3	Start RHR 3 train manually	5.10E-05	1.00E+00

581. Whilst the lack of detailed analysis for the risk important HBSCs represents a gap in the generic safety case, the RP has conservatively placed no high reliability claims on the associated HBSCs. The HEPs claimed within the PSA are relatively high (from 1.00E-01 to 2.60E-02).

582. Three additional Type B HBSCs were identified for detailed analysis by the RP from a list of PIEs and OPEX review (Ref. 10: Section 4.2), which are listed below. Given the level of design and licensee arrangement detail available during GDA, I consider this proportionate for GDA.

- Fuel Handling Operations.
- Heterogeneous Boron Dilution.
- Liquid Waste Discard.

Scope of HRA - Type C HBSCs

583. Of the 1065 HBSCs identified in the response to RQ-UKHPR1000-1734 Collated HBSC Data, 355 entries are Type C errors. As with the Type A HBSCs, a significant number of the Type C HBSCs result from multiple repeated entries for what is essentially the same Type C error, throughout multiple PSA models.

584. However, unlike Type A errors, the Type C errors represent a failure to perform required actions during post fault recovery and therefore the fault or hazard context may differ between PSA models, impacting on the required response. For this reason, my TSC did not interrogate the data to identify unique HBSC entries, but did explore how similar Type C errors are represented by bounding scenarios. This is discussed in Section 4.4.1.3 below.

Notwithstanding these multiple entries, I have examined the Type C HBSC listings across the various PSA models as presented in RQ-UKHPR1000-1734 Collated HBSC Data (and duplicated in Appendix H of the HRA Summary Report) in order to understand how they are distributed across the models, including risk significant HBSCs, as presented in Table 8 below.

Table 8: Distribution of Type C HBSCs across PSA Models

PSA Model	Type C HBSC	Risk Significant HBSC
Internal Events Level 1 PSA	77	23
Internal Events Level 2 PSA	89	26
Spent Pool Internal Events Level 1 PSA	26	16
Fire Internal Events Level 1 PSA	29	9
Fire Internal Events Level 2 PSA	23	8
Flooding Internal Events Level 1 PSA	22	13
Flooding Internal Events Level 2 PSA	26	9
External Hazard Level 1 PSA	24	12
External Hazard Level 2 PSA	19	5
External Flooding Level 1 PSA for Reactor Core	10	0
External Flooding Level 1 PSA for Spent Fuel Pool	10	7
Totals	355	128

585. As with the Type A and Type B HBSCs, my TSC found discrepancies. Examples include:

- Only 9 risk significant Type C HBSCs are identified for the Internal Events Level 1 PSA scope within the HRA Summary Report, compared with 23 in Table 8 above.
- Only 7 risk significant Type C HBSCs are identified for the Internal Events Level 2 PSA scope within the HRA Summary Report, compared with 26 in Table 8 above.

586. The HRA Summary report describes the HBSCs selected for detailed assessment from across the various PSA models, without stating the total number of risk significant HBSCs, making it difficult to draw further comparison. In total, 23 Type C bounding cases are defined in the HRA Summary Report and subject to detailed analysis. These

HBSCs are summarized below. My TSC also identified another bounding assessment of HBSCs for 'Internal Fire PSA' (Ref. 76) that was missing from this list of 23, which they considered in their assessment.

Table 9: Overview of Type C Bounding Cases selected for details assessment

Source	Bounding cases
Internal Events Level 1 PSA	10
Internal Events Level 2 PSA (and SAA)	5
Spent Pool Internal Events Level 1 PSA	2
Fire Internal Events Level 1 PSA	1
Fault Schedule (DSA)	4
Internal Hazards Analysis (DSA)	2
Total	24

587. I explore the degree to which these cases bound similar HBSCs across the scope of the HRA in Section 4.5.3.2 below.

588. The following exceptions from detailed analysis are listed in the HRA Summary Report. "There are also many Type C HBSCs found in the External Flooding Level 1 PSA for Spent Fuel Pool, they are bounded by the same ones in Internal Event Level 1 PSA"

589. My TSC checked the full list of HBSCs (Ref. 69) and found that most of the risk significant HBSCs from the External Flooding PSA, are indeed duplicated from the Internal Flooding Internal Events Level 1 PSA. They confirmed that the majority of these are assessed in the 2 bounding cases.

590. For those HBSCs that are similar between the PSAs, they noted that scenarios initiated by the occurrence of a hazard may present different challenges to operators than those considered in an Internal Events analysis. Fire, Flood, and Seismic events can all impact negatively on the working environment, availability of important equipment, and stress / workload levels, which I discuss further in Section 4.4.1.3.

591. "For the External Events Level 1 PSA, after discussion with PSA and external hazard area, the high risk Type C HBSCs are similar as the Type C HBSCs in Internal Events Level 1"

592. My TSC confirmed this to be true, except for 2 HBSCs with the description "Perform trip of CRF pump manually", which are both risk significant. Again, it should be noted that scenarios initiated by the occurrence of a hazard may present different challenges to operators, which I discuss further in Section 4.4.1.3.

593. Additionally, my TSC noted that an External Hazards analysis has identified a Type C event for analysis in the site-specific phase. It is not clear why it was not assessed during GDA. The event is "Opening of Secondary Passive Heat Removal System SPHRS[ASP] circulation pumps and manual valves to heat the SPHRS[ASP] tank".

594. “The other HBSCs from the Fault Schedule, which are not relied on the transition from the controlled state to the safe state, have enough available time because these actions completion time is not sensitive in safety calculation.”

595. My TSC confirmed that a total of 5 Class 1 HBSCs have been identified in the Fault Schedule and they are all addressed within the 4 Fault Schedule (DSA) bounding cases. They expected several Class 2 HBSCs to be identified for detailed analysis in line with the RPs screening methodology (see Section 4.4.1.3), but were unable to find any examples. However, I do not consider this to be a significant omission as I would anticipate that given their nature there is likely to be considerable overlap between Class 2 HBCS in the Fault Schedule and HBSCs in the PSA.

596. To conclude, I consider the RP’s approach to the identification of HBSCs to be generally sound, displaying most of the attributes that constitute RGP. Whilst a detailed assessment of HRA integration within the PSA logic models is outside of scope of my assessment, I have been able to confirm that:

- HBSCs are fully integrated into the Level 1 and 2 PSAs.
- All modes of operation are considered, along with the fuel route and the most significant hazards.

597. Whilst there are some limitations with respect to detail, these are generally commensurate with the design detail available during GDA.

598. Although my TSC observed discrepancies amongst the data reported in the RPs outputs, I judge that these are likely a result of the HRA Summary Report being released at Revision A late in the GDA process, and therefore being the first attempt to present the whole case, issued without the benefit of iterative review and update. I consider the HRA Summary report adds significant value to the RPs submission, alleviating many of the difficulties that I, and my TSC, have observed when navigating the suite of HRA submissions prior to its issue.

599. In summary, I consider that the RP has employed effective methods for the identification of HBSCs and the scope of HRA presents a coherent and sufficient set of human reliability claims for GDA, within the constraints of design maturity and licensee input. I have identified some omissions from scope which I have noted and it is my expectation that these will be addressed by the licensee during the site-specific stage as part of the development of the HRA and PSA.

Whilst the HRA Summary Report has been a recent enhancement to the case and serves as a good platform from which to build from in the site-specific stage, improvements in how the HRA is iterated will be required during these stages. There is a need for improvements in the integration between the qualitative and quantitative elements. This is covered by AF-UKHPR1000-0154.

4.5.3.2 Assessment of Screening and Bounding of HBSCs

This section presents my assessment of the RP’s application of human error screening and bounding methods, where I consider the RP’s screening criteria used to identify risk significant HBSCs (or ‘high risk’ HBSCs as the RP occasionally describes them), and whether the RPs approach has ensured production of a proportionate HRA. It was supported by independent TSC assessment work.

Screening Criteria

600. It is disproportionate and impractical to analyse every human action performed on a NPP; particularly for GDA. For SAP EHF.5, guides that Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of

the safety functions to which they contribute. Thus, a means of screening or identifying importance is necessary.

601. The RP defines two levels of analysis for HBSCs within its methodology documents: Task Analysis Method (Ref. 63) and Treatment of Important Actions Implementation Plan (Ref. 64). A 'Detailed Level' and 'High Level' assessment. Within these documents it defines the criteria for categorizing HBSCs. My TSC compared the adequacy of these criteria to RGP.

602. HBSCs obtained from the PSA are screened based on PSA importance measurements; specifically RAW and FV values. HBSCs are deemed to be risk significant if the RAW>=2,or FV>=0.005.

- RAW values provide insight into the importance of a human action with respect to plant risk. They show what increase, in core-damage frequency or large radioactive material release, would be expected if the task of interest was assumed to fail. For example, if a RAW value of 2.0 is revealed when an error probability is set to one (failure), this shows that if it failed, the result would be a doubling (100% increase) in plant risk.
- FV measures the overall percent contribution of cut sets containing a basic event of interest to the total risk. They are calculated by finding the value of cut sets that contain the basic event of interest and dividing by the value of all cut sets representing the total risk.

603. For HBSCs obtained from the DSA or SSA, risk significance is determined based on the Safety Function Category or the SSC Class of the safety system affected. Class 1 and 2 HBSCs are deemed risk significant and subject to detailed analysis. This approach is broadly commensurate with methods applied to an engineering category and classification assessment and is welcomed for GDA as it aligns with best practice for a modern standards safety case.

604. My TSC found the criteria applied for GDA prioritisation to be appropriate in reducing the number of HBSCs for further analysis to a manageable number. Whilst there is no universally agreed RGP in this area, the PSA risk importance values do align with previously used criteria on other GDAs. I do note, however, that the use of risk as the dominant criteria in the screening process has a tendency to narrow the analysis and does not necessarily result in providing evidence to demonstrate an ALARP position. Typically, FV and RAW values identify similar tasks, centred on small number of key locations and/or components. Consideration of task novelty and complexity criteria could have helped provide greater evidence for the ALARP demonstration.

605. From my TSC's assessment of the HRA scope (Section 4.4.1.2) I am satisfied that these criteria have been applied correctly by the RP, with only a small number of exceptions as is illustrated in Table 8 above. These I have ascribed to misalignments between the HRA and the PSA models as they each develop iteratively.

Bounding Scenario Definition

606. The definition of 'bounding case' within the ONR SAPS (Ref. 2) is "A single situation used to represent a wider class of situations that is more extreme than any member of the class in all important respects". By their nature bounding scenarios are likely to introduce a level of conservatism into the associated HEPs, but used properly they can simplify the modelling of human failures and reduce analysis effort.

607. The HRA Summary Report (Ref. 10) includes a section titled 'Bounding Case Explanation', which explains that where the same action may be claimed in many

accident sequences, the bounding case is determined according to the following aspects.

- The high frequency events
- The event with the fast process (timescale) and severe consequences
- The complexity of the human action.

608. My TSC found it difficult to find examples of bounding cases that were selected based on task complexity. Evidence that complexity was considered in the selection of bounding cases is provided for some Type A HBSCs, namely the HRAs for 'RPV Head Assembly Lifting and the Removal' (Ref. 77), and the HRA for 'Maintenance of the Pressuriser Heater' (Ref. 78), however the dominant criteria for selection of bounding scenarios are risk significance and the time available.

609. For Type C HBSCs, each of the detailed HRA assessments provides a summary of the top cut-sets featuring the HBSC of interest, ensuring that event frequency is considered during bounding scenario definition. The selected bounding cases are typically described as 'the most onerous for the operators' based on time available to respond, without acknowledging that task complexity is also a factor in determining how onerous a task is, and consequentially how reliably it can be performed. This is supported by my TSC's observations on the consideration of PSFs applied to Type C HBSCs. They found only a small number of HBSC included a PSF for complexity above a 'nominal' level (see Section 4.4.1.5). These examples tend to be HBSCs identified within the Level 2 PSAs, reflecting the difficult decision making typically associated with a devising a Severe Accidents response strategy (i.e. determining the damage to plant and selecting an appropriate strategy which may involve a release of activity to the environment), rather than the selection of a particularly complex bounding scenario.

610. However, among the individual HRA reports sampled for my TSC's assessment (see Section 4.4.1.5), and among the wider population of HBSCs that have been subject to detailed HRA, several the features that they considered to be typical of 'complex' scenarios are included in some of the HBSC scenarios.

611. Examples of such features include the co-ordination of Local-to-Plant actions, response to beyond design basis faults, and scenarios that occur during shut-down plant configurations. My TSC did not find evidence that coincidental loss of I&C had been considered within any scenarios, something I would have particularly expected to see for HBSCs that feature in internal or external hazards analysis (i.e. as a result of damage to sensors, transmitters, cables, or other related equipment).

612. The extent to which the assessed bounding cases are claimed to be representative of similar HBSCs which haven't been subject to detailed assessment, is not very clearly defined.

613. There are 88 Type A HFEs within the 'Internal Events Level 1 PSA' (Ref. 69) and all of them fall within the three bounding cases defined according to their HBSC description. However, only 45 of 88 have been allocated a more conservative 'HBSC HEP' from the bounding assessment, and the remaining 43 have 'N/A' in the column 'Link to justification for bounding assessment". Additionally, the 612 Type A HBSC entries in the other PSA models also have no bounding case linked. Clearly as these are pre-initiators, the bounding should apply equally across all models. This suggests that the majority of Type A HBSCs identified have not been linked to a bounding assessment although one exists for them, and the PSA risk calculations are based on the potentially optimistic HEPs that are not linked to and substantiated by the detailed HRA work.

614. My TSC sought to understand the extent to which bounding cases are claimed to be representative among Type Cs HBSCs, and again found it difficult due to a lack of clarity. For example, many HBSCs are identified as bounded by the 'HRA for Feed and Bleed' (Ref. 59), which covers HBSCs for implementing Feed and Bleed, Manual Start-up of the SBO DG, and Cross Connection of ASG tanks.

615. In total, 33 of the 77 Internal Events Type C HBSCs are bounded by this assessment, however only the Feed and Bleed error (OP_FB_SLOCA_A) was quantified. The calculated HEP for OP_FB_SLOCA_A has been declared "not valid" as it was assessed in a pilot study [HRA Summary Report (Ref. 10) – section 13.5.5]. The bounding case explanation (Ref. 10) states that OP_FB_SLOCA_A "is similar with all other similar feed and Bleed HBSCs", which means that this may have been intended to bound all 74 Feed and Bleed HBSCs across all PSA Models.

616. On examining the 278 HBSCs that are listed within PSA models other than the Internal Event Level 1 PSA, my TSC could not identify any unassessed HBSCs linked to a bounding case. They did find some statements within the HRA Summary report to infer that bounding cases would apply across PSAs, for example, "There are also many Type C HBSCs found in External Flooding Level 1 PSA for Spent Fuel Pool, they are bounded by these same ones in Internal Event Level 1 PSA ". Also, "For the External Events Level 1 PSA, after discussion with PSA and external hazard area, the high risk Type C HBSCs are similar as the Type C HBSCs in Internal Events Level 1 PSA".

617. My TSC noted that it would be difficult to bound a HBSC from a hazards PSA using an assessment from an internal events PSA without supporting justification, as the hazard context can introduce additional challenges impacting on reliability, which in turn can increase the HEP due to negative PSFs for environmental conditions, availability of important equipment, and stress / workload levels.

618. Effective implementation of a bounding approach to HBSC assessment, is an essential element of proportionate HRA. It provides an opportunity to leverage the benefits gained from detailed HRA substantiation by justifying its applicability to a wide population of HBSCs within the PSA, which in turn ensures that estimations of the human contribution to risk are underpinned by qualitative HF assessment. I consider the RP has done enough in this area for GDA, as it has resulted in a reasonable selection of detailed HRAs, which cover a wide scope of task types. However, improvements to clarity and approach for the identification and demonstration of bounding assessments will be required for the site-specific stage. I consider this normal business.

4.5.3.3 Assessment of Quantitative Human Reliability Methods

619. This section presents my assessment of the RP's selected methods for quantitative HRA, including comparison of the methods with RGP and review to confirm correct application of the methods. It is supported by independent TSC assessment work.

HRA Methods

620. ONR's HRA TAG (Ref. 4) guides that: "The methodology/ies selected for the HRA, and in particular for the evaluation of human error probabilities (HEP), including the choice of human reliability data sources, is/are justified.".

621. The methods selected for quantification of human error by the RP are described in the 'Methodology of Human Reliability Analysis' (Ref. 67). US Nuclear Regulatory Commission (NRC) HRA methods have been chosen primarily because of the RPs familiarity with their application, and due to their wide-spread use internationally over many years on nuclear design projects. The RP has argued that its selection of HRA

tools is based on a combination of US Nuclear Regulatory Commission (NRC) provenance, and its familiarity with these methods. As familiarity has been shown to be a key determining factor in producing best estimate HEPs, I am content with the RP's decision here.

622. The methods selected were:

- Type A Errors are modelled–using the Accident Sequence Evaluation Program (ASEP) (Ref. 37). ASEP is essentially a simplified version of the Technique for Human Error Rate Prediction (THERP) (Ref. 79).
- Type B Errors have been quantified using THERP (Ref. 80).
- Type C Errors are quantified using the Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) (Ref. 81), which is also a modified version of THERP intended to reduce analysis effort.

623. A review of HRA Methods conducted by the Health and Safety Executive (Ref. 82) classifies all of these methods as '1st Generation' HRA methods, the first tools developed to support quantification of human error. All the methods selected are based on THERP, which is recognized and widely applied within the UK.

624. However, THERP was developed at a time when analogue displays and controls were the norm in NPP MCRs, which means it has internationally recognised weaknesses concerning the ability to model HCI. Whilst the generic UK HPR1000 HMI design has yet to be developed, it will be operated predominantly via screen-based computer interfaces as per the FCG3 reference design.

625. Unless a suitable HRA method is identified, this could prove an analytical challenge during detailed design. The challenges of modelling human interaction with modern HCI are not insignificant. The types of interactions and potential error mechanisms can differ significantly from those found in a typical analogue control room, both in terms of frequency and complexity.

626. There is ongoing research in this area internationally that I would expect the Licensee to draw from. It is thus encouraging that the RP has recognised this weakness in the modelling approach since the first issue of its 'Human Reliability Quantification Methodology' in 2019 (Ref. 83), and has identified this need for the licensee to develop an approach for modelling HCI in the PSA in the FAP (Ref. 6).

627. However, the RP claims to have addressed this methodological weakness in part in its updated methodology (Ref. 67) by making some "optimizations", which appear to be limited to changes to task timings and some basic unsubstantiated assumptions relating to workload, situation awareness, and error likelihood that they appear to suggest can be addressed using more training. to improve reliability. I do not consider these optimisations demonstrate an understanding of the challenges that exist. I therefore raise the following AF.

AF-UKHPR1000-0155 – The licensee shall, as part of detailed design and substantiation of the human machine interfaces, implement a validated human reliability analysis approach for screen-based interfaces. This should be underpinned by relevant research on human machine interfaces.

628. All the selected HRA methods tend to drive a very mechanistic approach to HRA, particularly with ASEP and SPAR-H. Both methods drive a tick-box approach to HRA, which means their focus is on generating numbers for the PSA rather than offering risk insights into the task of interest.

629. Their application by the RP has largely mirrored the US model of HRA, which separates the qualitative HF Engineering (HFE) and the quantitative HRA elements, with the respective work commonly undertaken by different teams and requiring little integration. A failure to adequately integrate the HRA into the PSA and consider the human performance effects of the design, can lead to an unrealistic and superficial estimate if not modelled with suitable conservatisms. This is the subject of AF-UKHPR1000-0154 raised earlier.

630. ASEP was developed to enable systems analysts to make estimates of HEPs that are sufficiently accurate for use in PSAs, in short timescales, with limited training, and with minimum support and guidance from experts in HRA.

631. When applied to pre-initiator tasks, a generic error probability, which cover errors of omission and commission is applied to all tasks, and is subsequently modified by applying appropriate pre-defined recovery factors. The recovery factors reflect how the maintenance or calibration error could be identified and recovered, such as alarms prior to operations resuming, a post maintenance test, or post maintenance checks.

632. It is a simple technique to apply and tends to produce conservative results that are traceable. I consider it is well suited for its application in support of the generic UK HPR1000 GDA, where it is essentially providing screening HEPs for generic per-initiator errors for the PSA models. However, given its simplicity it does not necessarily lead the RP to consider all potential influencing factors and it provides limited insight for error reduction and design enhancements / optimisations towards an ALARP solution.

633. If sufficient design detail was available, I would have expected to see a more thorough analysis method applied to the pre-initiator HBSCs that are found to contribute significantly to risk post GDA. Given the lack of design maturity, I consider the use of ASEP at this stage appropriate. However, I would expect a more rigorous assessment and quantification of Type A errors for the detailed design. This expectation is captured in the previous Assessment Finding AF-UKHPR1000-0154. It should also be resolved as the wider HRA is updated during detailed design as part of normal business.

634. In the absence of any practical Generation II HRA tools, THERP remains a benchmark for a structured approach to HRA. It is an internationally recognised and accepted HRA tool.

635. However, THERP does not adequately treat cognitive processes that cannot be simplified to commission and omission errors. Where there is no THERP defined task which resembles the task under consideration, THERP can become difficult to apply. As the content of the error tables are control room biased, THERP can also be difficult to apply to complex activities ‘Local to Plant’, such as maintenance and fuel route operations.

636. For this reason, whilst THERP provides the analyst with sufficient flexibility to account for PSFs, it may not always provide a clearly applicable error type for some tasks that are typically the focus of Type B HRA i.e., maintenance activities, local to plant, lifting operations, and fuel handling activities associated with the fuel route. I discuss the application of the method and the results obtained by the RP further in Section 4.5.3.4.

637. SPAR-H (Ref. 81) method was developed as a further simplification of THERP, specifically to address the need to develop HRAs to support the Standard Plant Analysis Risk (SPAR) generic PSA models used by the US NRC. SPAR-H provides only two categories of activities— one is the probability of error in decision-making whilst the other is error probability during the execution of actions. Consistent with other methods, decision-making is considered less reliable than the skill-based

execution of actions. However, these baseline probability estimates are derived by taking an average from a range of more precisely described probability estimates that are provided in the THERP method.

638. Quantification in SPAR-H is not validated for newer technology applications, and therefore the licensee will also need to consider whether an alternative approach would be better to model the complex human computer interactions associated with modern HMI.

639. SPAR-H uses a 'check-box' approach, which utilizes fixed error mechanisms and associated probabilities without the need for an underpinning task analysis. In this respect it is a faster but less investigative method than THERP. It also provides very limited guidance on the identification and modelling of human errors, which in turn can limit its value in identifying risk reduction measures.

640. In the context of GDA, the scope for modelling the task context is limited to the application of 3 PSFs. Its application therefore relies entirely on the analysists level of HF expertise as the method does not mitigate the lack of experience like THERP.

641. The substantiation weakness in the SPAR-H method was raised early in GDA with the RP, and then again when shortfalls were noted in the early HRA submissions. In response the RP developed a template for HRA which required a task and error analysis to underpin all three HRA methods. The addition of the template adequately mitigated the SPAR-H substantiation weaknesses for GDA.

642. To conclude, I consider the RP's selection of HRA tools to be suitable for GDA. Given the importance of RP's familiarity in producing best estimate HEP data, I judge that, on balance, the use of proven and familiar methods outweighs the analytical shortfalls in the ASEP and SPA-H methods. Further, the RP has introduced mechanisms (prescriptive HRA template) to mitigate the lack of qualitative insight that these methods can suffer from. However, I would expect the licensee to make enhancements, either through the adoption of more insightful methods, or via improvements to the approach followed for GDA. I consider this achievable as part of normal business and as part of the resolution of AF-UKHPR1000-0154 and AF-UKHPR1000-0155.

Treatment of Dependency in HEPs

643. ONR TAG 0063 guides that: "The potential impact of dependency between separate activities (either by the same or by different persons) should be assessed. The HRA should qualitatively consider the effect of dependency on reliable human performance. …the duty-holder has also factored these considerations into their HEP estimates."

644. Failing to take proper account of dependency can fail to deliver a best estimate HRA due to building in excessive optimisms. In turn, this can lead to a failure to identify where a qualitative assessment of dependency is necessary.

645. ONR's assessment of HRA dependency within the PSA is predominantly discussed in in the PSA assessment report. In summary, it concludes that:

- The RP determined that there were no dependent sets of Type-A HEPs because they were due to failures during independent EMIT activities. The RP's reasoning for Type-A dependency is logical.
- The RP determined that there were no dependent sets of Type-B HEPs because there were no sets of Type-B errors. As Type-B errors lead to IEs, they are all analysed individually, rather than in a set. The RP's argument Type-B HEPs dependency modelling are sensible.

- The RP found several sets of potentially dependent Type-C HEPs and conducted dependency analysis on each of these sets. As a result, several values were changed in the PSA model for those HEPs found to be dependent to reflect the increased probability of failure of the subsequent HEPs in a set after the initial human error. ONR's assessment of a selection of Type-C HEP dependency calculations found them to be accurate.
- The RP performed inter-type dependency analysis (for example Type-A-Type B, etc) and did not find any applicable dependent sets. ONR's assessment of the RP's arguments has confirmed their findings.

646. To conclude, for GDA, the RP has performed and suitable and sufficient assessment of dependent failures in the HRA. However, there are weaknesses in the qualitative approach (see section 4.5.2.3).

647. For the site-specific stage, a more sophisticated and insightful analysis of dependency (intra and inter-task) will be required to ensure that the dependencies are actively identified, suitably and sufficiently modelled and mitigated to reduce risk ALARP. As the approach to modelling dependency is well-supported in RGP literature I consider this can be addressed by the licensee as part of normal business.

4.5.3.4 Assessment of Quantification of Human Error Probability

648. This section presents my assessment of the RP's quantitative analysis of Type A, Type B and Type C human errors, including consideration of the degree to which the quantification of HEPs and potential human error dependencies reflect the task context, error mechanisms, and PSFs identified in the qualitative assessment. It was support by independent assessment work by my TSC.

649. ONR SAP EHF. 5 guides that: "Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety."

650. It is my expectation that the RP has appropriately and proportionately applied its HRA methods to produce HRA data that is suitably best-estimate, taking account of the design and operational uncertainties associated with GDA.

651. To assess whether HEPs produced during GDA were suitably best estimate – or at least conservative – and appropriately modelled, my TSC sampled from the RP's HRA submissions, the sample list referenced in each section below. Their sample was selected based on:

- Selecting from each of the Error Types (i.e. Types A, B and C),
- Selecting actions modelled across the range of PSA models,
- Selecting scenarios that covered a range of Plant Operating States,
- Selecting actions to cover a range of HEP values (from 6.11e-01 for an action claimed under severe accident conditions, to 1e-05 based for a long timescale Spent Fuel Pool (SFP) fault on application of a HPLV).

652. I would expect:

- HRA analyses should be supported by a clear description of the claimed operator actions, safety function being supported, and the fault sequence within which it is claimed.
- Bounding scenarios should represent the most demanding conditions for the operators, so I would expect scenarios to be defined that include feature details of degraded conditions due to the fault or hazard context, such as unavailable systems or concurrent challenges to be managed.

- Wherever assumptions are made to address gaps in knowledge or available information due to the constraints of GDA scope for example, these should be clearly stated and captured for validation at a later point.

653. My TSC found that the detailed assessments have generally provided a sufficient description of the scenario within which the claim on human action is made. Assumptions are being captured, although my TSC noted several instances where assumptions are being tacitly made and not then captured in the assumptions table within the report.

Type A Errors

654. My TSC sampled three Type A HRA reports to inform my judgement. These comprised:

- HRA for Safety Valve Maintenance (Ref. 45)
- HRA for Typical Valve Maintenance (Ref. 65)
- HRA for Instrument Calibration (Ref. 55)

655. My TSC found inconsistencies between the level of quantitative assessment undertaken in each analysis. However, they concluded that there was sufficient information to support quantification using the ASEP methodology.

656. Due to the limitations of the methodology, the RP was not able to assign a probability of error that directly reflected the potential error mechanisms identified. In each case a basic HEP of 0.03 was used to reflect possible errors of omission and errors of commission. Where poor procedures or HMI could degrade task performance, this can be modified to 0.05, but appropriately for GDA, these factors were assumed not to negatively impact on task performance. Whilst other PSFs cannot be addressed in the quantification, my TSC noted that the qualitative assessment has considered them and raised assumptions and recommendations related to these.

657. The basic HEPs were modified by the selection of appropriate Recovery Factors, with recovery likelihood dependent on the means available to identify and recover the initial error to be available. My TSC noted that each of these assessments is presented as a representative case for multiple similar HBSCs.

658. Given the broad application of these assessments, my TSC found that the claimed recovery factors and the corresponding HEPs were appropriately conservative.

659. The HEP for instrument calibration errors is based on an assumed functional test that was not confirmed by qualitative assessment during GDA. Without this assumption, the overall HEP would be 1.4e-01, which my TSC considered would be excessively conservative for a calibration task. The final HEP with this assumption accounted for is 2.4e-03, which I consider to be reasonable for a generic HEP for calibration activities, given the limitations on detailed information during GDA.

660. In all cases, the TSC found that each of the identified error mechanism is summed to provide the final HEP, with no requirement to consider intra-task dependency. The HEPs derived for the valve maintenance activities are calculated as 6.0e-03 for Typical Valves and 3.3e-03 for Safety Valves. Whilst the Safety Valve assessment has identified more potential error mechanisms, justification is provided for more reliable recovery factors to be claimed. In both cases, I judge the HEPs to be reasonable for use as a representative HEP for generic tasks during GDA.

661. In their review of the HEP data provided in response to RQ-UKHPR1000-1734 ‘Collated HBSC Data’ (Ref. 69), my TSC noted that the HEPs derived from these detailed assessments are higher than the corresponding ‘screening’ HEPs’ already

included in the PSA. They also noted that two of the HEPs have not been included correctly, with a HEP of 2.4e-03 recorded for Typical Valves and 3.0e-03 recorded for Safety Valves.

Type B Errors

662. Type B errors are unlikely to occur in isolation within the control room during normal at power operations, due to the high levels of automation and reactor protection afforded by modern reactor design. The 'HRA Summary Report' (Ref. 10) identifies only a small number of Type B errors within the Internal Events L1 PSA, stating that none of them are categorized as risk significant based on PSA importance measures.

663. Typically, Type B errors with conventional and nuclear significance are more likely to occur outside of the control rooms, e.g. fuel route and waste management, or where there is less automation within the design. For this reason, my TSC sampled the 'Fuel Handling Operations HRA' (Ref. 95) as the basis of their assessment of the adequacy of the Type B error HRA.

664. They found that tasks and error mechanisms identified within the assessment are underpinned by suitable and sufficient qualitative analysis. However, they note that the methodology for the identification of errors lacks clarity and could be improved upon (see Section 4.3.1.6).

665. The RP applied the THERP methodology to the assessment of Type B HFEs. The THERP methodology has a focus on control room operations, and whilst it can be applied to operations outside the control room, it can be difficult to identify representative error mechanisms from the THERP tables for some potential errors. My TSC identified that the THERP Table for errors of commission in operating manual controls has been applied to the task of selecting the correct container on a truck, which is stretching the validity of its application.

666. This approach is repeated throughout the assessment, with the same data applied to a failure to coordinate a crane move and a number of crane move errors resulting in collision. Similarly, they found that the THERP data for the selection of un-annunciated displays is incorrectly applied to several errors including incorrect attachment of a lifting hook to a fuel assembly, and errors associated with raising and lowering the fuel assembly.

667. They found that the resultant HEPs are generally conservative, and therefore appropriate for the GDA phase, so the consequences of the misapplication of THERP are likely minor. However, this does weaken the validity of the resulting HEPs. The lack of any acknowledgement that THERP lacks validity for modelling these HBSCs is of concern as it undermines the confidence in the competency of the analysts. Whilst the apparent conservatism mitigates this for GDA, I do not consider that it would be appropriate to continue this approach during the detailed design. However, I consider this shortfall easily resolvable during detailed design so consider it normal business.

668. Consideration of Type A HBSCs was excluded from the scope of the Fuel Route HRA. This is because the RP states that the management and operational aspects of the Fuel Route are not established for GDA.

669. The RP does however identify the need for the licensee to carry out a detailed HRA of the fuel route during detailed design (Ref. 6).

Type C Errors

670. My TSC sampled the following HRA submissions for their assessment of Type C errors:

- Human Reliability Assessment for Bleed and Feed, ASG Tank cross Connect and Start SBO (Ref. 59) (Reactor at Power; features in identified HFE dependency pairings).
- Human Reliability Assessment for starting Low Head Head Safety Injection – Safety Injection mode manually (Ref. 84) (Low Power / Shutdown conditions).
- Human Reliability Assessment for manual water injection to SG by ASG (OP_L2_FW) (Ref. 57) (Severe Accident conditions; Level 2 PSA model).
- Human Reliability Assessment Report for Loss of Spent Fuel Pool Cooling (Ref. 85) (Long timescale scenario; SFP PSA model).
- Human Reliability Assessment Report for the human actions in hazards analysis (Ref. 86) (Hazard context).

671. Their sample was selected to provide a representative range of Type C error types.

672. The type C assessments have generally provided a sufficient description of the scenario within which the claim on human action is made. However, the potential for concurrent demands on operators, has not been accounted for systematically (see Section 4.3.1.7).

673. In the assessment for starting low head safety injection in safety Injection mode manually' (Ref. 84), the potential for concurrent demands is not identified and tasks success is stated to be contingent on two HBSCs. The impact of the concurrent demand is not considered in the qualitative assessment and hence not reflected in the resultant HEP. Instead, an assumption that this second HBSC will not impact on task completion, on the basis that the concurrent demand would introduce conservatisms that impact on PSFs.

674. Whilst I am pleased that this point is addressed within the assessment and captured as an assumption, I would have expected the additional demand to have represented the most challenging scenario for the operators and therefore to have featured in the assessment.

675. In RQ-UKHPR1000-1135 'Risk Importance of HBSC' (Ref. 87) the RP states that "human actions relevant to hazards will be identified and assessed for all the hazards protection measures (including defence-in-depth measures) addressed in hazards schedule to obtain a comprehensive list of human based safety claims". This is an important claim because, whilst the assessments generally define the claimed action and the scenario context adequately, the assessments my TSC sampled did not present an evaluation of the impact of internal or external hazards on task performance.

676. The HRA for human actions in hazards analysis (Ref. 86) considered two claims from the Internal Hazards DSA related to preventing a potential fire and terminating an internal flood by isolating the source of a leak. Whilst I would expect the latter of these claims to feature a response conducted under degraded conditions, the scenario was selected as worst case based on volume and flow rate (activation of the fire protection system). It included direct indication and alarms to direct operators to the source of the flood. The scenario does not address a leak at all, and does not represent the difficult task of identifying and isolating one leak source from many. I do not consider this shortfall to be significant as the sensitivity analysis mitigates this for GDA and it can be readily addressed by a licensee during detailed design.

677. I have discussed in Section 4.3.1.3 the use of OPEX to inform quantification of human error. Whilst it can be difficult, as differences between designs, operating philosophies, and safety culture can make it difficult to apply the lessons learned to a new design, I would still expect to see an attempt to draw from a broad range of available OPEX, to support assertions that all credible error mechanisms and PSFs have been identified.

From my TSC's review of OPEX available in the public domain, they were able to identify a number of events related to Feed And Bleed, Low Head Safety Injection manual initiation, and loss of HMI that could have informed the RP's assessments. Whilst disappointing that this was not done, I do not consider it significant for GDA. The RP has identified in its FAP that the licensee will need to conduct further OPEX work, so I consider this can be addressed as part of this during normal business during the detailed design.

678. The SPAR-H method permits the analyst to dismiss the Diagnosis or the Action aspect of a task if appropriate arguments can be substantiated, but my TSC noted that all HBSCs in their sample included both the Diagnosis (DT1) and Action (AT1) components of human error for the claimed operator action. They also noted that in each of the assessments, the analysis has identified key safety significant steps from the TTA that include significant human errors with the potential to impact on task success, which they considered to represent good practice. As SPAR-H provides fixed HEPs for the diagnosis and action errors, the analyst must modify the associated PSFs to address the scenario, task context, and the significant errors related to the diagnosis and action tasks.

679. Many of the assessments claim recovery from human error by the Safety Engineer (DT2), who arrives in the MCR 15 minutes after the entry into Emergency Operating Procedure (EOP) conditions and implements their procedure on a dedicated control panel, independently of the ongoing tasks by the MCR Crew (see Section 4.3.1.7). Where conditions for EOP have not been met [47], this claim on recovery has been omitted, as is appropriate. However, my TSC noted that the claimed recovery actions are not consistently assessed in respect of reliability and impact on task timings.

680. Whilst credible error mechanisms were identified within the qualitative assessments, direct links between the failed task (AT1) and the recovery diagnosis by the Safety Engineer (DT2) are not identified within the assessments. My TSC found no discussion on how and when such errors would be revealed, or indeed whether such errors might have exacerbated the situation because of an error of commission.

681. Additionally, the assessments assume that just detecting the prior error is sufficient to ensure recovery, without considering what actions would be required (i.e. an AT2 component), and whether they can be completed in the corresponding timescale. In this regard, all claims on recovery by the Safety Engineer present an optimistic and unsubstantiated position.

682. Based on my TSC's assessment, I am content that the methodology has been applied appropriately as it relates to the justification of selected error mechanisms for GDA. However, the failure to adequately assess the contribution of the Safety Engineer role in the HRA does not meet RGP, and therefore will need to be resolved by the licensee as part of normal business during the detailed design.

683. A recognised objective of qualitative HRA is to identify the PSFs for the worst-case conditions under which the demand on the operator may be made. It is my expectation that the HRA should examine how the various factors that can influence reliable human performance and factor these considerations into estimates of human error probabilities.

684. Not all the PSFs available within the SPAR-H methodology have been considered in the assessments, due to the limited information available during GDA. My TSC therefore focussed on those that were considered in the RP's considerations of PSFs for Time Available, Stress and Complexity.

685. My TSC found that the time available to perform the claimed actions is usually conservative as the bounding scenarios are typically selected on the basis that the least available time is the most challenging situation. The qualitative assessment of time required to complete claimed actions is supported by 'Task Step Duration Data' to aid consistency between assessments and estimates of time required are usually provided for individual tasks steps. Within each assessment, a TLA is produced to support evaluation against time required and determination of an appropriate PSF Level. Whilst this approach is generally in line with good practice, My TSC identified aspects of the qualitative work that undermine the analysis and will require re-evaluation during detailed design (see 'Timeline Analysis' in Section 4.3.1.7).

686. Whilst my TSC found that the approach to evaluating the PSF level for available time is generally sound, the assessment of loss of spent fuel pool cooling (Ref. 85) they sampled, presents qualitative information that suggests the PSF level should be 'time available is approximately the time required' according to the SPAR-H method (a PSF multiplier of 10). Instead, the RP has selected 'insufficient information' (a PSF multiplier of 1). This assessment also states that 'The current prioritisation of activities is likely to delay the implementation of the claimed actions beyond the timescale that is available for the bounding scenario'.

687. My TSC concluded that the way in which this HRA was modelled to be optimistic. I would also have expected the assessment to dismiss any claims on recovery by the SE in this instance due to the lack of time, but this has been credited and the HEP modified accordingly.

688. Within the assessments that my TSC sampled, only one HBSC has assigned a nominal level of stress to the related tasks, which is justified on the basis that the related alarms are not high priority and there is no direct threat to plant safety (Ref. 86). All other assessments assigned either high or extreme stress PSFs, and their application was broadly in line with the guidance offered. For example, extreme stress was applied to a scenario that occurred during severe accident conditions involving core damage and an environmental release (Ref. 57).

689. The PSF for task complexity enables the analyst to modify the basic HEP to account for task difficulty or ambiguity. It also enables account to be taken for mental effort required, such as performing mental calculations, or utilising detailed mental models of system function. A nominal level is applied where there is little ambiguity regarding task requirements, and variables or inputs involved are easily managed. As ambiguity, the number of variables, or the degree of unfamiliarity with the situation increases, so does complexity. I would expect to see that scenarios that involve multiple system failures and/or coordination of LTP actions, should be categorised above nominal levels of complexity. Or, at the very least a robust substantiation provided to why they are not considered complex.

690. From the HRA reports that my TSC sampled, they noted that only one HBSC (OP_L2_FW) was assigned a complexity level above nominal (Ref. 57). In this scenario, there are multiple alarms occurring without a specific alarm related to the claimed action, there is a requirement for precise calculations to be performed, and there is a deficiency in information provided to do this, which has resulted in a recommendation to improve this. HBSCs are assigned a nominal level of complexity despite the need for many low significant actions to be performed and concurrent demands related to another HBSC (Ref. 84), or despite multiple equipment failures and the need to coordinate LTP actions (Ref. 86).

691. Whilst most assessments have some general discussion around the impact of a loss of Automatic Diagnosis function, none of the assessments sampled by my TSC identified related error mechanisms or PSFs, and as such the impact of a loss of Automatic

Diagnosis is not reflected in the quantification of human reliability. OPEX available in the public domain highlights the detrimental impact that a loss of HMI can have on Control Room Operators' situation awareness, and the importance of clear 'Loss of HMI' indications and administrative controls to ensure impacts on safety and operations are minimised (see section 4.3.1.3 - OPEX).

692. In all the HRA reports sampled, my TSC found that the correct PSF check sheets had been used, and the formulae to calculate human error probability had been applied correctly. Whilst they found some examples where they believe the application of PSFs has resulted in an optimistic estimation of human error probability, they acknowledge that some of the factors that influence performance tend to overlap the PSFs, rather than apply exclusively to one or the other.

693. For example, whilst SFP_R_H2 is assigned a nominal PSF for complexity despite the multiple equipment failures and LTP actions, it considers aspects related to these factors (e.g. such as occurrence of a CCF and degraded environmental conditions) in its assignment of an extreme PSF for stress. Generally, the HEPs obtained are reasonable compared to my expectations and experience, with a HEP approaching unity derived for the most challenging scenario, HEPs close to the defined cut off value of 1.0e-05 derived for long timescale SFP failures, and the other HEPs distributed between 1.0e-02 and 1.0e-04.

694. My TSC's observations in their assessment support the academic criticisms of the SPAR-H method; that it does not support the identification and treatment of credible internal error mechanisms, nor does it provide sufficient anchors or granularity to prompt the analyst to consider a range of conditions that would be found in the range of fault scenarios. However, for GDA, my TSC considers that the RP has done a suitable job of justifying its quantification of human error. Particularly, given the limitations imposed by the chosen method and available information at GDA.

695. However, it is important to note that during the detailed design, such analytical weakness will need to be suitably addressed. I consider this shortfall can be progressed by normal business but is also bounded by AF-UKHPR1000-0154.

696. Whilst individual HBSC evaluations each include consideration of the prior sequence of events that has led to the claimed manual actions, I would expect the assessment of dependency to consider those scenario factors common to potential dependency pairs by reviewing minimum cut-sets in which they appear. The method used to identify potential pairs (i.e. set all HEPs to 0.1) constrains the number of candidates for consideration, and does not support identification of a wide range of cut-sets in which the pairs appear.

697. The 'HRA Summary Report' (Ref. 10) describes the method applied to the assessment and quantification of dependency, but it does not include the results of this work. The assessment is presented in the 'Level 1- Internal Events At Power PSA Report' (Ref. 88), which also presents the PSA screening HEPs. In total, 12 HFE Pairings have been identified, but there is considerable duplication across the pairs, including variations of the following:

- Failure to start air conditioners in the MCR, followed by
- Failure to evacuate the MCR (5 pairs)
- Failure to cross connect ASGs, followed by
- Failure to perform Feed and Bleed (3 pairs)

698. My TSC found no detailed qualitative assessment to support the selection of dependency levels, as I have discussed in section 4.3.1.4 and 4.3.1.7. Instead, the evaluation of all 12 pairs is presented in a six-page table, which provides a statement

against each potential coupling mechanism to justify whether the coupling mechanism is considered applicable or not. The arguments presented are generally sound, but as I have already noted, I consider the conclusions from the qualitative assessments to be sometimes overly optimistic (e.g. identifying zero dependency where a stronger level of dependency is more appropriate).

699. My TSC found that based on the assigned levels of dependence, the RP has correctly calculated conditional probabilities using dependency formulae contained within the THERP method.

700. As presented, the assessment of human error dependency falls short of my expectations, due to the lack of a suitable and systematic approach to the qualitative assessment. When dependency is assigned with insufficient qualitative assessment of the common scenarios in which candidate dependency pairs could occur, it is not possible to identify the context within which potential dependency mechanisms could develop. This therefore means that it is difficult to identify whether a means exists within the design to break that dependency (e.g. different cue to break 'mind-set'), or whether there is a potential shortfall in the design. It can also lead to an optimistic evaluation of the human contribution to risk within related PSA.

701. The lack of qualitative underpinning of the dependency modelling must be considered in the HRA, but one that I consider acceptable at the GDA stage. This is because many of the factors important for best estimate dependency modelling have yet to be defined (e.g. task design, EMIT schedules, staffing concepts, training and procedures) the topic of dependency will need to be revisited as part of the PSA/HRA updates during detailed design. Further, and most importantly, I consider that the risk of a cursory assessment of dependency failing to identify a design feature that is sufficiently significant to prejudice the viability of the generic UK HPR1000 design to be suitably low given the design being assessed here is an evolutionary PWR design. I am therefore content for this shortfall to be resolved as part of normal business during the development of the HRA.

4.5.3.5 Assessment of Overall Human Contribution to Risk

702. This section presents my assessment of the Human Contribution to Risk based on the analysis presented by the RP, including consideration of the degree to which the incorporation of the HRA outputs into the PSA has resulted in a realistic assessment of human error probability. It was supported by my TSC's independent assessment of the HRA.

703. The role of the human on a NPP can be a significant contribution to risk and it is important that this is understood and suitably underpinned. To understand this contribution holistically, the safety case needs to present an aggregated view of the complex data within the suite of PSA and HRA analyses. Without such an holistic view, it can be difficult for the safety case users to understand general design vulnerabilities (to human error) and whether the balance of protection (human-technology) is appropriate.

704. The 'HRA Summary Report' (Ref. 10) contains within it a section on 'Contribution to Risk' which includes comparison of risk with Radiological Protection Targets defined in the ONR SAPS (Ref. 4).

705. ONR's SAPs contain 9 numerical targets and related requirements for evaluating site risk. Ref. 10 converts these targets to Radiation Protection Targets (RPT). For GDA it was only possible to show the human risk contribution for 5-9 due to the maturity of the analysis.

706. The targets are defined as (Ref. 10):

- RPT 5 is used to evaluate the risk of fatality to a worker on-site due to exposure to radiation from on-site accidents.
- RPT 6 is used to evaluate the frequency of any single accident in the facility which could give a dose to a worker on the site that is within a specified range.
- RPT 7 is the target for the individual risk of death to a person off the site, from accidents at the site resulting in exposure to ionising radiation.
- RPT 8 is a set of targets for the total predicted frequencies of accidents on an individual facility, which could give doses in specified dose bands to a person off the site.
- RPT 9 is the target for the total risk of 100 or more fatalities, either immediate or eventual,

707. The RP undertook sensitivity analysis to understand the degree to which the generic UK HPR1000 design is sensitive to human error. It also underpins the graded and targeted approach applied by the RP to its programme of HRA.

708. The sensitivity results are shown in the tables 10 and 11 below. When the HEPs for all human actions are set to 0.01, The RP's radiation protection targets are met.

709. It is important to note the potentially misleading figures for CDF and LRF when zero credit (HEPs set to 1) is taken for all human actions including Type A human actions.

710. Critical errors in the performance of Type A human actions result in the safety function of the engineered equipment on which the Type A action is being performed not being achieved. Thus, where zero credit is applied for Type A human actions, most safety systems will fail to deliver their safety function leading to core damage. When only the HEPs of Type B and Type C human actions are set to 1 (Type B and Type C errors modelling aggregating together to drive this figure), the CDF is 9.48E-04/ry.

711. For comparison, current generations PWR power stations typically present a core damage frequency of the order of 2 x 10-3 without taking credit for HBSC and 3.9 x 10-5 with credit (Ref. 89).

Table 10: The Sensitivity Analysis Results (internal events PSA)

HEP	CDF	LRF	RPT5	RPT6	RPT7	RPT8	RPT9
1	1.3	1.21	BSL Not Met	BSL Not Met	BSL Not Met	BSL Not Met	BSL Not Met
0.1	2.63E-03	7.26E-04	BSL Not Met	BSL Not Met	BSL Not Met	BSL Not Met	BSL Not Met
.01	1.70E-06	2.09E-07	BSO Met	BSO Met	BSO Met	BSO Met	BSL Met
.001	2.92E-07	4.84E-08	BSO Met	BSO Met	BSO Met	BSO Met	BSL Met
Actual	3.85E-07	6.05E-08	BSO Met	BSO Met	BSO Met	BSO Met	BSL Met

Table 11: HEP sensitivity on Core Damage Frequency (CDF) and Large Release Frequency (LRF) by PSA

PSA	HEP	CDF	LRF
Internal Events	1	1.3	1.21
	0.1	2.63E-03	7.26E-04
	0.01	1.70E-06	2.09E-7
	0.001	2.92E-07	4.84E-08
	Actual Value	3.85E-07	6.05E-08
Internal Fire	1	4.16E-02	4.15E-02
	0.1	1.06E-03	8.25E-04
	0.01	1.86E-06	1.09E-07
	0.001	1.29E-07	1.31E-08
	Actual Value	1.16E-07	1.51E-08
Internal Flooding	1	1.04E-03	1.35E-02
	0.1	1.38E-05	7.98E-06
	0.01	1.91E-08	2.92E-09
	0.001	1.95E-09	7.08E-10
	Actual Value	1.14E-08	1.34E-09
External Hazards	1	8.96E-04	1.74E-03
	0.1	1.74E-03	4.14E-06
	0.01	7.33E-08	1.86E-07
	0.001	8.95E-09	5.34E-09
	Actual Value	5.34E-09	5.28E-09

712. As can be seen in Table 10, at the 0.01 probability, the risk targets appear to be met. It is important to note that not all the HEPs derived from detailed HRA assessment appear to have been included in the PSA so any conclusions on the tolerability of the design to human error need to be considered in this light. Nevertheless, an aggregate human reliability of 0.01 (1 in 100) should be possible to achieve with even the most basic of HFE programmes and little consideration of HF and just good engineering practices following lessoned learned from PWR design evolution.

713. The sensitivity study does provide some confidence that the generic UK HPR1000 design is not overly sensitive to human error. The CDF for 'true value' HEPs (CDF = 3.85E-07) is marginally higher than that obtained when all HEPs are set to 0.001 (CDF=2.92E-07), and an order of magnitude lower than that obtained when all HEPs are set to 0.01 (CDF=1.7E-06). Across these three scenarios, the results of comparisons with risk targets remain the same.

714. This suggests that additional conservatisms could be introduced by substituting the HEPs from the detailed assessment, without changing these findings significantly.

715. It is difficult to draw this conclusion with a high degree confidence given the complexity of PSA modelling and the conclusions of my HRA review. Whilst I take confidence from the detailed HRA performed, my TSC identified several findings that suggest that the HRA presented veers towards optimistic rather than best estimate. Where conservative HEPs have been determined, they are higher than those already included in the PSA as the 'real/actual' value. For example, a review of the response to RQ-UKHPR1000-1734 Collated HBSC Data identifies approximately 80 Type A HBSCs with a HEP of 1e-05, and a small number that are even lower despite the cut-off value stated by the methods. These are roughly two orders of magnitude lower than the Type A HEPs derived in the bounding cases my TSC examined.

716. I explored this further with ONR's PSA inspector to gain an understanding of the apparent disconnect between the two sets of HRA data (PSA derived and HF derived). It appears to be a consequence of the PSA and HF work programme being out of step with each other, and the relatively late addition to the project of an HF capability able to produce modern standards HRA work. I consider this lack of integration between HF team derived HRA and PSA team derived HRA to be acceptable at GDA as this has been suitably mitigated for GDA by sensitivity analysis. However, an integrated approach will be necessary for the site-specific stage to ensure that the analysis supports the legal requirement for a suitable and sufficient risk assessment. This is addressed by AF-UKHPR1000-0154 which requires more effective HF/PSA integration in the development of HRA during detailed design.

4.5.4 Strengths

- The RP's approach to the identification of HBSCs is sound, displaying most of the attributes which are recognised as RGP. The scope of the HRA presents a coherent and sufficient set of human reliability claims for GDA, within the constraints of design maturity and licensee input.
- A comprehensive and proportionate analysis of tasks important to safety has been undertaken. This is supported by the definition of appropriate screening criteria, which has been applied to reduce the scope of detailed HBSC analysis to a manageable level.
- Whilst I judge that the selected HRA quantification methods are perhaps overly simplistic and lacking with regards to the ability to model human-computer interaction, they are appropriate for GDA given the lack of a detailed design or defined organizational arrangements.
- The approach taken to identify potential candidates for dependency analysis is transparent. Whilst there is a degree of optimism in the application of methods

to identify potential dependencies and evaluate the level of dependence that exists, the method by which the conditional probabilities are calculated aligns with good practice.
- Where the qualitative analysis has identified assumptions that impact on the probability of human error, these are adequately documented.
- Calculated HEPs are reasonable as best estimate and reflect the qualitative analysis undertaken. Generic assessments (Type A) are appropriately conservative.
- The HRA Summary Report has been a recent enhancement to the case and serves as a good platform from which to build from in the site-specific phase.
- HBSCs are fully integrated into the Level 1 and 2 PSAs. All modes of operation are considered, along with fuel route and the most significant hazards.

4.5.5 Outcomes

- There has been a lack of suitable integration between the HF and HRA teams, leading to the inconsistent use of HF derived PSFs within the PSA. This undermines the arguments presented on the human contribution to risk. The RP recognises this and has committed to addressing this in the site-specific stage. There is a lack of suitable integration / synergy between the task analytic work conducted for HF derived HRA and other pieces of analysis, e.g. task-verification of the HFE and AoF. The RP recognises these shortfalls.
- The HBSC substantiation work is not complete and will need to be developed during detailed design.
- Claims on recovery by the Safety Engineer are not supported with appropriate qualitative analysis and introduce unjustified optimism. There is no discussion regarding how and when the related errors would be revealed to the SE, and the assessments assume that detection of the prior error is sufficient to ensure recovery, without considering what actions would be required and whether they can be completed in available time.
- Whilst most assessments have some general discussion around the impact of a loss of Automatic Diagnosis function, no corresponding error mechanisms or PSFs are identified within the assessments. This means that a loss of Automatic Diagnosis is not reflected in the quantification of human reliability.
- Two Assessment Findings are raised AF-UKHPR1000-0154 and AF-UKHPR1000-0155 to address the lack of integration between the HF programme and the PSA/HRA programme and need to identify a suitable and sufficient approach to modelling human computer interactions during the detailed design.

4.5.6 Conclusion

717. I consider that the approach to HRA followed by the RP for GDA to be suitable and sufficient. The RP has demonstrated an effective process for the capture and management of HBSCs, sufficient to provide an effective basis for planning risk informed and targeted HFE and Safety Analysis by the licensee. It is also evident that the HF interfacing disciplines have supported the capture of HBSCs within the relevant safety analysis schedules (e.g. fault studies, internal and external hazards) during GDA.

718. I also note the improvements made by the RP in the quality of its qualitative HRA over the course of the GDA, and the commitment to developing a summary HRA report, to better support the licensee's (and ONR's) understanding of the risk contribution of the operator on this NPP design.

719. However, I would consider that the general approach followed for GDA will not be fit for purpose during the detailed design due to the shortfalls identified during my assessment. These are the subject of the AFs raised by my assessment.

4.6 Demonstration that Relevant Risks Have Been Reduced to ALARP

4.6.1 Assessment

720. Under UK legislation (Ref. 90), a duty holder is required by law to demonstrate that risks have been reduced ALARP. It is important that the information provided by the RP in the safety case is suitable and sufficient to demonstrate to ONR that risks have been reduced ALARP. As part of this demonstration, the RP is required to show that the technical standards it has used result in a design in which risk has been reduced ALARP. This needs to include consideration of any updates to those technical standards since the original design and safety analysis were completed (Ref. 1).

721. My assessment of ALARP considers:

- The suitability of standards that the generic UK HPR1000 design has been designed and / or assessed against. (Section 4.4)
- Whether the generic UK HPR1000 design meets these standards (Section 4.4)
- Whether the RP has demonstrated that the human contribution to risk is tolerable. (Section 4. 5)
- Whether there is evidence that the HFI programme has resulted in reasonably practicable design improvements from the reference design to reduce the risk SFAIRP. (Sections 4.2)

722. The RP has submitted a specific document for the demonstration of ALARP for the HF topic area (Ref. 7). This document is supplemented by several other documents which together support safety case claim 3.4 ‘The safety assessment shows that the nuclear safety risks are ALARP.’ The principal supporting documents include:

- Summary Report for Human Factors Integration (Ref. 17)
- HRA Summary Report (Ref. 10)
- Supporting report on ALARP Assessment for DNB analysis (Ref. 91).
- Allocation of Function Review Report (Ref. 25)

723. Ref. 7 presents a holistic ALARP assessment and an example specific ALARP assessment. The holistic assessment summarises the generic UK HPR1000 design’s compliance with HF RGP and the HF identified and incorporated design changes, technical change notes supported by HF assessment and planned site commitments.

724. As already discussed in section 4.2 above, I am content that the HFE standards selected for the generic UK HPR1000 design meet RGP expectations sufficient for GDA. I am also content, subject to the caveats and Assessment Findings raised in sections 4.4, that the generic UK HPR1000 design meets RGP sufficiently for GDA.

725. Ref. 7 cites 8 category 2 design modifications that have been adopted:

- M63 Modification for Passive IVR Operation Time Problem.
- M64 Modification of Isolation of the Water Intake Pipeline of the RCV Charging Pump from VCT and Hydrogenation Station Manually
- M65 Modification of Injection of MHSI with Large Miniflow Line Closed Manually
- M66 Modification on Spent Fuel Delivery Process
- M75 Modification of Means of Safe Access to the Cranes in Fuel Building (BFX)
- M76 Modification of Fuel Handling Equipment in Fuel Building
- M77 Modification of Operation Envelop Control of Auxiliary Crane
- M78 Modification for Maintenance of Spent Fuel Cask Crane

726. It also states that there are 155 site commitments that will be addressed as the design is progressed during the site-specific stages. It also notes that the HF team has supported in the sentencing of 170 technical change notes which I consider evidences the role that the HF team have in support the ALARP process during GDA.

727. I am content that for GDA, this is sufficient evidence to show that the RP is working towards an ALARP position for the design. It evidences an active HFE programme, with the necessary scope and reach to effect and support change.

728. Ref. 7 includes an example (M63 – TCN GHTCN000178) to demonstrate the ALARP optioneering process. This example relates to the IVR safety case. Due to its risk significance, the human actions associated with successful passive IVR were selected for detailed HRA.

729. Passive IVR is claimed in the event of a severe accident (core outlet temperature > 650C) and is predicated on manually flooding the reactor pit to remove decay heat from the RPV. Passive IVR needs to be initiated within 20 minutes in the event of a double-ended guillotine rupture occurs on the cold leg in the main loop at full power.

730. The associated HRA found that the time required for the operator's action was 44.5 minutes due to the protective measures (electrical isolation of the 4 IVR valves) included to protect against spurious activation of the Passive IVR system. Initiation of Passive IVR could only be achieved following an operator performing local manual actions to re-energise the 4 IVR valves. The measures protecting against spurious Passive IVR essentially stopped the correct functioning of the system.

731. An ALARP review was conducted to identify design changes to deliver the Passive IVR function. The ALARP review considered 4 design change options:

- Combining electrical withdrawable units of two trains' passive valves into one of electrical switchboard.
- Combining electrical withdrawable units of two trains' passive flooding valves into one electrical switchboard and moving the switchboard to the room near main control room.
- Removing the electrical isolation.
- Replacing the administrative local lockout with remote manual permissive function operated from the MCR.

732. I assessed the RP's ALARP review and concur with its logic from the HF perspective. The RP found that the first two options offered only small time-savings, which given Passive IVR will be used in a severe accident scenario with its attendant high stress levels, I consider rejecting these options to be a suitably conservative decision. Scheme 3 was found to not be viable due to space restrictions. Scheme 4 was chosen as it offered the greatest time margin for successful passive IVR operation.

733. As part of its ALARP demonstration, the RP also carried out a first-principle assessment of the nuclear critical safety functions (Ref. 25) and whether these had been appropriately allocated between the technology and the operator. I discuss this in detail in section 4.3. I consider the approach to be modern standards and there is evidence that the process has delivered ALARP improvements.

734. What is not reported in Ref. 7 is any numerical demonstration that risk are reduced ALARP. Demonstration of risk tolerability against ONR's relevant SAP does not replace the need for good engineering and HF practices, but it is a consideration in determining ALARP. The criteria for determining whether an explicit ALARP demonstration is required in relation to the Engineering and HF SAPs, are not set out in numerical terms. Instead, if the relevant SAP is evidently well satisfied, then the

design is considered to meet the equivalent of the tolerability of risk broadly acceptable criterion on that point and therefore there is unlikely to be a need for further assessment against ALARP.

735. To address the lack of numerical insight in the ALARP case, I advised the RP to develop an HRA summary document, which I assess in detail in section 4.5. The RP's sensitivity analysis performed as part of the development of this report shows that the generic UK HPR1000 design meets ONR's numerical targets 5-9 when the HEPs for all human actions are set to 0.01.

4.6.2 Strengths

736. The RP has provided a comprehensive summary of the work that has been done to demonstrate that, from an HF perspective, risks are reduced ALARP.

4.6.3 Outcomes

737. I have not identified any shortfalls or issues from my assessment of ALARP in the HF topic area.

4.6.4 Conclusion

738. I consider the RP has provided in both its 'ALARP Demonstration Report of PCSR Chapter 15' (Ref. 7) and associated submissions (e.g. Refs. 17, 10, 21 and 95) suitable and sufficient demonstration that, as far as is reasonably practicable within the scope of GDA, that the design reduces the human contribution to risk ALARP.

4.7 Consolidated Safety Case – PCSR Chapter 15

4.7.1 Assessment

739. At the end of GDA the RP is required (Ref. 1) to re-consolidate the design reference and generic PCSR and supporting documentation to consider:

- the additional information that has been provided in response to ONR technical questions;
- and ν design (and safety case) changes that ONR has agreed can be included in the GDA scope.

740. This is captured in the Master Document Submission List (Ref. 92)

741. My assessment of the generic UK HPR1000 HF safety case for GDA has been based on:

- Safety case submissions provided by the RP.
- ROs and RQ responses during GDA.
- RP supplied Information during technical interactions.

742. To confirm the suitability and sufficiency of the safety case consolidation, I have undertaken a sample across the suite of submissions.

743. I assessed the PCSR Chapter 15 version 2 (Ref. 3). It provides a current summary of the claims, arguments and supporting evidence on which the safety case is predicated. It references the latest versions of the supporting evidential submissions. I consider it meets the expectations set by SAP SC.4 for the purpose of GDA.

744. The most risk significant RO raised in the HF area was RO-UKHPR1000-0030 Justification for Use of Automatic Diagnosis (Ref. 49). I therefore chose to sample the

RP's response to this to ensure that the information contained within the RO resolution plan was consolidated in the MSDL. The plan committed to the delivery of three additional RP submissions:

- Justification of the AD Safety Classification
- Qualification Plan of the AD System
- AD System Design Analysis Report

745. I can confirm, all three of these documents have been consolidated into the MSDL.

746. Given the effective capture and management of HBSCs is critical for the successful site-specific stage, I also chose to sample a number of HBSC related RQ responses by the RP. The sample spanned the entirety of GDA steps to ensure revision updates were reflected in the MSDL.

- RQ-UKHPR1000-0499 Class 1 Operator Claims (Ref. 93). This RQ required additional clarification on Class 1 operator claims in the Fault Schedule. I can confirm that the information within this RQ response is contained within the latest version of Fault Schedule (Ref. 21) and HRA Summary Report (Ref. 10)
- RQ-UKHPR1000-1435 Human-based safety functions and requirements relevant to the Hazards Schedules. This RQ required additional clarification on the omission of some HBSCs within the internal and external hazard schedules. The relevant output (additional HBSCs identified) of the RQ response was added to Ref. 50 HBSC listing which is consolidated into the MSDL.
- RQ-UKHPR1000-0098 The Role of the Operator in Assuring Nuclear Safety (Ref. 94). This RQ required the RP to provide a summary of the concept of operations and a summary of the risk important HBSCs from safety analysis. In response to this RQ the RP stated that it would submit a concept of operations report (Ref. 8) which is consolidated within the MSDL and has been regularly updated during GDA to revision G.

747. Further, I also assessed the MSDL HF submission list to judge whether there was sufficient scope and breadth to support the licensee in its development of a suitable and sufficient HFI programme. The MSDL appears to contain all the method documents submitted to date in their latest revised states. It also appears to contain the totality of the submitted HFE and HRA reports.

748. Based on this sample, I am content that the information from ROs and RQs has been adequately incorporated in the generic UK HPR1000 safety case.

4.7.2 Strengths

749. Following my assessment of the generic UK HPR1000 consolidated safety case I have identified the following strengths:

- I consider the MSDL is suitably representative and current of the HF submissions during GDA.
- PCSR Chapter 15 version 2 (Ref. 3) provides an adequate overview of the consolidated safety case with references out to supporting information and meets the expectations set by SAP SC.4 for the purpose of GDA.

4.7.3 Outcomes

Following my assessment of the generic UK HPR1000 consolidated safety case I have not identified any specific outcomes.

4.7.4 Conclusion

750. Based on the outcome of my assessment, I have concluded that information provided to me by the RP has been sufficiently consolidated in the MSDL and PCSR Chapter 15.

4.8 Comparison with Standards, Guidance and Relevant Good Practice

751. I have used the RGP, standards and guidance explained in sub-section 2.4.3 of this report to compare with the RP's submissions relating to HF.

752. I consider that the work conducted by the RP broadly aligns with my regulatory expectations as set out in ONR's SAPs and TAGs, and other RGP.

753. Where shortfalls have been noted during my assessment, these are explicitly cited within section 4 of this report.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

754. This report presents the findings of my HF assessment of the generic UK HPR1000 design as part of the GDA process.

755. Based on my assessment, undertaken on a sampling basis, I have concluded the following:

- The RP has successfully demonstrated that the HFI programme has been of benefit to the safety of the generic UK HPR1000 design as it has produced a number of design enhancements.
- The RP has developed an HF capability – including team growth, securing specialist support, and improving technical capability – sufficient to meet the needs of the GDA process.
- The safety functional allocation between the technology and the human has been appropriately validated during GDA using a new proprietary method developed by the RP for GDA. I consider the method to represents best practice as it considers the complex nature of allocation that new technologies support. The RP recognises the limitations of its analysis and has identified where further work will be necessary by the licensee, to consider a wider range of safety functions, such as activities relating to maintenance.
- The probabilistic HRA case shows that the design is suitably tolerant to human error against ONR's risk targets. The design has been shown to meet the BSO for ONR's numerical targets 5-8 when all PSA HEPs are set to 1 in 100.
- The RP has demonstrated effective management of human based safety claims during GDA. This is an important enabler for the licensee. HBSCs are captured in the Fault Schedule, PSA, and Internal and External Hazard Schedules.
- The RP has submitted a further action plan to demonstrate it recognises the limitations of GDA and set out what additional work will be required by the licensee. The plan closely aligns with my own assessment.
- Many of the shortfalls against regulatory expectations I have identified during my assessment can be mitigated during detailed design, affording the opportunity during the site-specific stages to address any HFE shortfalls. It is important to note that this carries an enhanced design foreclosure risk. I consider the risks of foreclosure of design options manageable but will lead to a significant HF programme of work for the licensee.
- The quality of design and safety analysis submissions will need to continue to improve during the site-specific stage. The variability does not challenge my overall judgements, but will need effort from the licensee to resolve.
- A lack of integration between HF team derived HRA and PSA team derived HRA. This has been suitably mitigated for GDA by sensitivity analysis, but I would expect the licensee to ensure that the analysis delivers best estimate HRA data, whilst taking account of the uncertainties endemic in HRA modelling. I am confident the licensee can resolve this.
- The approach to HRA, which fails to suitably take account of, and model, the impact of credible errors on factors such as task timing, dependent failures, and workload requires improvement. This was mitigated for GDA by appropriate sensitivity analysis within the HRA.
- Some HFE submissions do not always provide suitable and sufficient evidence to demonstrate compliance with HF RGP. Site-specific design work affords an opportunity for the licensee to address this shortfall.
- The expansion in scope and scale of the HFI programme to meet regulatory expectations led to a lack of clarity in RP's suite of submissions.

- A lack of task-driven HFE design, in preference to code and standard compliance.
- Not adequately capitalising on available OPEX and organisational learning, sufficient to inform the design and safety analysis.

756. Overall, based on my sample assessment of the safety case for the generic UK HPR1000 design undertaken in accordance with ONR's procedures, I am satisfied that the case presented within the PCSR and supporting documentation is adequate. On this basis, I am content that a DAC should be granted for the generic UK HPR1000 design from a HF perspective.

5.2 Recommendations

757. Based upon my assessment detailed in this report, I recommend that:

- **Recommendation 1**: From a Human Factors perspective, ONR should grant a DAC for the generic UK HPR1000 design.

- **Recommendation 2**: The 15 Assessment Findings identified in this report should be resolved by the 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. ONR. www.onr.org.uk/new-reactors/ngn03.pdf

2. *Safety Assessment Principles for Nuclear Facilities*. 2014 Edition, Revision 1. January 2020. http://www.onr.org.uk/saps/saps2014.pdf

3. *Chapter 15 Human Factors - Pre-construction Safety Report* HPR/GDA/PCSR/0015@002 29/09/2021. Issue 2. 2021. CGN

4. *Technical Assessment Guides*

   The Purpose, Scope and Content of Safety Cases. NS-TAST-GD-051. Revision 4. July 2016. ONR.

   Safety Systems. NS-TAST-GD-003 Revision 9, ONR, 2018.

   Fundamental Principles. NS-TAST-GD-004. Revision 7, ONR, 2019.

   Guidance on the Demonstration of ALARP. NS-TAST-GD-005. Revision 11, ONR, 2020.

   Examination, Inspection, Maintenance and Testing of Items Important to Safety. NS-TAST-GD-009. Revision 6, ONR, 2019.

   Computer Based Safety Systems. NS-TAST-GD-046. Revision 6, ONR, 2019.

   The Purpose, Scope and Content of Nuclear Safety Cases. NS-TAST-GD-051. Revision 7, ONR, 2019.

   Design Safety Assurance. NS-TAST-GD-057. Revision 6, ONR, 2017.

   Human Factors Integration. NS-TAST-GD-058. Revision 4, ONR, 2020.

   Human Machine Interface. NS-TAST-GD-059. Revision 5, ONR, 2019.

   Workplaces and Work Environment. NS-TAST-GD-062. Revision 4, ONR, 2020.

   Human Reliability Analysis. NS-TAST-GD-063. Revision 5, ONR, 2018.

   Allocation of Function between Human and Engineered Systems. NS-TAST-GD-064. Revision 4, ONR, 2017.

   Licensee Design Authority Capability. NS-TAST-GD-079. Revision 6, ONR, 2020.

   Guidance on Mechanics of Assessment. NS-TAST-GD-096. Revision 0. April 2020. http://www.onr.org.uk/operational/tech_asst_guides/index.htm

5. *GDA Step 4 Assessment Plan of Human Factors topic for the UK HPR1000 Reactor.* UKHPR1000-AP-19-011 Revision 0. February 2020. ONR. CM9 Ref. 2020/0028113.

6. *Further Action Plan for HF work stream.* GHX00100184DIKX03GN@B. Revision B. 2021. CGN.

7. *ALARP Demonstration Report of PCSR Chapter 15.* HX00100058KPGB03GN@D. Revision D. 2021. CGN.

8. *Concept of Operations.* GHX00100004DIKX03GN@G. Revision G. 2020. CGN.

9. *General Safety Requirements*, GHX00100017DOZJ03GN, Revision F, November 2019. CGN.

10. *HRA Summary Report.* GHX00100183DIKX03GN@A. Revision A, 2021. CGN.

11. *UK HPR1000 GDA - Step 3 Assessment Note - Human Factors.* ONR-NR-AN-19-017. 2020. ONR. CM9:2020/6343.

12. *Substantiation of HRA Inputs in PSA Model*. RO-UKHPR1000-0018. September 2019. ONR. CM9:2019/254390.

13. *Performance Analysis of UK HPR1000 Heating Ventilation and Air Conditioning Systems*. RO-UKHPR1000-0039. April 2020. ONR. CM9:2020/106859.

14. *Identification and Use of Operational Experience (OPEX) in the UK HPR1000 Generic Design and Safety Case*. RO-UKHPR1000-0044. May 2020. ONR. CM9:2020/150572.

15. *Design and Safety Case for Class 1 and 2 Human Machine Interfaces Employed in the Main Control Room and Remote Shutdown Station*. RO-UKHPR1000-0052. November 2020. ONR. CM9:2020/305756.

16. *Human Factors Capability and Integration to Deliver the GDA of UK HPR1000*. RO-UKHPR1000-0011. May 2019. ONR. CM9:2019/133072.

17. *Summary Report for HFI*. GHX06001066DIKX03GN@D. Revision D. April 2021. CGN.

18. *Operating Experience Feedback Review Summary Report*. GHX99980001DIKX02GN@E. Revision E. August 2020. CGN

19. *Development of a Suitable and Sufficient Safety Case.* RO-UKHPR1000-0004. September 2018. ONR. CM9:2018/255957.

20. *Closure of Regulatory Observation RO-UKHPR1000-0011 - Human Factors Capability and Integration to Deliver the GDA of UK HPR1000*. UK HPR1000 - REG-GNS-0125N June 2021. ONR. CM9:2021/50796.

21. *UK HPR1000 Fault Schedule*. GHX00600276DRAF02GN@E. Revision E. August 2021. CGN.

22. *Function Allocation Methodology*. GHX06001019DIKX03GN@D. Revision D. March 2020. CGN.

23. *A Methodology for Allocating Nuclear Power Plant Control actions to Human or Automatic Control*. NUREG/CR-3331. 1983. U.S. Nuclear Regulatory Commission.

24. *The role of automation and humans in nuclear power plants*. IAEA Tecdoc 668. 1992. IAEA.

25. *Allocation of Function Review Report*. GHX00100011DIKX03GN@A. Revision A. 2020. CGN.

26. *HFE Guidelines for Human Machine Interface Design*. GHX06001039DIKX03GN@E. Revision E. July 2020. CGN.

27. *HFE Guidelines for Control Room Design*. GHX06001021DIKX03GN@E. Revision E. July 2020. CGN.

28. *HFE Guidelines for Local Area Design*. GHX0600100001DIGL03GN@D. Revisions D. July 2020. CGN.

29. *Suitability Analysis of Codes and Standards in Human Factors* GHX00800011DIKX02GN@C. Revision C. December 2020. CGN.

30. *Target Audience Description for UK HPR1000*. GHX00100155DIKX03GN@A. Revision A. September 2019. CGN.

31. *UK HPR1000 - Step 4 Electrical Engineering Assessment Report*. ONR-NR-AR-21-011. 2021. ONR.

32. *Safety of Nuclear Power Plants: Design. Specific Safety Requirements*. SSR-2/1. Revision 1. 2016. IAEA.

33. *Baseline Human Factors Assessment Report.* GHX00100107DIKX03GN@A. Revision A. April 2019, CGN.

34. *HF Verification of HMI and Workspaces Related to Risk Significant HBSCs based on FCG3*. GHX06001065DIK03GN@B. Revision B. August 2020, CGN.

35. *Light and Lighting of Work Places. Indoor Work Places*, BS EN 12464-1:2011, British Standards Institution.

36. *General Layout HF Report Review*. GHX00100003DNBX03GN@F. Revision F. June 2021. CGN.

37. *HF Assessment of General Layout of Typical SCCs.* GHX06001062DIKX03GN@C. Revision C. October 2020. CGN.

38. *NI Crane Operations HF Review Report.* GHX00100111DPZS03GN@D. Revision D. April 2021, CGN.

39. *HVAC System HF Assessment*. GHX00100001DCNT03GN@A. Revision A. September 2020, CGN.

40. *Chapter 24 – DECOMMISSIONING.* HPR/GDA/PCSR/0024@002. Revision 2. September 2021. CGN.

41. *Consistency Evaluation for Design of Facilitating Decommissioning* GHX71500005DNFF03GN@E. Revision E. March 2021. CGN.

42. *Chapter 30 – COMMISSIONING.* HPR/GDA/PCSR/0030@002. Revision 2 September 2021. CGN.

43. *Human Reliability Assessment Report for Steam Generator Access and Inspection* GHX00100124DIKX03GN@B. Revision B. December 2020. CGN.

44. *Human Reliability Assessment for Safety valve Maintenance activity* GHX00100159DIKX03GN@A. Revision A. August 2020. CGN.

45. *OPEX on Decommissioning*. GHX71500008DNFF03GN@D Revision D. April 2020. CGN.

46. *MCR Workspaces Design HF Review Report*. GHX00100008DIKX03GN@F Revision F. May 2021. CGN.

47. *UK HPR1000 - Step 4 C&I Assessment Report*. ONR-NR-AR-21-005. January 2022. ONR. CM9-2021/46296.

48. *Generic Design Assessment (GDA) of the UK HPR1000 Reactor - Human Factors - FCG3 Trials and Simulations*. ONR-NR-AN-21-036. July 2021. ONR. CM9 2021/53285.

49. *Assessment of the Response to RO-UKHPR1000-0030 - Justification For The Use Of Automatic Diagnosis*. ONR-NR-AN-21-034. June 2021. ONR. CM9:2021/50738.

50. *HBSCs list.* GHX00100005DIKX03GN@C. Revision C. July 2020. CGN.

51. *ALARP Demonstration Report of PCSR Chapter 15.* GHX00100058KPGB03GN@D. Revision D. July 2021. CGN.

52. *Step 4 PSA Assessment Report*. ONR-NR-AR-21-020. January 2022. ONR. CM9:2021/49362.

53. *UK HPR1000 - Step 4 Internal Hazards Assessment Report*. ONR-NR-AR-21-012. January 2022. ONR. CM9:2021/55302.

54. *UK HPR1000 - Step 4 External Hazards Assessment Report*. ONR-NR-AR-21-006. January 2022. ONR. CM9:2021/46598.

55. *Human Reliability Assessment Report for instrumentation calibration Activity* GHX00100160DIKX03GN@A. Revision A. September 2020. CGN.

56. *Human Reliability Assessment for Fuel Handling Operations*. GHX00100011DPFJ03GN@A. Revision A. January 2019. CGN.

57. *Human Reliability Assessment for manual water injection to SG by ASG (OP_L2_FW)* GHX00100170DIKX03GN@A. Revision A. October 2020. CGN.

58. *Human Reliability Assessment Report for Isolating Impaired SG Manually (OP_ISO_SGTR).* GHX06001046DIKX03GN@B. Revision B. November 2020. CGN.

59. *Human Reliability Assessment for Bleed and Feed, ASG Tank cross Connect and Start SBO*. GHX00100007DIKX03GN@A. Revision A. March 2020. CGN.

60. *Nuclear Power Plant Operating Experiences from the IAEA/NEA Incident Reporting System 2002-2005.* NEA No. 6150. NEA.

61. https://www.laka.org/docu/ines/event/675.

62. *Nuclear Regulatory Commission (NRC) Report from October 17th, 1992 (Nuclear Regulatory Commission (NRC) Information Notice No. 93-47: Unrecognised Loss of Control Room Annunciators*, 1993, US NRC.

63. *Task Analysis Methodology*. GHX06001042DIKX03GN@C. Revision C. August 2019. CGN.

64. *Treatment of Important Human Actions Implementation Plan*. GHX06001015DIKX03GN@E. Revision E. March 2019. CGN.

65. *Human Reliability Assessment Report for Typical Valve*. GHX06001045DIKX03GN@B. Revision B. August 2019. CGN

66. *HBSC Reliability Assessment for restarting RHR pump manually (OP_RHR_S1).* GHX00100164DIKX03GN. October 2020. CGN.

67. *Methodology of human reliability analysis*. GHX00650030DOZJ02GN@B. Revision B. March 2020. CGN.

68. *RQ-UKHPR1000-1700 - Human Factors - HRA Summary Document*. April 2021. ONR CM9:2021/33742.

69. *RQ-UKHPR1000-1734 - Human Factors – Collated HBSC Data* - May 2021. ONR. CM9:2021/36983.

70. *RQ-UKHPR1000-1437 Qualitative assessment of task timings and workload*. January 2021. ONR. CM9:2021/5628.

71. *International Atomic Energy Agency, Development and Application of Level 1 Probabilistic Safety Assessment for Nuclear Power Plants, Safety Standards Series Specific Safety Guide.* SSG-3. 2010. IAEA.

72. *HBSC Reliability Assessment for restarting RHR pump manually (OP_RHR_S1)*. GHX00100164DIKX03GN@A. Revision A. October 2020. CGN.

73. *HBSC Reliability Assessment for isolating break by operator manually (OP_ISO_LOCA)*. GHX00100165DIKX03GN@A. Revision A. October 2020. CGN

74. *Human Reliability Assessment for Performing LHSI Injection (cold leg and hot leg) (OP_LHSI_HC1)* GHX06001052DIKX03GN@A. Revision A. August 2020. CGN.

75. *Human Reliability Assessment for Isolating the Source of Dilution (OP_ISO_DIL1/OP_ISO_DIL2).* GHX06001051DIKX03GN@A. Revision A. September 2020. CGN.

76. *Internal Fire Level 1 PSA.* GHX00650005DOZJ02GN@C., Revision C. July 2021. CGN.

77. *Human Reliability Assessment Report for Reactor Pressure Vessel Head Assembly Lifting*. GHX06001048DIKX03GN@B. Revision B. September 2020. CGN.

78. *Human Reliability Assessment for Maintenance work of PZR heater replacement. / Human Reliability Assessment Pilot Report for Type A HBSCs* GHX00100108DIKX03GN@A. Revision A. September 2020. CGN.

79. *Accident Sequence Evaluation Program: Human Reliability Analysis Procedure*. NUREG/CR-4772. 1987. USRNC.

80. *Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, Final Report*. NUREG/CR-1278. 1983, USNRC.

81. *The SPAR-H Human Reliability Analysis Method.* NUREG/CR-6883. 2005. USNRC.

82. *Review of Human Reliability Assessment Methods*. RR679. 2009. HSE.

83. *Human Reliability Quantification Methodology*. GHX06001056DIKX03GN@A. Revision. August 2019. CGN.

84. *Human Reliability Assessment for starting LHSI-SI mode manually* GHX00100168DIKX03GN@A. Revision A. September 2020. CGN.

85. *Human Reliability Assessment Report for water make-up at non-refuelling state in Spent Pool (SFP_N_H2/SFP_R_H2/SFP_N_REC_H2/SFP_R_REC_H2)* GHX06001053DIKX03GN@A. Revision A. September 2020. CGN.

86. *Human Reliability Assessment Report for the human actions in hazards analysis* GHX00100173DIKX03GN@B. Revision B. January 2021. CGN.

87. *RQ-UKHPR1000-1135 - Human Factors - Risk Importance of HBSC - Full Response*. October 2020. CGN. CM9:2020/305050.

88. *Internal Events Level 1 PSA (and model).* GHX00650001DOZJ02GN@C. Revision C. July 2021. CGN.

89. *Generic Design Assessment – New Civil Reactor Build Step 4 Human Factors Assessment of the Westinghouse AP1000® Reactor Assessment Report.* ONR-GDA-AR-11-012. Revision 0. November 2011. ONR. CM9:2010/581519.

90. *Health and Safety at Work etc. Act 1974*.

91. *Supporting report on ALARP Assessment for DNB analysis*. GHX00120001DRAF00GN@D. Revision D. March 2021. CGN.

92. *Master Document Submission List.* HPR-GDA-REPO-0197. Revision 000. November 2021. CGN.

93. *RQ-UKHPR1000-0499 - Human Factors - Class 1 Operator Claims - Full Response.* November 2019. CGN. CM9:2019/3540.

94. *RQ-UKHPR1000-0098 - Human Factors - The Role of the Operator in Assuring Nuclear Safety – Detailed Required to Support Step 2 Assessment – Full Response*. May 2018. CGN. CM9:2018/181553.

95. *Human Reliability Assessment Report for Fuel Handling Operations* GHX06001055DIKX03GN@A. Revision A. July 2019. CGN.

Annex 1

Relevant Safety/ Assessment Principles Considered During the Assessment

SAP/SyAP No	SAP/SyAP Title	Description
EHF.1	Integration within design, assessment and management	A systematic approach to integrating human factors within the design, assessment and management of systems and processes should be applied throughout the facility's lifecycle.
EHF.2	Allocation of safety actions	When designing systems, dependence on human action to maintain and recover a stable, safe state should be minimised. The allocation of safety actions between humans and engineered structures, systems or components should be substantiated.
EHF.3	Identification of actions impacting safety	A systematic approach should be taken to identify human actions that can impact safety for all permitted operating modes and all fault and accident conditions identified in the safety case, including severe accidents.
EHF.4	Identification of administrative controls	Administrative controls needed to keep the facility within its operating rules for normal operation or return the facility back to normal operations should be systematically identified.
EHF.5	Task analysis	Proportionate analysis should be carried out of all tasks important to safety and used to justify the effective delivery of the safety functions to which they contribute.
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.
EHF.7	User interfaces	Suitable and sufficient user interfaces should be provided at appropriate locations to provide effective monitoring and control of the facility in normal operations, faults and accident conditions.
EHF.10	Human reliability	Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety.
SC.4	The regulatory assessment of safety cases, safety case characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.
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.

SAP/SyAP No	SAP/SyAP Title	Description
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).
ERL.3	Engineered safety measures	Where reliable and rapid protective action is required, automatically initiated, engineered safety measures should be provided.
ESS.5	Plant interfaces	The interfaces between the safety system and the plant to detect a fault condition and bring about a stable, safe state should be engineered by means that have a direct, known, timely and unambiguous relationship with plant behaviour.
ESS.8	Automatic initiation	For all fast-acting faults (typically less than 30 minutes) safety systems should be initiated automatically and no human intervention should then be necessary to deliver the safety function(s).
ESS.9	Time for human intervention	Where human intervention is needed to support a safety system following the start of a requirement for protective action, then the timescales over which the safety system will need to operate unaided, before intervention, should be demonstrated to be sufficient.
ESS.13	Confirmation to operating personnel	There should be direct means of confirming to operating personnel: (a) that a demand for safety system action has arisen; (b) that the safety systems have operated (actuated) fully and correctly; and (c) whether any limiting condition (operating rule) has been exceeded which takes the safety system beyond its substantiated capability (see Principle ESS.10).
ESR.1	Provision in control rooms and other locations	Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations.
ESR.3	Provision of controls	Adequate and reliable controls should be provided to maintain all safety-related plant parameters within their specified ranges (operating rules).
ESR.7	Communications systems	Adequate communications systems should be provided to enable information and instructions to be transmitted between locations on and, where necessary, off the site. The systems should provide robust means of communication during normal operations, fault conditions and severe accidents.
FA.1	Design basis analysis, PSA and severe accident analysis	Fault analysis should be carried out comprising suitable and sufficient design basis analysis, PSA and severe accident analysis to demonstrate that risks are ALARP.

SAP/SyAP No	SAP/SyAP Title	Description
FA.2	Identification of initiating faults	Fault analysis should identify all initiating faults having the potential to lead to any person receiving a significant dose of radiation, or to a significant quantity of radioactive material escaping from its designated place of residence or confinement.
FA.5	Initiating faults	The safety case should list all initiating faults that are included within the design basis analysis of the facility.
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. Where safety functions are delivered or supported by human action, these human actions should be identified and classified on the basis of those functions and their significance to safety (see Principle EHF. 3). The methods used for determining the classification should be analogous to those used for classifying structures, systems and components outlined in the following paragraphs.
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.

Annex 2

Human Factors Design Improvements Adopted Into GDA

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-5	M14	GHTCN000094	Modification for the access bility of ASG System local valves in BSX	In order to ensure the operators can evacuate from staircase to outside, BSC2024ZRM doesn't have fire sources any more. Therefore, two compartments will be added, cables and cabinets in BSC2024ZRM will be removed into additional compartments and BSC2024ZRM won't have any fire sources. The fire area of BSC2024ZRM can be modified to SFA	Affected System: None Affected structure: BSC Affected component: pipes, ducts	3D Model has been modified but GDA stage does not draw from 3D model, so it is not included in D.R.	NA
HF-GDA-32 HF-GDA-33	M20 Optioneering sheet GH-OP-NPD-FJ-002 Technical Specification for Auxiliary Crane（GHX45600008DPFJ44DS, Rev. D）GHTCN000099	GHTCN000099	Design Modification of Auxiliary Crane (lifting mechanism & speed matching)	The container may collide with the ground of the new fuel receipt room if the container is excessively lowered. And the auxiliary crane operator should match the speed of horizontal movement and vertical movement manually, which places great dependence on the skill of crane operator. Adding real-time monitor and interlock in the design of auxiliary crane control system. While the monitor detects over-speed or excessive lowering, the brake can stop the lowering operation quickly. Adding an interlock in the auxiliary crane control system which can match the speed of horizontal movement and vertical movement while carrying out the rotating operation.	Affected system: PMC Affected structure: BFX Affected component: auxiliary crane	Yes, D.R2.1	GHX45600008DPFJ44DS, Rev. E, Technical Specification for Auxiliary Crane

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-38	M19 Optioneering sheet GH-OP-NPD-FJ-001 GHTCN000098	GHTCN000098	Modification of Interlocking of Refuelling Machine	The refuelling machine may collide with the auxiliary refuelling platform in case of human error. The refuelling machine will add an interlock in the control system with the auxiliary refuelling platform. Only when the auxiliary refuelling platform is located at the end of reactor pool, can the refuelling machine move towards the reactor core.	Affected system: PMC Affected structure: BRX Affected component: refuelling machine	Yes, D.R2.1	GHX45600005DPFJ44DS, Rev. C, Technical Specification for Refuelling Machine
HF-GDA-93; HF-GDA-131	M63	GHTCN000178	Modification for Passive IVR Operation Time Problem	In-Vessel Retention (IVR) strategy requires that IVR injection should be implemented during 30 minutes once the core outlet temperature exceeds 650℃. But according to timeline analysis of human factor, the operation time is beyond time window requirement. So it is necessary to optimize the IVR design to reduce the effect of core melt accident. The electrical isolation function for passive IVR valve is replaced by remote manual permissive function.	Affected System: IVR Affected structure: None Affected component: None	Yes, D.R2.2	GHX06002012DIYK03GN, Rev.B, Severe Accident Control and Instrumentation System (KDA) [SA I&C] System Requirements Specification GHX00100002DNHX45 CGN,Rev.C,Optioneering on the EHR [CHRS] Related to the Inadvertent Reactor Pit Flooding

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-125	M64	GHTCN000174	Modification of Isolation of the Water Intake Pipeline of the RCV Charging Pump from VCT and Hydrogenation Station Manually	The function (Isolation of the water intake pipeline of the RCV charging pump from Volume Control Tank (VCT) and hydrogenation station-RCV-SF-04-3M) is FC2 which is not consistent with the rule "Manual functions to reach controlled state should be FC1".	Affected System:RCV Affected structure: None Affected component: None	Yes, D.R2.2	GHX00600276DRAF02GN，Rev.E，UK HPR1000 Fault Schedule

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-126	M65	GHTCN000171	Modification of Injection of MHSI with Large Miniflow Line Closed Manually	The function Injection of Medium Head Safety Injection (MHSI) with large miniflow line closed manually is FC2 in Steam Generator Tube Rupture (SGTR) (one tube) which is not consistent with the rule "Manual functions to reach controlled state should be FC1". In order to meet the radioactive release requirements of controlled state in SGTR (one tube) and the category requirements in Function Allocation Methodology simultaneously. "Injection of MHSI with large miniflow line closed manually" classified as Category 1, and the "Injection of MHSI with large miniflow line closed manually" signal could directly initiate the MCD function automatically.	Affected System：RIS Affected structure: None Affected component: None	Yes, D.R2.2	GHX00600276DRAF02GN，Rev.E，UK HPR1000 Fault Schedule

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-137	M15	GHTCN000087	Modification regarding one special mechanical interlocking between circuit break and lift truck	One special mechanical interlocking between circuit break and lift truck will be added for the UK version of the Hua-long Pressurized Reactor (UK HPR1000) with purpose that circuit breaker can be pushed out of the cabinet only with right location on lift truck. The connection box of mobile diesel generator is arranged in NI 0m of train A, which room is BSA2025ZRM. The connection box is connected to the LAP battery charger by the cable tray. The special mechanical interlocking between circuit break and lift truck will be added in the next update vision of the MV switchboard technical specification in mid of Nov 2019.	Affected System: None Affected structure: None. Affected component: MV AC Switchgear	Yes, D.R2.1	GHX52210001DEDQ44DS, Rev.D, Technical Specification of the NI MV AC Switchboard

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-138	M16	GHTCN000085	Modification regarding vis ble window of the MV switchboard	1. With propose to check the operating position of earthing switch, the visible window is proposed to be added at UK HPR1000. 2. The visible window requirement will be added in the next update vision of the MV switchboard technical specification in mid of Nov 2019.	Affected System：None Affected structure: None. Affected component: MV AC Switchgear	Yes, D.R2.1	GHX52210001DEDQ44DS,Rev.D,Technical Specification of the NI MV AC Switchboard
HF-GDA-139	M17	GHTCN000096	Modification of the direction of door opening in BWX	Necessary measures for the escape and rescue of trapped persons should be considered during HF design. In one room, if the escape routes door opens opposite the direction of escape, the person couldn't escape effectively. During HF review, it is found that the door of BWX2510ZRM opens opposite the direction of escape route. The arrangement will be modified to meet the requirement of escape.	Affected System：None Affected structure: BWX. Affected component: None	Yes, D.R2.1	GH9WX000004DNBZ43DD, Rev.D, Radioactive Waste Treatment Building General Arrangement Drawing Plan View +5.50m

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-140	M18	GHTCN000097	Modification of reducing the noise effect in –BNX3675ZRM	During HF review, It is found that operators have to go through -BNX3676ZRM (air fans room) to -BNX3675ZRM (switchgears room). The passage way is long and personnel may be affected by noise from air fans room. In order to meet the HF requirement, the access will be modified. The access to -BNX3675ZRM will be set separately from that to -BNX3676ZRM and be connected to –BNX3675ZRM directly (from the corridor).	Affected System：None Affected structure: BNX Affected component: Pipes	Yes, D.R2.1	GH1NX000008DNBZ43DD, Rev.D, Nuclear Auxiliary Building General Arrangement Drawing Plan View +16.05m
HF-GDA-143	M14	GHTCN000094	Modification for the access bility of ASG System local valves in BSX	Valve layout should meet the accessibility requirement during operation and maintenance. During HF review, some valves (1ASG6101/6115/6102/6125/6103VD/ASG6201/6202/6103VD-) are reviewed and it is found that the ASG6102VD- is inaccess ble. The arrangement will be modified to meet the accessibility requirement	Affected System：ASG Affected structure: None. Affected component: pipes and valves	3D Model has been modified.but GDA stage does not draw from 3D model, so it is not inluded in D.R.	NA

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
HF-GDA-275	M66	GHTCN000179	Modification on Spent Fuel Delivery Process	The present maximum lifting height of spent fuel transfer cask is much higher than the qualified drop test height when it is above the fuel hoisting pit. The cask is not fully sealed when it is being transferred between the loading pit and cleaning pit. Integrity of spent fuel transfer cask cannot be completely guaranteed if the cask drops on the lifting route. The dropped load analysis results show that the release of radioactive substances and the dose exposure to workers will exceed the acceptable limit value in case of spent fuel transfer cask drop. So, modification should be implemented for the present spent fuel delivery process to reduce the relevant risk to a level that is ALARP. The solution is to lower the lifting height of the cask and place impact limiters below the lifting route.	Affected System：PMC Affected structure: None Affected component: Spent fuel transfer cask	Yes, D.R2.2	GHXFX000001DNBZ43DD, Rev.F,Fuel building General arrangement drawing Plan View -9.60m; GHXFX000002DNBZ43DD, Rev.G, Fuel building General arrangement drawing Plan View -4.90m : GHXFX000003DNBZ43DD, Rev.G, Fuel building General arrangement drawing Plan View ±0.00m: GHXFX000004DNBZ43DD, Rev.F, Fuel building General arrangement drawing Plan View +4.50m: GHXFX000005DNBZ43DD, Rev.G, Fuel building General arrangement drawing Plan View +9.10m: GHXFX000006DNBZ43DD, Rev.H, Fuel building General arrangement drawing Plan View +13.70m;

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
	M75	GHTCN000183	Modification of Means of Safe Access to the Cranes in Fuel Building (BFX)	The spent fuel pool crane, auxiliary crane and spent fuel cask crane in BFX need to be accessed during the annual maintenance by walking along the crane brackets. And risk of falling from height is identified. Personal Protective Equipment (PPE) is provided to prevent the personnel falling from the edge of the crane brackets when they are walking along the crane brackets. According to Approved Code of Practice (ACoP) L113, where access to or egress from any part of the lifting equipment is required you should provide a safe means of doing so. It is RGP in the UK to provide a walkway along the full length of one the rails of a gantry crane which would allow safe access to the crane in any position. Meanwhile, according to the Construction (Design and Management) (CDM) regulations and the Working at Height Regulations, PPE is low on the hierarchy of desired solutions.	Affected System：None Affected structure: BFX Affected component: None	Yes, D.R2.2	GHXFX000007DNBZ43DD, Rev.H, Fuel building General arrangement drawing Plan View +18.30m: GHXFX000008DNBZ43DD, Rev.G, Fuel building General arrangement drawing Plan View +22.50m; GHXFX000009DNBZ43DD, Rev.H, Fuel building General arrangement drawing Plan View +26.00m; GHXFX000010DNBZ43DD, Rev.G, Fuel building General arrangement drawing Plan View Roof; GHXFX000011DNBZ43DD, Rev.F, Fuel building General arrangement drawing Section A-A; GHXFX000012DNBZ43DD, Rev.G, Fuel building General arrangement drawing Section B-B;

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
	M76	GHTCN000184B	Modification of Fuel Handling Equipment in Fuel Building	Several modifications for the fuel handling equipment in fuel building to prevent falling from height, over-raising and crane collision.	Affected System：PMC,DMK Affected structure: Fuel Handling Hall Affected component: spent fuel pool crane, auxiliary crane, spent fuel cask crane new fuel elevator	Yes, D.R2.2	GHXFX000013DNBZ43DD, Rev.F, Fuel building General arrangement drawing Section C-C. Note: the change of the contour size outside the buildings shows that the rooms has become larger, but the size inside the room is not obvious because it is not marked in the drawing.
	M77	GHTCN000185	Modification of Operation Envelop Control of Auxiliary Crane	Providing mechanical limitation of the long and cross-travel of the spent fuel pool crane and auxiliary crane to limit their movements within the undesirable areas of the Fuel Building. The spent fuel pool crane would be limited to operation only within the confines of the spent fuel pool, transfer compartment and loading pit; The auxiliary crane would be prevented from operating over the spent fuel pool and transfer compartment during fuel handling operations. Reallocate the lifting requirement of auxiliary crane to spent fuel cask crane.	Affected System：PMC,DMK Affected structure: Fuel Handling Hall Affected component: Spent fuel cask crane	Yes, D.R2.2	

HF. No.	Modification No.	TCN Coding	Title of design change	Brief Description of the design change	Affected System, Structure or Component	Included in the DR or it is planned to be included	TCN Reference
	M78	GHTCN000186	Modification for Maintenance of Spent Fuel Cask Crane	Provide new crane for the maintenance of spent fuel cask crane, especially for the heavy components, like drum, motor.	Affected System：DMK Affected structure: Fuel Handling Hall Affected component: Spent fuel cask crane	Yes, D.R2.2	
HF-GDA-286	M13 GHTCN000100	GHTCN000100	Modification of Main Control Room air conditioning system	Indoor conditions of the Main Control Room have been changed from 18℃-24℃ of temperature and 40%-60% of relative humidity to 20℃-24℃ of temperature in winter and 23℃-26℃ of temperature in summer and 30%-70% of relative humidity. So suitable modification should be done in order to meet above requirements. Capacity of the electrical heaters and cooling coil of the existing DCL system could meet new requirements of the indoor conditions, but some information on changing of the input of the temperature and relative humidity will be modified in System Design Manual (SDM).	Affected System：DCL Affected structure: None. Affected component: None	Yes, D.R2.1	GHX17DCL004DCNT45GN, Rev. D, DCL-Main Control Room Air Conditioning System Manual Chapter 4 System and Component Design

Annex 3

Assessment Findings

Number	Assessment Finding	Report Section
AF-UKHPR1000-084	The licensee shall develop a resourced Human Factors Integration Plan to deliver the Human Factors related elements of the detailed design and safety case. This should include, but not be limited to: • Justifying the Human Factors activities at the team and deliverable level. • Developing a detailed resource loaded programme showing the dependencies between activities and deliverables, including non-Human Factors activities. • Justifying the processes that ensures that the programme remains updated, integrated, informs work activities and underpins the development of the site-specific safety case and detailed design. • Demonstrating the graded approach for the integration of Human Factors Engineering across the entirety of the engineering, operational, and organisational design. The approach should recognise the need to integrate work from a wide range of stakeholders	4.2.2
AF-UKHPR1000-0085	The licensee shall develop the Human Factors operational experience review undertaken during GDA to support the site-specific safety case and underpin the substantiation that the detailed design reduces risk to as low as reasonably practicable. This should resolve the shortfalls identified during GDA, including, but not limited to: • Reviewing feedback from wider sources to ensure learning opportunities are included. • Developing a process to capture learning from experience. • Capturing learning from the reference plant as it moves through design, build, commissioning and operations. • Capturing learning from relevant simulators on human performance data.	4.2.3

Number	Assessment Finding	Report Section
AF-UKHPR1000-0086	The licensee shall demonstrate that the Human Factors shortfalls and Human Engineering Deficiencies identified during GDA are resolved. This should include sentencing, documenting and ensuring that the Human Factors requirements are implemented in the site-specific safety case.	4.2.4.1
AF-UKHPR1000-0144	The licensee shall, as part of detailed design, demonstrate that a complete set of Human Factors related assumptions underpinning the design and safety analysis is identified. This should include reviewing the early documentation produced during GDA.	4.2.4.2
AF-UKHPR1000-0145	The licensee shall, as part of detailed design, demonstrate that the allocation of function analyses addresses all necessary safety significant functions. This should include, but not be limited to: • Ensuring the work to address this Assessment Finding is integrated to avoid design foreclosure. • Ensuring the output links to, and informs, the human reliability analysis and substantiation of human based safety claims. • Demonstrating that those functions identified as too complex for automation, can be delivered by the human to the required level of reliability. Where this is not the case, further analysis should be undertaken to establish that risks have been reduced to as low as reasonably practicable. • Ensuring that diverse functions, emergent functions, severe accident, and non-reactor safety functions, are addressed. • Ensuring that the allocation of function decision making, up to and including design changes, is appropriately documented.	4.3.1
AF-UKHPR1000-0146	The licensee shall demonstrate that the Human Factors Engineering design guidance to support the detailed design resolves the shortfalls identified during GDA.	4.4.1.3

Number	Assessment Finding	Report Section
AF-UKHPR1000-0147	The licensee shall, as part of detailed design, undertake proportionate task verification and validation activities for all risk important human based safety claims including, but not limited to: • Examination, Maintenance, Inspection, and Testing • Normal Operations • Fault Responses • Interactions with risk important structures, systems, components and equipment.	4.4.2.2
AF-UKHPR1000-0148	The licensee shall, as part of detailed design, justify that the steam generator access aperture is consistent with UK anthropometric design requirements.	4.4.2.4
AF-UKHPR1000-0149	The licensee shall substantiate the human factors aspects of the supervisory human machine interface provided in the primary control locations. The human machine interfaces design for supervision should recognise the role differences between operation and supervision.	4.4.2.5
AF-UKHPR1000-0150	The licensee shall, in developing its human machine interfaces, implement guidance and a testing methodology to ensure that the deployment of hybrid, soft, and hard-wired interfaces support effective management of safety and reduces human error during normal and fault states to as low as reasonably practicable.	4.4.2.5
AF-UKHPR1000-0151	The licensee shall, as part of detailed design, demonstrate that the testing required for the automatic diagnosis system will provide evidence to demonstrate that human errors resulting from revealed and unrevealed failures are reduced to as low as reasonably practicable.	4.4.2.5
AF-UKHPR1000-0152	The licensee shall, as part of detailed design, substantiate that the Safety Engineer role is adequately supported by the remote shutdown station human machine interface. This should justify the associated claims made in the generic safety case or demonstrate that this role is not needed for the tasks performed at this location.	4.4.2.5

Number	Assessment Finding	Report Section
AF-UKHPR1000-0153	The licensee shall, as part of detailed design, conduct a graded verification and validation of the human factors aspects of the human machine interfaces, up to and including formal integrated system validation trials where appropriate to do so, to demonstrate their safety and operability. The verification and validation approach should resolve the shortfalls identified during GDA including, but not limited to: • All human machine interfaces important for safety, including emergency control centres, and other risk important control locations. • Partial and complete failures (revealed and unrevealed) of the human machine interfaces and their effects on factors such as task duration / time window, situational awareness, error detection and recovery, and cognitive workload. • Migration of command and control between primary and back-up control locations. • Suitable fidelity in the scenarios, including taking account of parallel or competing activities.	4.4.2.5
AF-UKHPR1000-0154	The licensee shall, as part of detailed design, ensure that an integrated and holistic approach is adopted to develop the human reliability analysis. This should ensure that: • The qualitative Human Factors analysis informs the quantification of the human errors in the Probabilistic Safety Analysis (PSA). • The PSA considers the outputs from the HF engineering programme, where appropriate.	4.5.3.1
AF-UKHPR1000-0155	The licensee shall, as part of detailed design and substantiation of the human machine interfaces, implement a validated human reliability analysis approach for screen-based interfaces. This should be underpinned by relevant research on human machine interfaces.	4.5.3.3