Office for Nuclear Regulation

New Reactor Division – Generic Design Assessment

Step 2 Assessment of Human Factors for the UK HPR1000 Reactor

Assessment Report ONR-GDA-UKHPR1000-AR-18-007
Revision 0
October 2018

Published 10/18

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 results of my Human Factors assessment of the UK HPR1000 undertaken as part of Step 2 of the Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA).

The GDA process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments increasing in detail as the project progresses. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain (GB), of the design fundamentals, including ONR's review of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls that could prevent ONR from permitting the construction of a power station based on the design.

During GDA Step 2 my work has focused on the assessment of the Human Factors (HF) aspects within the UK HPR1000 Preliminary Safety Report (PSR), and a number of supporting references and supplementary documents submitted by the RP, focusing on design concepts and claims.

The standards I have used to judge the adequacy of the RP's submissions in the area of Human Factors have been primarily ONR's Safety Assessment Principles (SAPs), in particular SAPs EHF.1 to .3, EHF.5 to .7 and EHF.10, ECS.2 and SC.4 and ONR's Technical Assessment Guides NS-TAST-GD-005 (Rev 5). Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable), NS-TAST-GD-058 (Rev 3) Human Factors Integration, NS-TAST-GD-060 (Rev 3) Procedure Design and Administrative Controls, NS-TAST-GD-063 (Rev 3) Human Reliability Analysis, NS-TAST-GD-064 (Rev 3) Allocation of Function between Human and Engineered Systems, NS-TAST-GD-030 (Rev 5) Probabilistic Safety Analysis, NS-TAST-GD-003 (Rev 8) Safety Systems and NS-TAST-GD-051 (Rev 4) Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.

My GDA Step 2 assessment work has involved regular engagement with the RP in the form of technical exchange workshops and progress meetings, including meetings with the plant designers.

The UK HPR1000 PSR is primarily based on the Reference Design, Fangchenggang Unit 3 (FCG3), which is currently under construction in China. Key aspects of the UK HPR1000 preliminary safety case related to Human Factors, as presented in the PSR, its supporting references and the supplementary documents submitted by the RP, can be summarised as follows:

- A description of the organisation and arrangements that will deliver adequate Human Factors Integration (HFI) into the UK HPR1000.
- A description of the codes, standards, and methods that will be used to ensure that HFI is effectively delivered and that all relevant areas of the design meet relevant good practice, where reasonably practicable.
- A description of the process by which operator claims important for nuclear safety will be systematically identified and substantiated to ensure that the design is optimised and risks are reduced ALARP.
- A description of the design process, which will ensure that the UK HPR1000 is a balanced design in terms of allocation of protection.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to Human Factors, I have identified the following areas of strength:

- Despite differences between the ONR's regulatory framework and that of the Chinese Regulator, the RP has made significant strides during Step 2 in understanding ONR's

regulatory expectations. It has established a robust model of HFI, which should enable it to successfully deliver the GDA. The HFI process is adequately underpinned by a suite of HF process claims, which I consider to be credible. It has put in place measures to ensure that its organisational model will not be a barrier to widespread integration of HF across disciplines.

- The RP has quickly established an appropriate supply chain to gain the necessary GB nuclear industry knowledge, along with developing a credible resource model, which will be needed to deliver the necessary HF analysis to support the GDA. It has embarked upon a programme of training for all HF and interfacing disciplines to facilitate the necessary understanding of regulatory expectations.
- The methods, codes and standards proposed generally meet Relevant Good Practice (RGP) and establish a baseline for achieving a design where risks are As Low As Reasonably Practicable (ALARP).
- The FCG3 baseline design is currently in build and is an evolution of the CPR1000, CPR1000+, and ACPR1000 designs. The FCG3 baseline design has been designed, taking into account international and domestic evolutionary operational experience; key to which are the lessons learned from the Fukushima accident, which placed significant operational demands on the operator. Those pertinent to my HF assessment include improvements to the main control room habitability and the introduction of in-vessel retention capability to extend the operator grace times for emergency equipment preparation. The design also benefits from a development simulator that has been employed for user testing.

During my GDA Step 2 assessment of the UK HPR1000 aspects of the safety case related to Human Factors, I have identified the following areas that require follow-up:

- The role the operator plays in ensuring nuclear safety has not been adequately defined during Step 2. The RP will need to provide a more cogent and coherent description of this role for Step 3.
- The Human Based Safety Claims (HBSC) supplied at the end of Step 2 is lacking detail and context. This will need developing throughout GDA.
- It is unclear what the baseline HF case is for FCG3. This will need to be developed during Step 3 as it informs the forward work programme.
- The RP has indicated that the focus of HF work on FCG3 was mainly control rooms. The expansion of HFI into other risk important areas of the plant will need to be monitored by ONR to ensure a proportionate and consistent approach.
- The approach to Human Reliability Analysis (HRA), as described, broadly aligns with RGP. However, further discussion with the RP is needed to ensure that screening and modelling during Step 3 meet expectations. This intervention will be jointly carried out by ONR's HF and Probabilistic Safety Analysis (PSA) inspectors.
- The RP's approach to Allocation of Function (AoF) is a sensible starting point but will require further modification to accommodate the subtleties of AoF for highly complex sociotechnical systems.
- Whilst the RP has made good progress with improving capability, it remains to be seen how effective this will be in delivering the GDA. The organisational capability of the RP will require monitoring to ensure it is delivering to schedule and quality.
- A targeted intervention on the application of the HF design guidance across the UK HPR1000 design to ensure that claims of HFI are valid. This intervention will be jointly carried out by a range of discipline appropriate ONR inspectors ranging from Mechanical Engineering to Management for Safety and Quality Assurance (MSQA).

During my GDA Step 2 assessment, I have not identified any fundamental safety shortfalls in the area of Human Factors that might prevent the issue of a Design Acceptance Confirmation (DAC) for the UK HPR1000 design.

LIST OF ABBREVIATIONS

ASEP	Accident Sequence Evaluation Program
AoF	Allocation of Function
ALARP	As Low As Reasonably Practicable
BSO	Basic Safety Objective
BMS	Business Management System
CGN	China General Nuclear Power Corporation
CoO	Concept of Operations
C&I	Control and Instrumentation
DAC	Design Acceptance Confirmation
DBA	Design Basis Analysis
EDF	Électricité de France
EDF-NG	EDF-Nuclear Generation
EMIT	Examination, Maintenance, Inspection and Testing
EA	Environment Agency
FCG3	Fangchenggang Unit 3
FV	Fussel Vesely
GDA	Generic Design Assessment
GNI	General Nuclear International
GB	Great Britain
GNS	General Nuclear System Ltd
HBSC	Human Based Safety Claims
HF	Human Factors
HFI	Human Factors Integration
HFIP	Human Factors Integration Plan
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HIS	Human Systems Interfaces
IC	Intelligent Customer
IAEA	International Atomic Energy Authority
MCR	Main Control Room
MSQA	Management for Safety and Quality Assurance
NPP	Nuclear Power Plants
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulation Commission Regulation
ONR	Office for Nuclear Regulation
OPEX	Operating Experience Review
PCSR	Pre-Construction Safety Report

PSR	Preliminary Safety Report
PWR	Pressurised Water Reactor
PSA	Probabilistic Safety Analysis
RI	Regulatory Issues
RO	Regulatory Observations
RQ	Regulatory Queries
RGP	Relevant Good Practice
RP	Requesting Party
RAW	Risk Achievement Worth
SAP	Safety Assessment Principles
SA	Severe Accident
SAA	Severe Accident Analysis
SPAR-H	Standardized Plant Analysis Risk Human Reliability Analysis
SQEP	Suitably Qualified and Experienced Person
SSC	Systems, Structures and Component
TAD	Target Audience Description
TAG	Technical Assessment Guide
TSC	Technical Support Contractors
THERP	Technique for Human Error Rate Prediction
US	United States
WENRA	Western Regulators Nuclear Association

TABLE OF CONTENTS

Tables

1 INTRODUCTION

1. The Office for Nuclear Regulation's (ONR) Generic Design Assessment (GDA) process calls for a step-wise assessment of the Requesting Party's (RP) safety submission with the assessments increasing in detail as the project progresses. General Nuclear System Ltd (GNS) has been established to act on behalf of the three joint requesting parties (China General Nuclear Power Corporation (CGN), Électricité de France (EDF) and General Nuclear International (GNI)) to implement the GDA of the UK HPR1000 reactor. For practical purposes, GNS is referred to as the 'UK HPR1000 GDA Requesting Party'.

2. During Step 1 of GDA, which is the preparatory part of the design assessment process, the RP established its project management and technical teams, and made arrangements for the GDA of the UK HPR1000 reactor. Also during Step 1, the RP prepared submissions to be assessed by ONR and the Environment Agency (EA) during Step 2.

3. Step 2 commenced in November 2017. Step 2 of GDA is an overview of the acceptability, in accordance with the regulatory regime of Great Britain (GB), of the design fundamentals, including ONR's assessment of key nuclear safety and nuclear security claims (or assertions). The aim is to identify any fundamental safety or security shortfalls that could prevent ONR permitting the construction of a power station based on the design.

4. My assessment has followed my GDA Step 2 Assessment Plan for Human Factors (HF) (Ref. 1) prepared in October 2017 and shared with GNS to maximise openness and transparency.

5. This report presents the results of my HF assessment of the UK HPR1000 as presented in the UK HPR1000 Preliminary Safety Report (PSR) (Ref. 2) and its supporting documentation.

2 ASSESSMENT STRATEGY

6. This section presents my strategy for the GDA Step 2 assessment of the HF aspects of the UK HPR1000 (Ref. 1). It also includes the scope of the assessment and the standards and criteria I have applied.

2.1 Scope of the Step 2 Human Factors Assessment

7. The objective of my GDA Step 2 assessment was to assess relevant design concepts and claims made by the RP related to HF. In particular, my assessment has focussed on the following (Ref. 1):

- Review of GNS's safety submission/s to confirm whether the claims related to HF that underpin the safety of the UK HPR1000 are complete and reasonable in the light of our current understanding of reactor technology and human physiology and psychology.
- Assessment of safety claims related to HF (noting that in depth examination of the detailed arguments and evidence that support the claims will be undertaken in my assessment during Steps 3 and 4 of GDA).
- Increased familiarisation with the UK HPR1000 design to provide a basis for planning subsequent, more detailed, assessment during Steps 3 and 4 of GDA.
- Undertaking of preparatory work for my Step 3 assessment in order to make a judgement on the readiness to proceed to Step 3.
- Raising, as / if appropriate, Regulatory Queries (RQ), Regulatory Observations (RO) and / or Regulatory Issues (RI).
- Engaging with the RP via progress teleconferences and face-to-face technical meetings and workshops.
- Preparation of an Assessment Report to summarise the work done and my conclusions and recommendations.

8. During GDA Step 2 I have also evaluated whether the safety claims related to HF are supported by a body of technical documentation sufficient to allow me to proceed with GDA work beyond Step 2.

9. Finally, during Step 2 I have undertaken the following preparatory work for my Step 3 assessment:

- Preliminary supporting work to inform my assessment plan for Step 3.
- Identification of suitably qualified and experienced HF engineers that can provide technical support to the Step 3 assessment.
- Continued engagements with the RP to agree a credible schedule of submissions in order to provide suitable and sufficient material for a meaningful Step 3 assessment.

2.2 Standards and Criteria

10. For ONR, the primary goal of the GDA Step 2 assessment is to reach an independent and informed judgment on the adequacy of a preliminary nuclear safety and security case for the reactor technology being assessed. Assessment was undertaken in accordance with the requirements of the ONR How2 Business Management System (BMS) guide NS-PER-GD-014 (Ref. 3).

11. In addition, the Safety Assessment Principles (SAPs) (Ref. 4) constitute the regulatory principles against which duty holders' and RP safety cases are judged. Consequently, the SAPs are the basis for ONR's nuclear safety assessment and have therefore been used for the GDA Step 2 assessment of the UK HPR1000. The SAPs 2014 Edition are aligned with the International Atomic Energy Authority (IAEA) standards and guidance.

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

13. The relevant SAPs, IAEA standards and WENRA reference levels are embodied and expanded on in the Technical Assessment Guides (TAG) on HF (Ref. 5). These guides provide the principal means for assessing the HF in practice.

2.2.1 Safety Assessment Principles

14. The key SAPs (Ref. 4) applied within my assessment are SAPs EHF.1 to .3, EHF.5 to .7 and EHF.10, ECS.2 and SC.4 (see also Table 1 for further details).

2.2.2 Technical Assessment Guides

15. The following TAGs have been used as part of this assessment (Ref. 5):

- NS-TAST-GD-005 (Rev 5). Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)
- NS-TAST-GD-058 (Rev 3) Human Factors Integration.
- NS-TAST-GD-060 (Rev 3) Procedure Design and Administrative Controls.
- NS-TAST-GD-063 (Rev 3) Human Reliability Analysis.
- NS-TAST-GD-064 (Rev 3) Allocation of Function between Human and Engineered Systems.
- NS-TAST-GD-030 (Rev 5) Probabilistic Safety Analysis.
- NS-TAST-GD-003 (Rev 8) Safety Systems.
- NS-TAST-GD-051 (Rev 4) Guidance on the Purpose, Scope and Content of Nuclear Safety Cases.

2.2.3 National and International Standards and Guidance

16. The following national and international standards and guidance have been considered as part of this assessment:

17. IAEA standards (Ref. 6)

- International Atomic Energy Agency, Specific Safety Requirements: Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series No. SSR-2/1 Rev 1, IAEA, Vienna 2016.
- International Atomic Energy Agency, Specific Safety Guide: Deterministic Safety Analysis for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-2, IAEA, Vienna 2010.
- International Atomic Energy Agency, Specific Safety Guide: Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna 2016
- International Atomic Energy Agency, Specific Safety Guide: Design of Instrumentation and Control Systems for Nuclear Power Plants, IAEA Safety Standards Series No. SSG-39, IAEA, Vienna 2016
- International Atomic Energy Agency, Development and Application of Level 1 Probabilistic Safety Analysis for Nuclear Power Plants. Specific Safety Guide Safety Standards Series No SSG-3, IAEA, Vienna (2010)
- International Atomic Energy Agency, Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plants. Specific Safety Guide Safety Standards Series No. SSG-4-4, IAEA, Vienna, (2010)
- International Atomic Energy Agency, Probabilistic safety assessments of nuclear power plants for low power and shutdown modes, IAEA-TECDOC-1144,

- International Atomic Energy Agency, Determining the quality of probabilistic safety assessment (PSA) for applications in nuclear power plants, IAEATECDOC-1511, IAEA, Vienna (2006)
- International Atomic Energy Agency, Safety of Nuclear Power Plants: Design Specific Safety Requirements, Safety Standards Series SSR-2/1, IAEA, Vienna (2012).
- International Atomic Energy Agency, Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3), IAEA-Safety Series 50-P-12, IAEA, Vienna (1996).
- International Atomic Energy Agency, The role of automation and humans in nuclear power plants - TecDoc 668. IAEA, Vienna, 1992 ISSN 1011-4289

18. WENRA references (Ref. 7)

- WENRA Safety Reference Levels for Existing Reactors. September 2014. Western European Nuclear Regulators' Association Reactor Harmonisation Working Group.

19. Other national standards (Ref. 8)

- Health and Safety at Work (etc.) Act 1974

20. Other international standards (Ref. 9)

- US Nuclear Regulatory Commission, Human-System Interface Design Review Guidelines, NUREG 0700, Revision 2, May 2002.
- International Nuclear Safety Advisory Group, Basic Safety Principles for Nuclear Power Plants, 75-INSAG-3 Rev. 1, IAEA, Vienna (1999)

2.3 Use of Technical Support Contractors

21. During Step 2 I have not engaged Technical Support Contractors (TSC) to support the assessment of HF for the UK HPR1000.

2.4 Integration with Other Assessment Topics

22. Early in GDA, I recognised the importance of working closely with other assessors (including EA's assessors) as part of the HF assessment process. Similarly, other assessors sought input from my assessment of the HF for the UK HPR1000. I consider these interactions key to the success of the project in order to minimise gaps, duplications or inconsistencies in ONR's assessment. I have endeavoured to identify potential interactions between the Human Factors and other technical areas and will continue to do so throughout the UK HPR1000 GDA.

23. Interactions between HF and some technical areas need to be formalised since aspects of the assessment in those areas constitute formal inputs to the HF assessment, and vice versa. These comprise:

- Fault Studies / Design Basis Analysis (DBA): provide input to the identification of Human Based Safety Claims (HBSC). This formal interaction has commenced during GDA Step 2. This work is being led by the Fault Studies Inspectors.
- PSA: provides input to the identification of the HBSCs, human failure events and evaluation of their importance to UK HPR1000 risk. In addition, the HF assessment provides input to the PSA for the HRA components. This formal interaction has commenced during GDA Step 2. This work is a coordinated effort between the PSA inspector and myself.

- Internal and external hazards assessments provide input to the identification of the human-based safety claims aspects of the HF assessment. This formal interaction will commence during Step 3. This work will be jointly led by the Internal / External hazards inspectors and myself.
- Structural Integrity assessments provide input to the identification of the HBSC aspects of the HF assessment. This formal interaction has commenced during GDA Step 2. This work is being led by the Structural Integrity Inspector.
- The HF assessment provides input to and is informed by the assessment of Electrical and, Control and Instrumentation (C & I) aspects of the UK HPR1000. This work is jointly coordinated between the Electrical and C & I inspectors and myself.
- The HF assessment provides input to and is informed by the assessment of Mechanical Engineering aspects of the UK HPR1000. This work is jointly coordinated between the Mechanical Engineering inspectors and myself.

24. These interactions will expand as the GDA progress and will be recorded in later ONR assessment reports.

3 REQUESTING PARTY'S SAFETY CASE

25. During Step 2 of GDA, GNS submitted a PSR and other supporting references that outline a preliminary nuclear safety case for the UK HPR1000. This section presents a summary of RP's preliminary safety case in the area of HF. It also identifies the documents submitted by the RP that have formed the basis of my HF assessment of the UK HPR1000 during GDA Step 2.

3.1 Summary of the RP's Preliminary Safety Case in the Area of Human Factors

26. The RP states that "*The overall safety objective for the HF activities in the Generic Design Assessment (GDA) for the UK HPR1000 is to ensure that appropriate HF input is provided to all relevant design, safety case and associated management processes so that the nuclear safety risks associated with human error are As Low As Reasonably Practicable (ALARP).*" (Ref. 2). The aspects covered by the UK HPR1000 preliminary safety case and supporting submissions in the area of HF can be broadly grouped under 3 headings which can be summarised as follows:

- Human Factors Integration (HFI)
- Identification and assessment of HBSC
- Baseline Design

3.1.1 Human Factors Integration

27. The RP's HFI approach is summarised in the PSR with detail provided in the Human Factors Integration Plan (HFIP) (Ref. 10). The submissions describe the RP's approach to ensuring HF is integrated throughout the UK HPR1000, ensuring that the risk from human error is reduced ALARP, by:

- Integrating and interfacing with safety and design disciplines,
- Using appropriate methods to conduct HF analysis,
- Identifying and analysing human based safety claims,
- Capturing and identifying HF issues, assumptions, recommendations and requirements,
- Having a suitably qualified and experienced HF team.

3.1.2 Human Based Safety Claims

28. The RP claims, "*Human Actions important to safety will be systematically identified and task reliability and effective task performance will be substantiated*". In order to do this, the RP describes its approach for identification, assessment and substantiation of HBSCs through several submissions (Refs. 10-11).

29. The submissions identify the methods for identifying, screening and assessing and substantiating human based safety claims including: task analysis methods that will be used to describe and evaluate human-system interactions and the human reliability analysis methods that will be used quantify human error.

30. In addition to the above submissions, the RP provided a short list of HBSCs identified from the FCG3 project that are applicable to the UK HPR1000, in response to RQ-UKHPR1000-0098 The Role of the Operator in Assuring Nuclear Safety (Ref. 12). The list identifies HBSC in the Level 1 and 2 PSAs, accident analyses and the severe accident analyses.

3.1.3 Baseline Design

31. Chapter 2 of the PSR (Ref. 13) provides details on the basic HPR1000 design and its evolution through the CPR models. Neither this, nor the HF Chapter (Ref. 2), summarise the HFI into these designs or the allocation of functions. However, the design considers the following factors during the process of allocation:

- Performance requirements.
- Capabilities / limits of human and machine.
- Existing practices.
- Operating experience.
- Management requirements.
- Technical feasibility.
- Cost.

3.2 Basis of Assessment: RP's Documentation

32. The RP's documentation that has formed the basis for my GDA Step 2 assessment of the safety claims related to the HF aspects of the UK HPR1000 is presented in:

- Preliminary Safety Report Chapter 15 Human Factors, HPR/GDA/PSR/0015, October 2017 (Ref. 2). This report summarise the RP's safety case for HF
- Human Factors Integration Plan, GH X 06001 016 DIKX 03 GN, April 2018 (Ref. 14).
- Function Allocation Methodology, GH X 06001 019 DIKX 03 GN, April 2018 (Ref. 15).
- HFE Design Guidelines for Control Room, GH X 06001 021 DIKX 03 GN, April 2018. This document summarises RGP for control room design into a guidance document (Ref. 16).
- Task Analysis Methodology, GH X 06001 042 DIKX 03 GN, April 2018. Task analysis is the process by which HF engineers gain insight into human-technology performance and this document describes the RP's method for this analysis (Ref. 17).
- Methodology of Human Reliability Analysis, GH X 00650 030 DOZJ 02 GN, May 2018 (Ref. 11). Human Reliability Analysis attempts to identify where human errors can occur. This document describes the RP's approach for quantitatively modelling the probability of these errors.
- Treatment of Important Human Actions Plan, GH X 06001 015 DIKX 03 GN, July 2018 (Ref. 10). This document describes how the most important human actions will be identified for further task and human reliability analysis.

33. In addition, during April 2018, GNS submitted to ONR for information, an advance copy of the UK HPR1000 Pre-Construction Safety Report (PCSR). Chapter 15 (Ref. 2) addresses HF. Having early visibility of the scope and content of this chapter/s has been useful in the planning and preparation of my GDA Step 3 assessment work.

4 ONR ASSESSMENT

34. This assessment has been carried out in accordance with HOW2 guide NS-PER-GD-014, "Purpose and Scope of Permissioning" (Ref. 3).

35. My Step 2 assessment work has involved continuous engagement with the RP's HF specialists, including two technical exchange workshops (in China) and regular progress meetings. In these exchanges, I have provided advice and guidance to the RP to provide clarity of ONR's regulatory expectations in the area of HF. Advice and guidance has been provided in the following areas:

- Technical HFI, i.e. where in a plant design would HFI be expected.
- Organisational HFI, i.e. the expected working interfaces between the HF team and other technical disciplines.
- Safety case expectations.
- Approaches to HRA, including qualitative analysis / substantiation.
- ONR's regulatory concerns over the use of modern digital screen-based control rooms.

36. During my GDA Step 2 assessment, I have identified some gaps in the documentation formally submitted to ONR. Consistent with ONR's Guidance to Requesting Parties (Ref. 18), these normally lead to RQs being issued. At the time of writing my assessment report during Step 2, I have raised four RQs to facilitate my assessment (See Annexe 2).

37. Details of my GDA Step 2 assessment of the UK HPR1000 preliminary safety case in the area of HF, including the conclusions I have reached, are presented in the following sub-sections of the report. This includes the areas of strength I have identified, as well as the items that require follow-up during subsequent steps of the GDA of UK HPR1000.

4.1 Human Factors Integration

4.1.1 Assessment

38. 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, and as ONR is a sampling organisation, we place significant reliance on the efficacy of the HFI process.

39. ONR's expectations within this area are set out within NS-TAST-GD-058 (Rev 3) Human Factors Integration (Ref. 5). These expectations can be summarised as the RP (or licensee) demonstrating suitability and sufficiency in the following areas:

- The capability of the organisation / HF Team
- The scope of HFI
- Technical programme
- Concept of Operations
- Managing Issues and Assumptions
- Standards, Codes, and Methods

40. It is recognised good practice to describe the detailed approach in the above areas in a HFIP, which provides an organising framework for the integration of HF.

41. The RP submitted its UK HPR1000 HFIP (Ref. 14) at the end of April 2017. My judgement on the adequacy on the RP's HFI capability is discussed below.

4.1.1.1 HF TEAM

42. A key focus of my regulatory engagements with the RP for Step 2 has been to ensure that the RP organisation has a sufficient and capable HF organisation to deliver a generic reactor design that could be built and operated, in a way that is acceptably safe and secure (subject to site specific assessment and licensing).

43. The HF capability for the UK HPR1000 GDA currently lies within the CGN organisation. GNS does no yet, have in post a HF Suitably Qualified and Experienced Person (SQEP) to act as an Intelligent Customer (IC). Currently IC advice is being provided by EDF-Nuclear Generation (EDF-NG) HF SQEPs. At the time of writing this report, the RP is in the process of securing additional UK supply chain support.

44. I consider the lack of IC capability within GNS to be a gap against expectations. GNS recognise this gap and are seeking to rectify it and I have observed EDF-NG providing suitable IC level advice in the interim period. Evidence of this in practice was the decision by the RP not to issue an HBSC report to ONR because it had failed to meet the RP's quality standards. I have also observed a steady improvement in deliverable quality since the start of Step 2, although I note further improvements are required during Step 3.

45. In addition, the CGN HF capability is typical of many international reactor design organisations as it resides within the C&I discipline. Whilst this organisational approach has been shown to support the delivery of safe and operable C&I based Human Systems Interfaces (HSI), during previous GDAs, it has sometimes been initially deleterious to integrating HF into areas outside of C&I. This also means that the majority of the HF team have C&I backgrounds rather than formal HF training. I raised these concerns with the RP early in Step 2. The RP has made a considerable effort to address this shortfall and have committed to ensuring that areas outside of the Main Control Room (MCR) receive the necessary HFI commensurate with risk. The lack of integration into areas other than the MCR is a shortfall, but one I consider mitigated at Step 2 by the fact that the HPR1000 is an evolutionary Pressurised Water Reactor (PWR) design rather than one featuring high levels of novel technology.

46. CGN has started a programme of training for its internal HF resource, which is being delivered by EDF-NG. CGN recognised the potential for significant differences between GB and Chinese regulatory expectations and has contracted EDF-NG to provide bespoke general training in HF. It has also established a programme of UK supply chain support in the area of HF.

47. I am satisfied that CGN are undertaking all reasonably practical measures to address the GB specific knowledge gap for GDA.

48. The RP presented to me the results from a work-planning exercise to predict the resource levels required to support the entirety of GDA. The resource levels identified were broadly commensurate with previous GDAs. An early understanding of resource needs for GDA is critical to its success and maximises the likelihood of securing the necessary resource.

49. At this stage of GDA, the RP has not sufficiently demonstrated its extant HF organisational capabilities. However, it has provided sufficient evidence for me to be confident that an adequate resource position can be reached during Step 3. This confidence comes from the significant improvement observed between the start of GDA and the end of Step 2, and in particular from information provided within the HFIP and Level 4 interactions that have shown a clear commitment to gaining sufficient in-house and external capability. I also draw confidence from the HFI evidence I was shown during the initial engagement meeting (Ref.19) where non-HF SQEPs have

ensured that consideration of the role of the operator has been considered as part of other disciplines design processes. Examples include, decommissioning considerations and the design of the fuel route crane.

50. This judgement is, of course, predicated on there being sufficient international resource available to support this project.

4.1.1.2 SCOPE OF HFI

51. I have sought evidence that the RP has demonstrated sufficient understanding of the technical scope of HFI expected by ONR to form the basis of a meaningful GDA.

52. At the close of Step 2, the RP has demonstrated sufficient understanding of the discipline interfaces necessary for effective HFI during GDA. I consider the HFIP adequately describes the HF interfaces and activities necessary to deliver a meaningful GDA and these meets regulatory expectations.

53. The HFIP identifies a comprehensive list of disciplines / technical areas (based on the PCSR chapters) where HF will need to be formally considered. I judge this list to be complete when considered against expectations for HFI.

54. The identification of these disciplines / technical areas has been used to inform the HF work programme discussed below in Section 4.1.1.3. To ensure that the necessary integration occurs in practice, CGN has committed (Ref. 14) to revising its design process to ensure there is formal consideration of HF, where appropriate to do so, by using a combination of: hold-points, design reviews, and process monitoring and reporting.

55. The descriptions of the work that will be undertaken in support of these areas are high-level, making a judgment of adequacy difficult. However, I am satisfied that the task detail underpinning these technical areas will be made available as and when necessary as it is the nature of a staged HFI process. I will follow-up the developing scope of the work packages during Step 3 to ensure that the work meets ONR's regulatory expectations.

56. The scope of the HFI programme has also been informed by a gap analysis performed by the RP between the HF work performed for FCG3 and ONR's regulatory expectations. This analysis identified 3 high level gaps:

- Gap 1 - The Operating Experience Review (OPEX) scope is not appropriate in the GB context.
- Gap 2 - There are several gaps in identification and substantiation of important
- human actions:
  - Gap 2.1 - Important human actions list is not complete
  - Gap 2.2 - The method for screening actions for detailed human reliability assessment is not appropriate in the UK context
  - Gap 2.3 - The HRA method used for Type C human error events is not appropriate under ONR's regulatory framework
- Gap 3 - There are several gaps in HF supporting SSC design
  - Gap 3.1 - HFE specification for FCG3 was based on Chinese human dimensions and target audience habits.
  - Gap 3.2 - For the equipment and Human Machine Interface (HMI) local to plant (outside the MCR area), there is no systematic process for HF supporting Systems, Structures and Component (SSC) design.

57. Whilst significant work will be needed to address these gaps, the gaps are consistent with other Step 2 starting positions during previous GDAs. Having a clear

understanding of the scope of HFI and how it informs the work programme is key to a successful GDA and I am satisfied that the RP adequately understands this scope.

58. However, the RP acknowledges that the HFI into the FCG3 design was primarily focussed on the main control areas, e.g. MCR and remote shutdown room. This would not be acceptable under ONR's regulatory framework, and whilst I have observed that some non-HF disciplines have specifically considered the role of the operator, this was not achieved under a systematic programme of HFI. I also note that other disciplines are also capturing, and committing to addressing, HF shortfalls. For example, I welcome the fact that the Fault Studies team noted in their gap analysis of the SAPs that they would need to classify HBSCs, as done for SSCs. A practice not conducted in China.

59. Given such widespread levels of HFI are novel for the RP, during Step 3 I will pay particular attention to how HFI is managed outside of control rooms and in areas where the RP acknowledges it has little HFI experience. Again however, I consider this shortfall somewhat mitigated at Step 2 by the evolutionary nature of the HPR1000 design.

4.1.1.3 TECHNICAL PROGRAMME

60. Another key focus of my regulatory engagements with the RP, during Step 2, has been to influence the early production of a HF work programme integrated into the wider GDA design and safety programme. I consider this an essential planning tool to ensure that dependencies and critical paths are accounted for during the scheduling of packages of work. It is also key to ensuring that sufficient SQEP resources are available as and when needed; an important consideration in a discipline where there are shortages of SQEP resource.

61. I have been shown a number of iterations of the HF programme over the course of Step 2. I am satisfied that the RP recognises the importance of developing the programme and have observed that it is being correctly used to identify resource requirements and to schedule deliverables. The RP now has an estimate of the total numbers of HF SQEPs needed to support GDA, which appears reasonable when compared to previous GDAs.

62. The latest formal version of the HF programme is presented within Appendix 1 of the HFIP (Ref. 14) and currently contains 25 high level tasks. It is possible to align these 25 tasks with the disciplines / technical areas described in Section 4.1.1.2 and the Gaps identified within the FCG3 gap analysis reported in the HFIP (Ref. 14).

63. Currently not shown are the dependencies and critical path, as would be expected when following RGP. I have also not had visibility of how the HF work programme integrates into the wider GDA programme. I expect this programme plan to expand significantly during Step 3 as the detail underpinning the 25 high level tasks is better understood. However, for Step 2, I judge that the level of detail presented is sufficiently complete and detailed to gain sufficient confidence in the RPs understanding of what needs to be done in the area of HF during GDA for Step 3.

64. Post assessment note: Since completing my assessment, I have been shown a revised work plan that contains significantly more detail than that contained within the HFIP. This provides good confidence in the RP's ability to be able to understand and plan the necessary HFI required for the UK HPR1000.

4.1.1.4 CONCEPT OF OPERATIONS

65. It is relevant good practice to define the Concept of Operations (CoO) for a new reactor design, and this is reflected as an expectation within TAG 058 (Ref. 5). ONR expects the following:

- A statement of the operational purpose of the systems. This will highlight the functions to be performed by the system and how the system is operating to achieve those functions.
- A consideration of the command and control philosophy – how is the system intended to be operated during normal and fault response situations.
- The staffing concept for the system and an indication of their required capabilities and responsibilities. This is also known as the Target Audience Description (TAD).
- The basic details of the working environment.

66. The RP has provided limited information in these areas for Step 2, but acknowledges this gap and a CoO deliverable is described in the RP's HFIP, to be provided early in Step 3. Whilst this is later than ideal for GDA, I consider it adequately mitigated. The FCG3 baseline design is currently in build and an evolution of the CPR1000, CPR1000+, and ACPR1000 designs. The HPR1000 has been designed, taking into account international and domestic evolutionary operational experience; key to which are the lessons learned from the Fukushima accident, which placed significant operational demands on the operator. These evolutionary advances are summarised within Chapter 2 of the PSR (Ref. 13). Those pertinent to my HF assessment include improvements to the MCR habitability and the introduction of in-vessel retention capability to extend the operator grace times for emergency equipment preparation.

67. What remains unclear within the submissions to date is the balance of human actuated safety systems and those activated automatically. The RP acknowledges this information gap and has committed to providing further detail within the fault schedule, which aligns with relevant good practice.

68. To better understand the balance of automation prior to the delivery of the fault schedule, I raised RQ-UKHPR1000-0098 The Role of the Operator in Assuring Nuclear Safety – Detail Required to Support Step 2 Assessment to elicit further information on the role that the operator with respect to nuclear safety. The response to this RQ was not satisfactory as it failed to provide sufficient detail on the functional split between the human and the technology. The key points established were:

- Start-up to 15% power is manually performed,
- 15-100% power is performed automatically,
- The design is compliant with SAP ESS.8 Automatic Initiation – the '30 minute rule'. No operator actions are required within the first 30 minutes of a design basis fault.
- For '*most*' design basis faults the plant can be brought to a safe stable state by automation alone. There are '*some*' instances where human intervention is required.

69. The detail behind '*most'* and *'some'* was not provided. This is an area I will be following up during Step 3.

70. A TAD was not supplied for Step 2. As per the CoO document, the RP has declared that the TAD will be completed early within Step 3. The TAD will be required to inform design reviews of the baseline design to flag up compatibility issues between the Chinese and GB operators; these reviews will not start until Step 3.

71. The RQ response sets the assumption that the command and control philosophy will be similar to that used in existing GB Nuclear Power Plants (NPP). Further details on command and control assumptions will need to be defined as the GDA progresses, but for Step 2, it is sufficient to have clarity that the model will be that used in GB and not in China.

72. Although the detail relating to the concept of operations is lacking at Step 2, there are a number of factors that mitigate this gap. The UK HPR1000 is not a completely new or novel design. It is an evolution of previous operational designs and has taken on board OPEX from these precursor designs as well as international OPEX, such as that from Fukushima. It also benefits from a development simulator which has been used for user testing. I thus consider the likelihood of finding a significant HF issue – one that cannot be rectified during Steps 3 and 4 of GDA – to be low. I will however, follow-up on this matter early in Step 3.

4.1.1.5 MANAGING ISSUES AND ASSUMPTIONS

73. It is RGP to proactively identify, record, sentence and address HF issues for a new reactor design, and this is reflected as an expectation within TAG 058 (Ref. 5). A similar expectation exists for assumptions, which should be captured for future validation by the operating organisation.

74. The creation of an issues and assumptions register is currently work-in-progress by the RP. There is a commitment to delivering this tool early within Step 3 and the HFIP provides an overview of the process. However, it is important to note that there already exists a formal design issue resolution process within CGN so there are existing tools for managing all issues.

75. I consider the creation of this tool for Step 3 to be late within the GDA process, but as I will be an enhancement of an existing process, I am satisfied it can be delivered within Step 3.

4.1.1.6 STANDARDS, CODES, AND METHODS

76. The requirement for risks to be ALARP is fundamental and applies to all activities within the scope of the Health and Safety at Work (etc.) Act 1974. In simple terms it is a requirement to take all measures to reduce risk where doing so is reasonable. In most cases, this is not done through an explicit comparison of costs and benefits, but rather by applying established RGP and standards. The development of RGP and standards includes ALARP considerations so in many cases meeting them is sufficient. Therefore, key to a successful GDA and demonstration of ALARP is establishing and applying a suite of appropriate standards, codes and methods.

77. It is clear the FCG3 baseline design has been informed by a combination of international, US, and domestic Chinese standards, codes and guidance. Where Chinese domestic standards have been followed, these are often based on US or International standards.

78. The RP recognises that the standards followed for the FCG3 design may not be applicable for deploying the reactor design in GB. It notes that there may be differences between GB and Chinese operators and has committed (Ref. 14) to conduct research into this area to establish which elements of baseline design can be carried forward for the UKHPR1000.

Human Factors Engineering Guidance (Codes and Standards)

79. ONR expects the suitable and sufficient provision of workplaces and user interfaces for nuclear facilities (SAPs EHF.6 and EHF.7).

80. A key enabler to the delivery of these workspaces and interfaces is establishing a baseline of appropriate modern codes and standards.

81. For Step 2, the RP has only submitted one of three currently planned design guidance documents. The submitted guidance concerns the layout and environmental specifications for control rooms. It also provides some guidance on analogue HMI layout. The two submissions not ready for Step 2 comprise: guidance on the design of SSCs to minimise Examination, Maintenance, Inspection and Testing (EMIT) error and guidance on the design of interfaces. As their application will be in Step 3, I do not consider this to be of significant concern.

82. I consider the control room guidance to be generally appropriate. It covers the following topics:

- Work Space
- Structure
- Space and Overall Layout
- Environment
- Operating Workstation
- Stand-up Control Console Design
- Display Devices
- Control Devices
- Layout of Display and Control Devices
- Labelling and Demarcations

83. It cites the relevant British and ISO standards and some United States (US) Nuclear Regulatory Commission Regulation (NUREG) standards relating to control room design. For example:

- Human-System Interface Design Review Guidelines – NUREG 0700. Revision 2. Nuclear Regulatory Commission.
- ISO 11064 Ergonomic Design of Control Centres

84. However, the content is poorly referenced, making it difficult to trace each requirement to the originating source to provide confidence that the correct and up-to-date standard has been used. I will carry out a targeted assessment of the application of design guidance during Step 3 to determine whether the design is being informed by current appropriate codes and standards.

85. Additional planned documents include:

- HF Guidelines for HMI Design.
- HF Guidelines for Local Control Area.

86. Assuming appropriate quality, I consider that these documents should address the omissions noted within the submitted design guidance.

87. Overall I am satisfied that RP has identified / will identify appropriate codes and standards for the HPR1000 GDA. It is an area I will follow up during Step 3.

Allocation of Function Methodology

88. ONR expects that when designing systems, dependence on human action to maintain and recover a stable and safe state should be minimised. The allocation of safety actions between humans and technology should be substantiated (SAP EHF.2). ONR TAG 064 (Ref. 5) guides that Allocation of Function (AoF) should not be a simple binary output as there can be many permutations involving both static and dynamic allocation and degrees of automation, each of which has positive and negative effects

on human performance. AoF decisions need to demonstrate appropriate consideration of the hierarchy of control, and record and substantiate where trade-offs have occurred to optimise the system performance.

89. The RP submitted Reference 15, "Function Allocation Methodology", to explain how it will allocate any new safety functions and re-visit previous allocation decisions to substantiate that they remain valid when being translated from the FCG3 baseline design to the UK HPR1000. The FCG3 AoF concept appears to have been driven by previous decisions and in response to OPEX. This provides some confidence that the fundamental AoF is likely to be sound as the HPR1000 design is an evolution of a number of older PWR designs.

90. The RP's method appears to be based on a combination of British Standards NUREG Guidance (Refs 20, 21, and 22). It considers the following factors:

- Performance requirements;
- Capabilities/limits of human and machine;
- Existing practices;
- Operating experience;
- Management requirements;
- Technical feasibility;
- Cost.

91. The output is a list of functions for which automatic or manual execution is required.

92. I consider this to be a sensible starting point, but it will need developing as the current binary output is not sufficiently subtle. It will also need a step adding to it in relation to validating the AoF decision to ensure that the theoretical optimisation is practically demonstrated. Automation is a highly complex topic as there are multiple automation levels and these levels can replace each of the human-sensory-processing-action stages (detect stimulus, process stimulus, determine decision based on stimulus, respond to stimulus). Whatever method is ultimately employed, it needs to be subtle enough to accurately determine the type of automation to be provided and at what stage so that the human-system performance is optimised; playing to the strengths of both. I will monitor the progression of the RPs AoF method during Step 3.

Qualitative HRA / Task Analytical methods

93. ONR expects that Task Analysis be performed of all tasks important to safety and that the analysis be of sufficient detail to justify the effective deliver of the safety functions to which they contribute (SAP EHF.5).

94. The RP's approach to task analysis is set out within several different references:

- Reference 17, Task Analysis Methodology, describes the RP's approach for Hierarchical, Tabular, and Time-Line analyses.
- Reference 15, Allocation of Function, describes the RP's approach for determining and retrospectively assessing Allocation of Function

95. The RP has clearly taken on-board the advice and guidance, provided by ONR during Step 2, on expectations regarding substantiating HBSC. The factors that the RP has identified to be considered during task analysis meet RGP and thus regulatory expectations. The method guides the analyst to consider all relevant performance shaping factors, such as the person, location, equipment, environment, temporal, etc. factors. As yet, I have seen no evidence of the output from this guidance, so whilst the guidance appears generally sound, I cannot comment on its application.

96. A further observation is that the guidance is limited to the three methods described below. Guidance does not yet exist for cognitive workload assessment, situational awareness assessment, misdiagnosis, and other areas where analysis may be necessary. These are not needed for Step 2, but the RP will quickly need to establish its approaches in each of these areas for Step 3, as they may need to be used to substantiate HBSCs during Step 3.

97. High quality task analysis is fundamental in substantiating the effective delivery of HBSCs, and I am content that the methods can deliver high quality task analysis. They adequately capture ONR's expectations that have been set out during regulatory interventions during the course of Step. 2.

Quantitative HRA Methods

98. To assess Human Reliability and understand the human contribution to numerical risk, the RP has elected to use US Nuclear Regulatory Commission (NRC) HRA methods. Reference 11, presents the RP's methods for Type A, B, and C error analysis and quantification:

- Type A Errors - Human errors during EMIT activities which lead to a latent failure or degradation of a safety system, structure or component - will be modelled using the Accident Sequence Evaluation Program (ASEP) (NUREG/CR-4772) (Ref. 23). ASEP is a modified version of the Technique for Human Error Rate Prediction (THERP) (Ref. 24) which has been used widely within the GB nuclear sector.
- Type B Errors – Human errors that can initiate a fault / unanticipated transient – will be modelled using THERP (Ref. 24)
- Type C Errors – Human errors that can occur during or following a transient / fault / accident sequence – will be modelled using the Standardized Plant Analysis Risk Human Reliability Analysis (SPAR-H) (Ref. 25) approach. SPAR-H is also based on the THERP method.

99. These methods have been selected on the basis of the RP's familiarity with their application and their wide-spread international use, which is sensible as familiarity of methods has been show in HRA studies as a determining factor in data accuracy. However, these methods are not without problems, and HRA in general is not an exact science.

100. First, as the above methods are based on the THERP method and the underlying data were collected during the early days of the US nuclear industry. This means that the underpinning database is not reflective of screen-based digital C&I interactions. In fact, THERP specifically excludes its use for modelling "*new display and control technology that is computer based*" (Ref. 24). Earlier generation control rooms were analogue dial and switch based, whereas the UK HPR1000 control room is controlled predominantly via screen-based computer interfaces.

101. Second, these methods were designed to support the US model of HRA, which typically splits HF and HRA into two separate disciplines. The qualitative analysis necessary to produce best estimate data is divorced from the HRA process; ASEP and SPAR-H use tick-box style pro-forma to elicit qualitative detail instead of detailed task and error analysis. ONR's regulatory expectations are that HRA and HF are fully integrated, with the emphasis being on the qualitative analysis rather than the numerical analysis. US HRA methods do not lend themselves to this approach.

102. In discussion with the RP, ONR's PSA inspector and I explained that whilst ONR has no fundamental objections to the use of these methods, we do expect the RP to specifically consider and address the above issues. The RP has acknowledged this

and we have discussed how these shortfalls may be addressed. However, this understanding and discussions are not reflected in the HRA methodology – produced by the HRA team within the PSA team. In particular the qualitative analysis section is lacking in detail. The RP's HF team has submitted a Task Analysis method document (Ref. 17) which in effect supplements the HRA method report, but neither report is referenced from the other and the Task Analysis report makes no mention of HRA. Thus, it is not possible to determine how the qualitative analysis will be used to inform the quantitative analysis. This is of concern as it reinforces the separate nature of HF and HRA rather than promoting an integrated approach, which is counter to the expectations given in SAP EHF.10 and is a clear regulatory expectation.

103. This gap has not undermined my Step 2 assessment, but it will require follow-up from ONR's HF and PSA Inspectors during Step 3, and improvements by the RP in its integrated approach to HRA. This topic is also the subject of RQ-UKHPR1000-0134 Human Reliability Analysis that has not been responded to within the time-scales of Step 2.

Identification and Screening of Human Based Safety Claims

104. ONR expects that a systematic approach should be taken to identify human actions that can impact safety during normal and fault conditions (SAP EHF.3).

105. ONR further expects that the identification process should consider a wide range of sources including the fault schedule, the PSA, and OPEX data (Ref 5).

106. The RP's approach for the identification and screening of HBSCs is set out in Reference 10, "Treatment of Important Human Actions Plan". The methodology describes the process for the identification of HBSCs drawing from the following sources:

- DBA
- PSA
- Severe Accident Analysis
- Conventional Safety Analysis
- OPEX data

107. Its scope also considers HBSCs for each human failure mode: Type A; Type B; and Type C.

108. Within each of these error types: omission, commission, and misdiagnosis errors will be considered. A review of human-human and human-system dependencies is also planned.

109. I consider the RP's approach to the identification of HBSCs to be generally sound displaying most of the attributes of what ONR would consider as RGP. However, I note a minor omission which is the lack of review of engineering substantiation reports / basis of safety type documents. These can be a source of implicit HBSCs which do not make it into the DSA / PSA / Severe Accident Analysis (SAA). I will follow this up as part of normal business during Step 3.

110. It would be both disproportionate and impractical to analyse every human action performed on a NPP. ONR recognises the need for proportionality under SAP EHF.5. The RP has recognised the importance of limiting the scope of the analysis to proportionate levels and has developed screening criteria for each of the human failure modes described above.

111. Type A errors are essentially screened on the basis of the importance of the equipment on which the EMIT activity is being performed, which is a sensible

approach. However, there are additional criteria used which can exclude EMIT HBSCs if these criteria are met. These include:

- Those errors which would cause an alarm to be raised in MCR can reasonably be expected to be identified and addressed. These will be recoded but not be assessed further.
- Those errors that would be captured by a required proof test can reasonably be expected to be identified and so will be recoded but not be assessed further.

112. These criteria may exclude important human actions which should be subject to detailed assessment. For example, just because an alarm is raised does not mean that a) the operator can practically do something about the failure, and b) the alarm may not be sufficient to prompt accurate diagnosis. Further, excluding on the basis of a proof test may mean that the plant has to tolerate a highly unreliable EMIT task on the basis that the proof test is likely to pick up a fault. This is neither ALARP nor sound engineering practice, and places significant reliance on the proof test, which may in itself not have been assessed. The PSA Inspector shares my concerns in this area, and whilst these concerns have not undermined my Step 2 assessment, they will require further regulatory interventions early in Step 3 to ensure that the RP has fit for purpose screening criteria for use during GDA.

113. Type B errors are rare within the control room during at power operations. Reactor protection systems are designed to prevent them. More likely, although still rare, are Type B errors relating to fuel route, waste handling, etc., type activities where direct human actions are more prevalent. I welcome the fact that the RP has recognised this and developed its screening criteria for Type B errors appropriately.

114. Type B errors are screened by identifying those systems that can lead to a worker or public dose and then reviewing the systems to determine whether mal-operation can result in radiation or contamination exposure. These reviews will utilise pre-existing master logic diagrams and failure modes and effects analysis. The RP will attempt to group / bound any errors identified as worst case scenarios. I consider this approach, in principle, to be sensible.

115. The RP is planning to screen Type C errors using the PSA, SAA, and the Fault Schedule.

116. PSA screening will be based on Risk Achievement Worth (RAW) and Fussel- Vesely (FV) values. These provide risk importance values for each human failure event within the PSA fault tree. The screening values for each of these criteria are yet to be defining and my PSA colleague and I will discuss this further with the RP at the start of Step 3. My PSA colleagues notes that there are further numerical criteria that can be used to provide additional analytical insight into the risk contribution of the operator and these will be discussed with the RP. In principle however, assuming the values are set with an appropriate sensitivity level, the use of RAW and FV can be considered to be RGP.

117. For those HBSCs relating Severe Accident (SA) response that are not yet modelled in the PSA, the RP plans to use SAA mitigating strategies to identify manually actuated systems, which by definition equate to a HBSC. The RP plans to include both MCR and local actions. Using both PSA and accident mitigation strategies to identify SA HBSCs is considered to meet RGP. However, there may be benefit in the RP looking at OPEX / lessons learned from previous accidents to inform the SA HBSC list.

118. The Fault Schedule will be used to identify HBSCs that support any safety functions. Class 1 and 2 safety function supporting HBSCs will be subject to detailed

assessment. For lower class (3 and below), only high level analysis will be performed. In principle, I consider this approach to follow RGP.

119. I note also that the RP plans to conduct analysis of human actions that can have conventional safety implications. The method for this has yet to be defined but I will seek input from my conventional and health and safety colleague with respect to judging its adequacy.

4.1.2 Strengths

120. During my GDA Step 2 assessment of HFI I have identified the following specific strengths:

- The RP has responded positively to constructive advice and guidance provided by ONR in the areas of HFI and the methods it plans to use during GDA. I have observed significant improvements in the organisation, planning, and methods to be used for GDA.
- The codes, methods and standards identified broadly align with RGP. Of note here, is the RP's improvements to the qualitative phase of its HRA method.
- The RP has quickly established a credible HF programme and has implemented sensible solutions to resource and capability shortfalls.

4.1.3 Items that Require Follow Up

121. During my GDA Step 2 assessment of Human Factors I have identified the following specific shortfalls:

- Whilst resource and capability levels within the RP have steadily increased throughout Step 2, there remains improvements in both resource and capability to be made. I will monitor progress in this area during the remainder of GDA.
- HFI of the scope expected by ONR is novel to the RP. I will continue to monitor progress in this area during the remainder of GDA to ensure that it is being suitably and sufficiently delivered.
- A fully integrated work programme is key to ensuring the timely and effective integration of HF into all appropriate analytical and design topics. The level of detail in the HF programme has substantially increased throughout Step 2 but this programme will need to be live throughout GDA. I will monitor the credibility and effectiveness of this programme throughout the remainder of GDA.
- The RP has committed to providing additional information on the concept of operations for the HPR1000. I will assess this deliverable during Step 3.
- I will monitor the effectiveness of the issues and assumptions register via sampling of its application. I will carry out this intervention jointly with discipline relevant ONR inspectors.
- The RP has committed to submitting its design guidance for local to plant interfaces and SSC design as well as human machine interface design. I will assess the adequacy of this guidance during Step 3.
- I have identified some shortfalls in the RP's allocation of function methodology in relation to how it optimises the level and type of automation selected. Currently it delivers a binary result: human or technology and fails to guide the optimised level of automation. I plan to conduct an intervention on this topic at a future Level 4 meeting.
- Human Reliability Analysis. The screening criteria presented may, in practice, exclude important human actions that should be subject to detailed HRA, but this can be addressed early in Step 3 before the method is fully deployed. The

RP has also not discussed how it plans to model misdiagnosis or human computer interactions. My PSA colleague and I plan to carry out an intervention in this area early in Step 3 to discuss the methodological detail and application of the totality of the HBSC / HRA approach.

122. During my GDA Step 2 assessment of HF I have identified the following area that may require research to be undertaken by GNS in order to underpin the safety claims made on the computerised interfaces. I will follow-up these matters, as appropriate, during Step 3:

- The RP's selected HRA methods are not suitable for modelling human-computer interactions as their underlying databases comprise data drawn from interactions using traditional analogue panels. Previous ONR work in this area during the first GDAs identified that the human error probabilities may be optimistic as a result. ONR expects that RPs should seek to address this weakness via appropriate means.

4.1.4 Conclusions

123. Based on the outcome of my Step 2 assessment of HFI, I conclude that the RP's approach to HFI broadly meets RGP. This judgement is based on the fact that the RP has addressed the initial organisational concerns about HF working predominantly within the C&I area and has submitted a credible suite of standards, codes and methods with which to ensure HF is adequately integrated into the design.

4.2 Human Factors Claims

4.2.1 Assessment

124. The primary aim of Step 2, with respect to HF, is to establish the acceptability of the key safety claims (HBSCs) in accordance with the GB regulatory regime (Ref. 18).

125. There are typically two fundamental claim types used within a safety case. These comprise:

- Process Claims, which typical refer to achieving a particular result by following processes / meeting standards.
- Safety Functional Claims – HBSCs in HF terms, which refer to the specific functioning of equipment or persons that directly relate to maintaining a critical safety function (e.g. control of reactivity and decay heat removal).

126. For Step 2, the RP has established a series of process claims:

- Claim 1 - The HF activities are organized and managed by an HF integration plan.
- Claim 2 - The allocation of safety actions between humans and engineered SSCs is substantiated to make sure that the dependence on human action to maintain and recover a stable, safe state be minimised.
- Claim 3 - Important human actions will be systematically identified and substantiated.
- Claim 4 - User-friendly interfaces are provided for delivering monitoring and control of the facility.
- Claim 5 - Workspaces where operations (including maintenance activities) are performed are designed to support reliable task performance.
- Claim 6 - Procedures will be developed to support reliable human performance by instructing human actions that could impact on safety.
- Claim 7 - Suitably Qualified and Experienced Persons will be available to operate the facility in all operational states.

127. I consider the RP has provided sufficient evidence to demonstrate that achieving these claims is credible within the GDA:

- It is in the process of establishing a fit for purpose HFI process, has identified its resource needs, and is in the process of securing additional resource and training.
- It has identified, and is continuing to identify, appropriate codes and standards appropriate for the deployment within GB.
- The process for identifying HBSCs, whilst still embryonic at this stage of GDA, is showing evidence that it can meet RGP.
- The allocation of function process, similar to the identification of HBSCs process, has now been established, and whilst in need of some iteration to meet RGP, is heading towards a position of acceptability.
- I have observed first-hand the RPs capability with respect to development of interface designs and its ability to evolve and test concept designs.
- Both procedures and training are outside of the scope of GDA and I have advised the RP as such. However, it is positive that the RP has identified these areas now, as it is important to capture assumptions in these areas for future validation.

128. Whilst the process for identifying HBSCs is likely to meet RGP early in Step 3, the detail concerning what role the operator plays in ensuring nuclear safety has been lacking for Step 2. I requested further information via UK HPR1000-0098 The Role of the Operator in Assuring Nuclear Safety (Ref. 12) in an attempt to better understand this role, but the information provided did not provide the necessary clarity. It at least provided confidence that the baseline FCG3 safety case did identify, albeit a small number, of HBSCs. It is apparent that whilst the design appears relatively mature – I have observed the FCG3 MCR design simulator and detailed 3D models – the HPR1000 HF safety case is embryonic at this stage and behind where it should be for Step 2. It is also clear that additional safety case information is available but currently only in Chinese.

129. I advised (Ref. 26) the RP of the importance of identifying a comprehensive set of HBSCs relating to normal and fault conditions – as per SAP EHF.3. Based on discussions I am confident that, with the help of EDF, this can be achieved given EDF's GB experience.

130. The RP is behind GDA schedule expectations in this area, and whilst this has not undermined my Step 2 assessment, it is important that this work be given high priority within the RP as a significant improvement in clarity of the role of the operator is essential to complete a meaningful and timely Step 3. I will therefore be seeking to ensure that the RP provides clarity on the safety role of the operator with respect to the identification of explicit and implicit claims and the macro allocation of function as soon as possible in Step 3. This is to de-risk the likelihood of identifying any fundamental shortcomings that could prejudice the future issue of a Design Acceptance Confirmation (DAC).

4.2.2 Strengths

131. The RP has identified a credible set of process claims that I consider, can likely be substantiated during the remainder of GDA.

4.2.3 Items that Require Follow-up

132. During my GDA Step 2 assessment of HF I have identified the following specific shortfalls:

- The role the operator plays in ensuring nuclear safety is not clear for Step 2. The RP will need to provide a much more cogent and coherent description of this role for Step 3.
- The HBSCs supplied at the end of Step 2 are lacking detail and context. This will need developing throughout GDA.

133. During my GDA Step 2 assessment of HF I have identified the following areas that may require research to be undertaken by GNS in order to underpin HBSCs. I will follow-up these matters, as appropriate, during Step 3:

- It is unclear how the RP will model or assess human-computer interactions, noting that none of the chosen HRA methods are deemed by their authors as appropriate for human-computer interaction modelling. The RP may need to conduct research into this area to address this shortfall and establish a method for assessing these interaction types.

4.2.4 Conclusions

134. Based on the outcome of my Step 2 assessment of HF Claims, I have concluded that:

- The RP has delivered sufficient confidence in the area of HF for Step 2 of GDA.
- The RP has been receptive to advice and guidance provided by ONR and taken this on board where appropriate.
- The RP has established a credible HFI framework with which to deliver the GDA.
- The RP has established a credible set of HF process claims, which I consider could be validated within GDA programme timescales.
- With some minor exceptions, the codes, methods and standards are appropriate for GB use and represent RGP.
- During Step 2, the ability of the RP to deliver right-first-time submission has suffered due to capability and resource gaps. The RP recognises this and has embarked upon a programme of up-skilling and resourcing to address this for Step 3.
- There are some minor issues that will require follow up during Step 3 and these are discussed in Section 4.1.4. The most important of these issues is a need to clearly articulate the safety role of the operator.

4.3 Human Factors Baseline

4.3.1 Assessment

135. The reference plant for the UK HPR1000 is FCG3. It is clear through regulatory interventions and submissions that the reference design has benefitted from HFI to some degree. However, at Step 2, I have been unable to establish a clear understanding of where and to what level, HF has been integrated into the reference design. It is important to understand this as it establishes the HF reference, and sets the context for future HF work. An important regulatory consideration is what level of confidence can be drawn from the original domestic design and analysis effort. This information is not present within the PSR. The RP has committed to performing this analysis during Step 3 of the GDA to establish an HF baseline.

136. Whilst this is a significant omission for GDA, it is of less importance for Step 2 due to a number of factors.

137. The FCG3 baseline design is currently in build and an evolution of the CPR1000, CPR1000+, and ACPR1000 designs. The FCG3 baseline design has been designed, taking into account international and domestic evolutionary OPEX; key to which are the

lessons learned from the Fukushima accident, which placed significant operational demands on the operator. These evolutionary advances are summarised within Chapter 2 of the PSR (Ref. 13). Those pertinent to my HF assessment include improvements to MCR habitability and the introduction of in-vessel retention capability to extend the operator grace times for emergency equipment preparation. The design also benefits from a development simulator which has been employed for user testing. Finally, it has already passed through the Chinese domestic regulatory process.

138. For a reactor design featuring high levels of novel and unproven technology the lack of HF baseline would have posed an unacceptable regulatory risk. However, as noted above, the HPR1000 is an evolutionary design that demonstrably takes account of lessons learned in international PWR development. I thus judge the lack of HF baseline at this stage to present a low regulatory risk with respect to identifying significant HF issues that cannot be addressed during Steps 3 and 4 of GDA.

139. Whilst this did not undermine my Step 2 assessment, it will be important for the RP to establish a clear reference position during Step 3. I will follow this matter up early in Step 3.

4.3.1 Strengths

140. The RP self-identifies this gap and has committed to address during Step 3.

4.3.2 Items that Require Follow-up

141. During my GDA Step 2 assessment of the Human Factors Baseline Design I have identified the following specific shortfalls:

- The RP has yet to establish an HF baseline for the FCG3. It will need to do this during Step 3.

4.3.3 Conclusions

142. Based on the outcome of my Step 2 assessment of the Human Factors Baseline, I have concluded that this is a significant shortfall against the expectations for Step 2. However, there are number of factors that sufficiently mitigate the significance of this shortfall. These comprise:

- The HPR1000 design is not a novel PWR design.
- It has demonstrably taken account of OPEX
- It benefits from a development simulator to test and demonstrate the design of the MCR interfaces.

4.4 Categorisation of Safety Functions and Classification of Structures, Systems and Components

4.4.1 Assessment

143. The classification of SSC is performed by engineering and fault analysis disciplines. HF does not typically play a role in this process. However, as discussed in an earlier section above, ONR SAP ECS.2 requires that HBSCs be classified in a manner similar to SSCs to ensure appropriate substantiation commensurate with their risk importance. This work was not performed for the FCG3 design, but it has been formally identified by the RP's fault studies team as a gap against GB regulatory requirements (Ref. 27). The RP has yet to submit its approach to classifying HBSCs, I consider this to be a minor shortfall which I am confident can be easily addressed during Step 3.

4.4.2 Strengths

144. The RP has identified the expectation that that HBSCs be classified similarly to SSCs is a gap within the baseline safety case. It has initiated a programme of work to develop a process of HBSC classification, which will be submitted in Step 3.

4.4.3 Items that Require Follow-up

145. During my GDA Step 2 assessment of HF I have identified the following specific shortfall:

- The RP currently has no mechanism for classifying HBSCs based on safety importance. I note that this is work in progress and will assess appropriately during Step 3.

4.4.4 Conclusions

146. Based on the outcome of my Step 2 assessment of the RPs classification of SSCs, I conclude that the RP has not classified the HBSCs by their risk importance for the baseline design. However, it has identified this as a gap against GB expectations and has committed to developing and applying a classification process. Given the RP has yet to starts its classification process; I am content that this gap is not significant.

4.5 ALARP Considerations

4.5.1 Assessment

147. The RP submitted its ALARP methodology (Ref. 28) late within Step 2 which has resulted in me not assessing it as part of my Step 2 assessment. Therefore, judgements against the adequacy of the ALARP arrangements have had to be made based on documentation submitted in the HF topic area.

148. My assessment of ALARP is thus solely focussed on its application with respect to reducing the risk of human error so far as is reasonably practicable. ALARP demonstrations should consider, first and foremost, factors relating to engineering, operations and the management of safety. These expectations are often referred to by the general term "relevant good practice". HSE define relevant good practice as "… those standards for controlling risk which have been judged and recognised by HSE as satisfying the law when applied to a particular relevant case in an appropriate manner." In nuclear safety applications, where the potential consequences of accidents can be very serious, the best practice identified as appropriate to the application would normally be required for new designs.

149. For new build designs, ONR expects the following (Ref. 5)

- There is a clear conclusion that there are no further reasonable practicable improvements that could be implemented, and therefore the risk has been reduced to ALARP.
- Relevant Good Practice: This is the basic requirement for demonstrating that designs meet the law. The Requesting Party (RP) must set out the standards and codes used and justify them to the extent that we can ‘deem’ them relevant good practice when viewed against our SAPs. This justification is expected to include a comparison with other international/ national standards. Clearly the standards and codes adopted by the RP must be shown to have been met.
- Options: This will comprise two stages: Firstly, an examination of the RP’s rationale for the evolution of the design, using its forerunners as a baseline, looking at why certain features were selected and others rejected and how this process has resulted in an improved design from a safety perspective.

Secondly, the RP needs to address the question “what more could be done?” and provide an argument of “why they can’t do it” (i.e. why it is not reasonably practicable). This second element could be done by postulating further options for improvement (previously discarded options may be suitable candidates) and evaluating them. Clearly if an option is shown to be reasonably practicable then that option should have been taken, or where it is found not to be excessively expensive to improve safety, then further avenues for risk reduction should be explored.

- Risk Assessment: The use of risk targets in isolation is not an acceptable means of demonstrating ALARP and we expect to see risk assessments used to identify potential engineering and/or operational improvements as well as confirming numerical levels of safety. The Basic Safety Objectives (BSO) in the SAPs represent broadly acceptable levels below which we have said that we expect to confine ourselves to considering the validity of the arguments that the BSOs have actually been met. We have also made it clear that the way in which we apply these numerical targets will depend heavily on the views we form on the engineering (and at a later stage, operational practices) and that meeting the BSOs is not a green light for RPs to forego further ALARP considerations. Nevertheless, well-supported numerical risk figures that show BSOs to be met can be an important element of support to the overall ALARP demonstration.

150. Of the four expectations, practically, only items 2 and the first part of 3 can be assessed during Step 2. However, it is possible to comment on the likelihood of the design process facilitating the achievement of requirement 1 based on the methods and standards assessed to date.

151. Two basic tenets of HFI are:

- A fit for purpose design process that critically analyses the design against standards and system performance requirements and improves the design where gaps against each are identified. I can confirm that the HFI design process (Ref. 14) should deliver against both these requirements as it combines clear verification and validation activities and the formal tracking and resolution of issues and management of assumptions.
- The identification and application of relevant good practice across all areas where human error could present a safety risk to the plant. I examined the RP’s submitted design guidance to date – noting that additional supplementary guidance will be delivered during Step 3 – and judged it to broadly meet RGP across all areas. I did the same for its analytical methods and again found broad alignment with RGP.

152. I have yet to assess evidence of the application of the RP’s risk assessment methods so cannot pass judgement against item 4 as they have not been formally trialled as yet. As discussed in earlier sections of this report I do consider that, on paper, they align with RGP. The initial application of the RP’s new risk assessment methods (HRA) was developed from advice and guidance provided by ONR and is being trialled in the interim period between the closure of Step 2 and the start of Step 3. I will assess the initial output from these methods early within Step 3.

4.5.2 Strengths

153. The RP's HF methods and standards, and its HFI process broadly align with RGP.

4.5.3 Items that Require Follow-up

154. During my GDA Step 2 assessment of ALARP I have identified the following to follow-up:

- Early within Step 3, the initial results of the RPs HRA methodology will be available for scrutiny. I plan to provide feedback on these early assessments to de-risk the bulk of the analysis being performed later during Step 3 and 4.

4.5.4 Conclusions

155. Whilst it is not possible to conclude at Step 2 that design reduces human error so far as is reasonably practicable, I can conclude that the necessary arrangements are in place to enable an ALARP position to be reached by the end of GDA.

4.6 Out of Scope Items

156. The following items have been left outside the scope of my GDA Step 2 assessment of the UK HPR1000 HF.

- Consideration of the adequacy of the UK HPR1000 design. The reason for leaving this matter out of the scope of my GDA Step 2 assessment is that the RP has provided insufficient design information to conduct a meaningful assessment within Step 2. I will assess the adequacy of the design from an HF perspective during Steps 3 and 4.
- Design for decommissioning. The reason for leaving this matter out of the scope of my GDA Step 2 assessment is that the RP has provided insufficient design information to conduct a meaningful assessment within Step 2. I will assess the adequacy of the design from an HF perspective during Steps 3 and 4.

157. It should be noted that the above omissions do not invalidate the conclusions from my GDA Step 2 assessment. During my GDA Step 3 assessment, I will follow-up the above out-of-scope items as appropriate; I will capture this within my GDA Step 3 Assessment Plan.

4.7 Comparison with Standards, Guidance and Relevant Good Practice

158. In Section 2.2, above, I have listed the standards and criteria I have used during my GDA Step 2 assessment of the UK HPR1000 HF, to judge the adequacy of the preliminary safety case. In this regard, my overall conclusions can be summarised as follows:

- SAPs: They key SAP for Step 2 in the area of HF is EHF.1 – Integration with design, assessment and management as this sets the basis for a successful GDA. Judged against this SAP, the RP has developed an approach which should ensure a systematic approach to HFI during the GDA. The SAPs associated with modelling and analysis, I also consider, have been largely met. However, whilst the RP has put systems in place that should ensure compliance with SAPs EHF.2 Allocation of safety actions, EHF.3 Identification of actions impacting safety, later during GDA, it is currently a shortfall.
- TAGs: The relevant TAGs for my assessment comprise: TAG-058 Human Factors Integration; TAG-062 Workplace and work environment; TAG-063 Human Reliability Assessment; TAG-064 Allocation of Function. As they guide

on the application of the SAPs, I judge that the RP has sufficiently met the guidance set out within these TAGs to complete Step 2 of the GDA. However, as discussed in section 4, further work is necessary in the area of HRA, the identification of HBSCs; and the process for allocating function between humans and technology.

4.8 Interactions with Other Regulators

159. I engaged in discussion with the Environment Agency (EA) at the end of Step 2 to ensure an efficient and consistent approach to the identification of HBSCs during Step 3. The purpose of this was to ensure that effort on the part of the RP to identify nuclear safety important human actions was not duplicated for the identification of environmentally important human actions.

160. I have had no interactions with any regulatory bodies outside of the UK.

5 CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

161. During Step 2 of GDA the RP submitted a PSR and other supporting references, which outline a preliminary nuclear safety case for the UK HPR1000. These documents have been formally assessed by ONR. The PSR, together with its supporting references, presents the process claims in the area of HF that underpin the safety of the UK HPR1000.

162. During Step 2 of GDA, I have targeted my assessment at the content of the PSR and its supporting references that is of most relevance to the area of HF; against the expectations of ONR's SAPs and TAGs and other guidance that ONR regards as RGP. From the UK HPR1000 assessment conducted so far, I conclude the following:

- The PSR, together with its supporting references, presents the process claims in the area of HF that underpin the safety of the UK HPR1000. I consider these claims to be largely valid and form a strong basis for a successful GDA.
- The safety case does not yet present the key HF safety functional claims underpinning the role of the operator in ensuring nuclear safety. Whilst this is a significant omission for Step 2, I am content that much of the information missing is available in Chinese; having been provided with visibility of a limited selection of translated HBSCs at the end of Step 2. I am also content that the necessary infrastructure and processes are in place to provide this detail within Step 3.
- Despite significant difference between the application of HF within the GB regulatory framework and that of China, the RP has made significant strides during Step 2 in understanding GB regulatory expectations. It has established a robust model of HFI, which should enable it to successfully deliver the GDA. The HFI process is adequately underpinned by a suite of HF process claims, which I consider to be credible. It has put in place measures to ensure that the normal organisational model of HF sitting within the C&I team will not be a barrier to widespread integration of HF across disciplines.
- The RP has quickly established links within the GB supply chain to gain the necessary understanding, along with developing a credible resource model, which will be needed to deliver the necessary HF analysis to support the GDA. It has embarked upon a programme of training for all HF and interfacing disciplines to facilitate the necessary understanding of GB expectations.
- The methods, codes and standards proposed generally meet RGP and establish a baseline for achieving a design where risks are ALARP.
- The FCG3 baseline design is currently in build and an evolution of the CPR1000, CPR1000+, and ACPR1000 designs. The FCG3 baseline design has been designed, taking into account international and domestic evolutionary operational experience; key to which are the lessons learned from the Fukushima accident, which placed significant operational demands on the operator. These evolutionary advances are summarised within Chapter 2 of the PSR (Ref. 13). Those pertinent to my HF assessment include improvements to MCR habitability and the introduction of in-vessel retention capability to extend the operator grace times for emergency equipment preparation. The design also benefits from a development simulator that has been employed for user testing. Finally, it has already passed through the Chinese domestic regulatory process. I thus consider the likelihood of inadvertently introducing a sufficiently significant HF issue during the evolutionary process – one that cannot be rectified during Steps 3 and 4 of GDA – to be acceptably low. It is thus unlikely that there are significant safety issues that exist in the HF domain that cannot be tolerated at Step 2.

- The Step 2 submissions fail to adequately articulate the role the operator plays in ensuring nuclear safety. A limited suite of HBSCs were presented at the end of Step 2 but I consider these insufficiently detailed and contextualised to provide the necessary assurance that the role of the operator has been optimised. This has hampered my understanding of the HPR1000 design as, for HF, the HBSCs are used to target the design assessment. The RP is aware of this shortfall in the safety case and towards the end of Step 2 secured the support of EDF's HF team to provide additional capability in this area. On this basis, and Level 4 discussions that established a shared understanding of what will be required, I consider this shortfall in the safety case recoverable within Step 3. It should also facilitate my better understanding of the HPR1000 design.
- The GB practice of HRA closely integrating the qualitative and quantitative elements is novel to the RP. The RP has significantly revised its HRA process to deliver HRA that will be acceptable to ONR. Despite significant improvements, there remains work to be done in this area. My PSA colleague and I are planning to conduct a joint intervention in this area early in Step 3.
- Whilst the RP has identified credible resource requirements for Step 3 and 4, the associated work programme lacks detail.
- The HFI focus for the FCG3 baseline design was on control rooms. This means that other risk important areas of the plant are unlikely to have benefitted from systematic HFI.
- The method of allocating function is basic and is unlikely to adequately address some of the complex subtleties of automation.
- Whilst I note that there are a number of shortfalls, these are relatively minor, mostly acknowledged by the RP and are relatively simple to address during Step 3. Balancing these shortfalls is the sound HFI process that the RP has developed and its willingness to expedite solutions to shortfalls as they are identified. The RP has made significant forward progress during Step 2 which it is to be commended for.

163. Overall, during my GDA Step 2 assessment, I have not identified any fundamental safety shortfalls in the area of HF that precludes proceeding to Step 3 and which might later prevent the issue of a DAC for the UK HPR1000 design.

5.2 Recommendations

164. My recommendations comprise:

- Recommendation 1: ONR should consider the findings of my assessment in deciding whether to proceed to Step 3 of GDA for the UK HPR1000.
- Recommendation 2: All the items identified in Step 2 as important to be followed up should be included in ONR's GDA Step 3 HF Assessment Plan for the UK HPR1000.
- Recommendation 3: All the relevant out-of-scope items identified in sub-section 4.2 of this report should be included in ONR's GDA Step 3 HF Assessment Plan for the UK HPR1000.

6 REFERENCES

1. *Generic Design Assessment of GNS's UK HPR1000 - Step 2 Assessment Plan for Human Factors* ONR-GDA-AP-17-007 Revision 1. ONR October 2017. TRIM Ref 2017/361560

2. *Preliminary Safety Report Chapter 15 Human Factors*, General Nuclear Systems Ltd, HPR/GDA/PSR/0015, October 2017

3. *ONR HOW2 Guide NS-PER-GD-014 Revision 6 - Purpose and Scope of Permissioning*. July 2014. http://www.onr.org.uk/operational/assessment/index.htm

4. *Safety Assessment Principles for Nuclear Facilities*. 2014 Edition Revision 0. November 2014. http://www.onr.org.uk/saps/saps2014.pdf

5. Technical Assessment Guides.

   - *Human Factors Integration* NS-TAST-GD-058 (Rev 3)
   - *Allocation of Function* (AoF NS-TAST-GD-064 (Rev. 3)) http://www.onr.org.uk/operational/tech_asst_guides/index.htm

6. IAEA guidance

   - *Safety of Nuclear Power Plants: Design. Safety Requirements*. International Atomic Energy Agency (IAEA). Safety Standards Series No. NS-R-1. IAEA. Vienna. 2000.
   - *Basic Safety Principles for Nuclear Power Plants*, 75-INSAG-3 Rev. 1, International Nuclear Safety Advisory Group, IAEA, Vienna (1999)
   - *Specific Safety Requirements: Safety of Nuclear Power Plants: Design*, International Atomic Energy Agency IAEA Safety Standards Series No. SSR-2/1 Rev 1, IAEA, Vienna 2016.
   - *Specific Safety Guide: Deterministic Safety Analysis for Nuclear Power Plants*, International Atomic Energy Agency IAEA Safety Standards Series No. SSG-2, IAEA, Vienna 2010.
   - *Specific Safety Guide: Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency IAEA Safety Standards Series No. SSG-39, IAEA, Vienna 2016
   - *Specific Safety Guide: Design of Instrumentation and Control Systems for Nuclear Power Plants*, International Atomic Energy Agency IAEA Safety Standards Series No. SSG-39, IAEA, Vienna 2016
   - *Development and Application of Level 1 Probabilistic Safety Analysis for Nuclear Power Plants*. Specific Safety Guide Safety Standards Series No SSG-3, International Atomic Energy Agency IAEA, Vienna (2010)
   - *Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plants*. Specific Safety Guide Safety Standards Series No. SSG-4-4, International Atomic Energy Agency IAEA, Vienna, (2010)
   - *Probabilistic safety assessments of nuclear power plants for low power and shutdown modes*, International Atomic Energy Agency IAEA-TECDOC-1144,
   - *Determining the quality of probabilistic safety assessment* (PSA) for applications in nuclear power plants, IAEATECDOC-1511, International Atomic Energy Agency IAEA, Vienna (2006)
   - *Safety of Nuclear Power Plants: Design Specific Safety Requirements*, Safety Standards Series SSR-2/1, International Atomic Energy Agency IAEA, Vienna (2012).
   - *Procedures for Conducting Probabilistic Safety Assessments of Nuclear Power Plants (Level 3)*, International Atomic Energy Agency IAEA-Safety Series 50-P-12, IAEA, Vienna (1996).

- *The role of automation and humans in nuclear power plants* - TecDoc 668. International Atomic Energy Agency IAEA, Vienna, 1992 ISSN 1011-4289

7. Western European Nuclear Regulators' Association.

- Safety Reference Levels for existing reactors WENRA September 2014, Reactor Harmonisation Working Group report on Safety of new NPP designs WENRA March 2013, http://www.wenra.org/

8. Health and Safety at Work (etc.) Act 1974

9. Other international standards used in my assessment:

- *Human-System Interface Design Review guidelines*, NUREG 0700, US Nuclear Regulatory Commission Revision 2, May 2002.
- *Basic Safety Principles for Nuclear Power Plants*, 75-INSAG-3 Rev. 1, International Nuclear Safety Advisory Group IAEA, Vienna (1999)

10. *Treatment of Important Human Actions Implementation Plan,* GH X 06001 015 DIKX 03 GN, General Nuclear Systems Ltd, July 2018

11. *Methodology of Human Reliability Analysis*, GH X 00650 030 DOZJ 02 GN, General Nuclear Systems Ltd, May 2018

12. *UK HPR1000 - Regulatory Query (RQ) Tracking Sheet*, ONR - 2 November 2017, TRIM 2017/407871

13. *Preliminary Safety Report – Chapter 2: General Plant Description*, HPR-GDA-PSR-0002, General Nuclear Systems Ltd, October 2017.

14. *Human Factors Integration Plan*, GH X 06001 016 DIKX 03 GN, General Nuclear Systems Ltd, April 2018.

15. *Function Allocation Methodology*, GH X 06001 019 DIKX 03 GN, General Nuclear Systems Ltd, April 2018

16. *HFE Design Guidelines for Control Room*, GH X 06001 021 DIKX 03 GN, General Nuclear Systems Ltd, April 2018

17. *Task Analysis Methodology*, GH X 06001 042 DIKX 03 GN, General Nuclear Systems Ltd, April 2018

18. *New Nuclear Reactors: Generic Design Assessment Guidance to Requesting Parties,* ONR-GDA-GD-001, ONR, Revision 3, September 2016

19. *HPR1000 CGN / GNS HF workshop – Shenzhen China*, ONR-NR-CR-17-680, Revision 0, ONR February 2018. TRIM 2018/6054575

20. BS EN 61839-2014 Nuclear power plants – Design of control rooms – Functional analysis and assignment, British Standards Institute.

21. *Human Factors Engineering Program Review Model*, NUREG-0711, Rev3, Nuclear Regulatory Commission.

22. *A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control,* NUREG/CR 3331, Nuclear Regulatory Commission,1983

23. *Accident Sequence Evaluation Program Human Reliability Analysis Procedure*, NUREG/CR-4772, Nuclear Regulatory Commission,1987.

24. *Handbook of human reliability analysis with Emphasis on Nuclear Power Plant Applications Final Report*, NUREG/CR-1278, Nuclear Regulatory Commission, 983.

25. The SPAR-H human reliability analysis method, NUREG/CR-6883, Nuclear Regulatory Commission, 2005.

26. *UKHPR1000 GDA – HPR1000 GNS/CGN Level 4 Human Factors Technical Meeting – 20th June 2018*, ONR-NR-CR-18-233, ONR, TRIM 2018/209859

27. *Methodology of Safety Categorisation and Classification*, GH X 00100 062 DOZJ 03 GN, General Nuclear Systems Ltd, 15 June 2018.

28. *ALARP Methodology*, GH X 00100 051 DOZJ 03 GN, General Nuclear Systems Ltd, May 2018.

Table 1

Relevant Safety Assessment Principles Considered During the Assessment

SAP No and Title	Description	Interpretation	Comment
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).	This principle ensures that sufficient 'thinking' time is permitted for the operators to plan any necessary response to a fault. It is a key driver for AoF decisions.	Addressed in Section 4 of this report. The RP claims in its safety case that HPR1000 design meets this principle.
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.	This principle ensures that assumptions regarding having sufficient time to respond to fault manually are formally substantiated within the safety case.	Addressed in Section 4 of this report. The RP's proposal for task analysis specifically considers the time available for responding to faults.
ESS.10 Definition of Capability	The capability of a safety system, and of each of its constituent sub-systems and components, should be defined and substantiated.	For HF this sets out the requirement to clearly define the role of the operator within the system.	Addressed in Section 4 of this report. The RP has not met this SAP. It has provided some very basic information on the role of operator, and some HBSCs (albeit without context). It is an area that will be followed up in Step 3.
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.	This principle sets the framework and requirements for ensuring that HF is systematically considered in the design and safety case assessment process at an early stage and continued throughout the entire design process and facility lifecycle. The intent of HF integration is to provide an organising framework for ensuring that all relevant HF issues are identified and addressed such that properly informed	Addressed in Section 4 of this report. The RP has largely met this SAP. It has provided an HFIP and commitments to ensure that HF is proportionally integrated into the facility design.

SAP No and Title	Description	Interpretation	Comment
		decisions on risk and design can be made. Soundly demonstrated HF integration can provide the basis for regulation of the HF aspects of a project and provide assurance to ONR inspectors that HF is being adequately accounted for.	
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.	This principle is about demonstrating an appropriately balanced AoF and its substantiation. This should take into human capabilities and limitations, what is appropriate for nuclear safety and what is technically feasible, whilst recognising the need to minimise reliance on human action to provide safety functions. It expects that an interdisciplinary approach to AoF and application of good practice methods are adopted for AoF analysis and making design decisions relating to this.	Addressed in Section 4 of this report. The RP has partially met this SAP. It has provided details of its methodology for allocating safety functions. I have found this method to be a sound starting position but requiring enhancements to improve its sensitivity. However, the RP has failed to provide sufficient description of the allocation between the human and the technology on the UK HPR1000 design.
EHF. 3 Identification of actions impacting Safety / **EHF.4 Identification of administrative controls**	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.	These principles have been combined as they relate to ensuring all human-based safety claims (HBSC) relevant to all plant states and conditions, including operator actions that implement administrative controls, are systematically identified in order that their feasibility, reliability and adequacy can be substantiated as part of the safety case.	Addressed in Section 4 of this report. The RP has partially met this SAP. It has provided details of its methodology for the identification of HBSCs. I have found this method to be generally sound but requiring some minor improvements prior to application. However, the RP has yet to apply this method and has only provided a limited selection of HBSCs drawn from the FCG3 safety case and submitted with little context.
EHF. 10 Human reliability analysis	Risk assessments should identify and analyse human actions or omissions that might impact on safety.	This principle is about demonstrating that a suitable and sufficient risk assessment and PSA is produced that incorporates all the ways in which risks can arise from human failures. It requires assurance that all Type A – C HFEs are identified and analysed, dependence mechanisms and failures are appropriately accounted for, that quantitative HEPs	Addressed in Section 4 of this report. The RP has submitted its approach for HRA, which includes both qualitative and quantitative analysis and broadly meets ONR expectations contained within this principle. Recognised HF and HRA quantification techniques will be used, along with

SAP No and Title	Description	Interpretation	Comment
		are derived using relevant and justified data and techniques and that this is underpinned by qualitative task analyses.	input from operational experience data as appropriate. Concerns have been raised with regards to HEP data for advanced HMI, although the RP is aware of the need to address this. At this stage I am confident that SAP EHF.10 will be met for the UK HPR1000.
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.	Addressed in Section 4 of this report. The RP has identified that the baseline FCG3 safety case does not currently classify HBSCs similarly to systems, structures and components as per SAP ECS.2. The RP has declared its intention to classify all HBSCs using a system similar to that used for its UK HPR1000 category and classification scheme. I am content that SAP ECS. 2 will be for the UK HPR1000.
SC.4 Safety Case Characteristics	A safety case should be accurate, objective and demonstrably complete for its intended purpose.	The principle essentially relates to ensuring that safety cases are fit-for-purpose for the life-cycle stage to which they relate, are suitably comprehensive, balanced, honest and provide the necessary information for the management of safety, the making of risk-informed decisions, and provide the demonstration that legal requirements have been met or how this will be achieved	The PSR chapter on HF and supporting documentation are judged to be unsatisfactory when compared against the expectations of this principle for an early HF safety case. The PSR is contains insufficient detail in a number of areas. However, the key shortcoming relates to the lack of information concerning the role the operator plays in ensuring nuclear safety. On this basis principle SC.4 is not considered to have been met for Step 2. To balance this and other shortcomings, the RP has committed to addressing them within the updated PCSR and Step 3 supporting documentation.