New Reactors Division

Step 4 Assessment of Human Factors for the UK Advanced Boiling Water Reactor

Assessment Report: ONR-NR-AR-17-023-UKABWR
Revision 0
August 2018

Published 07/18

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

Hitachi-GE Nuclear Energy Ltd is the designer and Generic Design Assessment (GDA) Requesting Party for the United Kingdom Advanced Boiling Water Reactor (UK ABWR). Hitachi-GE commenced GDA in 2013 and completed Step 4 in 2017.

This assessment report comprises my Step 4 assessment of the Hitachi-GE UK ABWR reactor design in the area of Human Factors (HF).

The scope of the Step 4 assessment is to review the safety, security and environmental aspects of the UK ABWR in greater detail, by examining the evidence, supporting the claims and arguments made in the safety documentation, building on the assessments already carried out for Step 3. In addition I have provided a judgement on the adequacy of the HF information contained within the Pre-Construction Safety Report (PCSR) and supporting documentation.

The early difficulties in securing HF resource to establish a credible Human Factors Integration (HFI) capability, and the maturity level of the UK variant of ABWR design, limited what was practicably achievable by Hitachi-GE during the GDA. Despite these constraints, I consider that Hitachi-GE did sufficient work in the HF area to support a meaningful GDA.

I am satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for HF. On this basis I consider that the UK ABWR is capable of being built and operated in GB on a site bounded by a generic site envelope, in a way that is acceptably safe and secure and thus support issuing a Design Acceptance Confirmation (DAC).

I consider that Hitachi-GE:

- Provided a PCSR and supporting references reflecting the design maturity at GDA, to demonstrate that the UK ABWR design is capable of being built and operated in Great Britain (GB), on a site bounded by a generic site envelope, in a way that is acceptably safe and secure. I expect that the development of the PCSR will continue as part of normal business post-GDA.

- Developed a clear initial claims and arguments structure in which it is possible to trace each Human Based Safety Claims (HBSCs) identified in the basis of safety case document, up through safety functional / property claims, into high level safety functions and fundamental safety functions. I expect that the identification and substantiation of HBSCs will continue as part of normal business post-GDA as the design matures and the additional scope items (that were outside the scope of GDA) are considered.

- Identified a comprehensive list of HBSCs, which are identified / modelled in both the fault schedule and Probabilistic Safety Analysis (PSA). The PSA considers pre-initiator, initiator, and post-fault errors and includes consideration of errors of omission and commission. It also appropriately models dependency. I expect that further identification and substantiation of HBSCs will be performed as part of normal business post-GDA as the design matures and the additional scope items of licensing and pre-operations are considered.

- Has applied its Human Reliability Assessment (HRA) method with suitable conservatism taking account the design maturity and assumptions associated with future licensee operation and arrangements. I expect that, post-GDA, the HRA approach will consider the need to account for the human interaction with a hybrid soft and hard interface design.

- Demonstrated that the risk contribution from the human is proportionate within what is considered practical for GDA. I expect that post-GDA; the risk contribution is reviewed in light of the maturing design and details becoming available relating to the operating regime.

- Provided sufficient evidence to substantiate that the HBSCs are credible within the limitations of GDA and without licensee input.
- Provided sufficient evidence demonstrating that the UK ABWR design submitted for GDA is balanced and minimises the risk from human error via the appropriate allocation of safety functions between technology and operators. The UK ABWR features high levels of automation. There are no plant intervention claims made on the operator within 30 mins of a fault occurring with automatic reactivity control and short term cooling. Other operator claims are typically simple responses to failed automatic safety system.
- Provided sufficient evidence to show that the Human Machine Interface (HMI) design is sufficiently mature for GDA, with sufficient contingency to mitigate the risk of foreclosing on future options as the design matures and the HMI becomes finalised.
- Identified a comprehensive set of domestic and international standards appropriate to inform the UK ABWR design.
- Identified an appropriate suite of tools and methods that meet GB regulatory expectations with respect to relevant good practice.
- Provided cogent evidence that these codes, standards, tools and methods were appropriately and proportionately applied.
- Developed a suitable process for capturing and sentencing HF engineering deficiencies.
- Developed a suitable process for capturing future operating and licensee arrangement assumptions.

My judgement is based upon the following:

- An assessment of the Human Factors Integration (HFI) process for design and safety analysis.
- An assessment of the applied codes, standards, and methods used during the GDA of the UK ABWR.
- A targeted assessment of HBSCs considering their completeness and the level of substantiation.
- A targeted assessment of the suite of evidence provided to underpin claims and arguments for the UK ABWR design.
- A targeted assessment of the design including the principal HMI and Allocation of Function (AoF) between the operator and the technology.
- A review of how Hitachi-GE consolidated its analysis together as part of, and in support of, a wider safety case for the UK ABWR.

I have identified no assessment findings. Where I have identified weaknesses in Hitachi-GE's submission, I am content that these weaknesses are captured by assessment findings within other Office for Nuclear Regulation (ONR) assessment reports or can be adequately addressed via normal business as the design progresses post-GDA. I expect that the submitted analysis will need to be reviewed and updated (assuming it is adopted by a future licensee) as the design evolves and details concerning out of scope items for GDA and the future operating regime become clear.

LIST OF ABBREVIATIONS

AC	Atmospheric Control
ADS	Automatic Depressurisation System
ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
ATWS	Anticipate Transients Without SCRAM
B/B	Backup Building
BBCP	Backup Building Control Panels
BBCR	Backup Building Control Room
BDBF	Beyond-Design Basis Faults
BS	British Standards
BSC	Basis of Safety Case
BWR	Boiling Water Reactor
C/B	Control Building
C&I	Control & Instrumentation
CCF	Common Cause Failure
CDF	Core Damage Frequency
CDM	Construction Design and Management Regulations
CESA	Commission Errors Search and Assessment
CIBSE	Charted Institution of Building Service Engineers
CRA - Synergy	Corporate Risk Associates - Synergy
CRD	Control Rod Drive
CST	Condensate Storage Tank
DAC	Design Acceptance Confirmation
DBF	Design Basis Faults
DC	Direct Current
DCD	Design Certification Document
DG	Diesel Generators
EA	Environment Agency
EDG	Emergency DG
EMIT	Examination Maintenance Inspection Testing
EOC	Errors of Commission
EOP	Emergency Operating Procedures
FAT	Factory Acceptance Test
FCVS	Filtered Containment Venting System
FHM	Fuel Handling Machine
FLSS	Flooding System of Specific Safety Facility,
FMEA	Failure Modes and Effects Analysis
FPGA	Field Programmable Gate Array
FPM	Fuel Preparation Machine

FSF	Fundamental Safety Function
GB	Great Britain
GDA	Generic Design Assessment
HAZOP	Hazard and Operability
HBSC	Human Based Safety Claims
HCI	Human-Computer Interfaces
HCITT	HCI Test Tool
HCU	Hydraulic Control Unit
HEA	Human Error Analysis
HEART	Human Error Assessment and Reduction Technique
HEP	Human Error Probability
HF	Human Factors
HFE	Human Failure Event
HFI	Human Factors Integration
HFIP	Human Factors Integration Plan/Programme
HFIR	Human Factors Issues Register
HFMP	HF Methodology Plan
HLSF	High Level Safety Functions
HLW	High Level Waste
HMI	Human Machine Interface
HNCW	HVAC Normal Cooling Water System,
HPCF	High Pressure Core Flooder System
HRA	Human Reliability Analysis
HRAR	Human Reliability Analysis Report
HSI	Human-System Interface
HVAC	Heating Ventilation and Air Conditioning System
HWBP	Hardwired Backup Panel
IAEA	International Atomic Energy Agency
IEAP	Internal Events at Power
IEF	Initiating Event Frequencies
ILW	Intermediate Level Waste
ISI	In-Service Inspection
ISV	Integrated System Validation
J-AWBR	Japanese Advanced Boiling Water Reactor
LOCA	Loss Of Coolant Accident
LPFL	Low Pressure Core Flooder System
MCC	Main Control Console
MCR	Main Control Room
MSQA	Management for Safety and Quality Assurance
NASA-TLX	National Aeronautics and Space Administration – Task Load Index

NB	Nuclear Boiler
NPP	Nuclear Power Plant
NRC	Nuclear Regulatory Commission
NRW	Natural Resources Wales
NSEDP	Nuclear Safety and Environmental Design Principle
ONR	Office for Nuclear Regulation
OPEX	Operational Experience
PCS	Plant Computer Systems
PCSR	Pre-Construction Safety Report
PCV	Primary Containment Vessel
PIF	Performance Influencing Factor
Pro-SWAT	Pro-Subjective Workload Analysis Tool
PSA	Probabilistic Safety Analysis
PWR	Pressurised Water Reactor
R/B	Reactor Building
RAW	Risk Achievement Worth
RBC	Reactor Building Crane
RCIC	Reactor Core Isolation Cooling System
RCW	Reactor Building Cooling Water System.
RGP	Regulatory Good Practice
RHR	Residual Heat Removal
RI	Regulatory Issue
RO	Regulatory Observation
RPV	Reactor Pressure Vessel
RSP	Remote Shutdown Panel
RSS	Remote Shutdown System
RSSR	Remote Shutdown System Room
RSW	Reactor Building Service Water System
Rw/B	Radioactive Waste Building
S/P	Suppression Pool
SA	Severe Accident
SACS	Safety Auxiliary Control System
SAuxP	Safety Auxiliary Panel
SAP	Safety Assessment Principle
SBO	Station Blackout
SFAIRP	So Far As Is Reasonably Practicable
SFC	Safety Functional Claim
SI	Structural Integrity
SLC	Standby Liquid Control System
SME	Subject Matter Expert

SPAR-H	Standardised Plant Analysis Risk Model – Human Reliability Analysis
SQEP	Suitably Qualified and Experienced Person
SPC	Safety Property Claims
SSC	Systems, Structures, and Components
SSLC	System Logic and Control System
SWF	Solid Waste Facility
SWMS	Solid Waste Management System
TAGs	Technical Assessment Guides
THERP	Technique for Human Error Rate Prediction
TRACEr	Technique for The Retrospective And Predictive Analysis Of Cognitive Error
TSC	Technical Support Contractor
TTA	Tabular Task Analysis
TR	Topic Reports
UK ABWR	United Kingdom Advanced Boiling Water Reactor
US	United States
V&V	Verification and Validation
WDP	Wide Display Panel

TABLE OF CONTENTS

Annexes

INTRODUCTION

1. This assessment report details my Step 4 Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR reactor design in the area of Human Factors.

GDA Background

2. Information on the GDA process is provided in a series of documents published on our website (**http://www.onr.org.uk/new-reactors/index.htm**). The expected outcome is a Design Acceptance Confirmation (DAC) from the Office for Nuclear Regulation (ONR) and a Statement of Design Acceptability (SoDA) from the Environment Agency (EA) and Natural Resources Wales (NRW).

3. The GDA Step 3 summary report is published on our website (**http://www.onr.org.uk/new-reactors/uk-abwr/reports/step3/uk-abwr-step-3-summary-report.pdf**).

4. The GDA of the United Kingdom Advanced Boiling Water Reactor (UK ABWR) has followed a step-wise approach in a claims-arguments-evidence hierarchy which commenced in 2013. Major technical interactions started in Step 2 with an examination of the main claims made by Hitachi-GE for the UK ABWR. In Step 3, the arguments which underpin those claims were examined. The reports in individual technical areas and accompanying summary reports are also published on ONR's website.

5. The objective of the Step 4 assessments is to undertake an in-depth assessment of the safety, security and environmental evidence. Through the review of information provided to ONR, the Step 4 process should confirm that Hitachi-GE:

   - Has properly justified the higher-level claims and arguments.
   - Has progressed the resolution of issues identified during Step 3.
   - Has provided sufficient detailed assessment to allow ONR to come to a judgment of whether a DAC can be issued.

6. The full range of items that might form part of the assessment is provided in ONR's 'GDA Guidance to Requesting Parties' (**http://www.onr.org.uk/new-reactors/ngn03.pdf**). These include:

   - consideration of issues identified in Step 3;
   - judging the design against the Safety Assessment Principles (SAPs) and whether the proposed design reduces risks to As Low As Is Reasonably Practicable (ALARP);
   - reviewing details of the Hitachi-GE design controls, procurement and quality control arrangements to secure compliance with the design intent;
   - establishing whether the system performance, safety classification, and reliability requirements are substantiated by the detailed engineering design;
   - assessing arrangements for ensuring and assuring that safety claims and assumptions are realised in the final as-built design; and
   - resolution of identified nuclear safety and security issues, or identifying paths for resolution.

7. All of the Regulatory Issues (RIs) and Regulatory Observations (ROs) issued to Hitachi-GE during Steps 2 to 4 are also published on ONR's website, together with the corresponding Hitachi-GE resolution plan.

8. During the step 4 Human Factors (HF) assessment I have undertaken a detailed assessment, on a sampling basis, of the HF safety case evidence.

Scope

9. The intended strategy for assessing HFs in GDA Step 4 was set out in the HF assessment plan (Ref. 1).

10. The scope of this assessment is broad as dictated by the scope of the HF discipline. Unlike some disciplines, it plays a key role in both design engineering and safety analysis. I have looked at the following areas to varying degrees of scrutiny:

- The HF capability embedded within Hitachi-GE and the supporting supply chain.
- The analytical HF methods deployed in support of the deterministic and probabilistic analysis.
- The suitability of the codes, standards, and HF methods used in support of the design engineering programme.
- Whether the principal claims on the human-technology performance have been identified and adequately demonstrated for GDA.
- Whether the risk from Human Failure Events (HFEs) has been shown to be reduced so far as is reasonably practicable for GDA.
- Whether the design appropriately and proportionately considers HF throughout.

11. The level of scrutiny within this scope was informed partly by risk importance and partly by the availability of both design detail and the availability of the HF safety case submissions which were delivered late in Step 4. It is important to note that design and safety case maturity need only be sufficient to provide confidence to ONR and the EA that no significant safety, environmental or security issues have been identified that cannot be resolved post-GDA.

12. Thus the emphasis has been on confirming that:

- Hitachi-GE has identified comprehensive set of normal and fault Human Based Safety Claims (HBSCs) for the UK ABWR.
- The numerical risk contribution from human error is neither disproportionate nor overly optimistic.
- The basic Allocation of Function (AoF) between the human and the technology on the design is adequate; thus de-risking major AoF design changes outside of GDA
- The codes, standards, and methods chosen meet Regulatory Good Practice (RGP) and have been applied proportionally and correctly.
- The primary Human Machine Interfaces (HMI) (e.g. Main Control Room) are sufficiently developed to mitigate future design change risks. Hitachi-GE recognised within Step 4 that the detailed design will be performed post-GDA. It also acknowledged that further substantiation of HBSCs will be required post-GDA where they feature human-machine interaction using one of the plant HMIs.
- Residual issues and assumptions relating to a future operating organisation are being managed in a manner suitable for future resolution / validation.
- The UK ABWR design is capable of being built and operated in Great Britain (GB), on a site bounded by a generic site envelope, in a way that is acceptably safe and secure.

13. Due to the following factors, I chose to exclude the full assessment of Examination Maintenance Inspection Testing (EMIT) HBSCs substantiation from my assessment.

- Hitachi-GE note that its HF review of error potential during maintenance was limited in scope due to known differences between the Japanese Advanced Boiling Water Reactor (J-ABWR) and UK ABWR design. It commits to a

forward programme of work in this area. I consider it essential for a future licensee to adopt this commitment.

- Maintenance regimes are within the scope of a licensee organisation, as are the methods and training associated with individual EMIT activities.

- The design of Systems, Structures, and Components (SSC) is ongoing and the detail needed to fully substantiate an EMIT task was not available for GDA.

14. The contribution of EMIT HBSCs was considered at a probabilistic level and an AoF level, as was the HF guidance underpinning the design of SSC.

15. My assessment report also excludes the specific consideration of areas where I have not been the lead assessor. Nevertheless, I have worked with other assessors to ensure that account was taken of HF issues within in their assessments. These areas include:

- Radiological Protection relating to spent fuel pool fault environments and evacuation times, (Ref. 2)
- Decommissioning (Ref. 3)
- Mechanical handling on the fuel route (Ref 3)
- HF in the inspection of structural integrity (Ref. 4)
- Evacuations, notably for Loss Of Coolant Accidents (LOCAs) during outages and fuel handling accidents (Ref. 5)

16. The above areas are also subject to the general Human Factors Integration (HFI) programme, so where HBSCs have been identified as being performed in these areas, they will have been subject to the HF design standards and principles that I have assessed. I can confirm that there is evidence of HFI in each of these areas (Ref. 6).

17. I also note that whilst I have not specifically assessed severe accident response, I have looked at several claims made within Hitachi-GE's human reliability analysis and the substantiation of these actions is reasonable in both time available versus time taken and the task complexity. However, given that neither the equipment nor the severe accident management strategy has been defined for GDA, and this is an area that will require considerable licensee input, I did not pursue this further.

Method

18. This assessment has been undertaken consistent with internal guidance on the mechanics of assessment within ONR (Ref. 7).

ASSESSMENT STRATEGY

Standards and criteria

19. The SAPs (Ref. 8) constitute the regulatory principles against which duty holders' safety cases are judged, and, therefore, are the basis for ONR's nuclear safety assessments, including the assessment detailed in this report. The SAPs are supplemented by Technical Assessment Guides (TAGs), which provide additional advice to ONR inspectors on assessing safety case submissions.

20. International guidance documents are also available which capture long-established RGP for reactor design basis analysis.

21. Further details are provided in sub-sections below.

Safety Assessment Principles

22. The following SAPs have been at the forefront of the HF assessment described in this assessment report:

- Engineering Human Factors EHF 1, 2, 3, 4, 5, 6, 7 and 10.
- Engineering Key Principles EKP 3, 4, and 5
- Engineering Layout ELO 1
- Engineering Safety Systems ESS 3, 8, 9, and 13
- Engineering Control & Instrumentation of safety related systems ESR 1and 3

23. Based on experience, these SAPs were identified at the start of GDA Step 4 in the Assessment Plan (Ref. 1) and have informed both the interactions with Hitachi-GE during the step and this record of my assessment presented in this report.

Technical Assessment Guides

24. TAGs provide additional guidance to ONR inspectors on the interpretation application of the SAPs. The following TAGS have informed this HF assessment of Hitachi-GE submissions.

- NS-TAST-GD-005 Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable) (Ref. 9)
- NS-TAST-GD-030 Probabilistic Safety Analysis (Ref. 10)
- NS-TAST-GD-058 Human Factors Integration (Ref. 11)
- NS-TAST-GD-059 Human-System Interface (Ref. 12)
- NS-TAST-GD-062 Workplaces and Work Environment (Ref. 13)
- NS-TAST-GD-063 Human Reliability Analysis (Ref. 14)
- NS-TAST-GD-064 Allocation of Function between Human and Engineered Systems (Ref. 15)

National and international standards and guidance

25. There are International Atomic Energy Agency (IAEA) standards (Ref. 16) which are relevant to the HF assessment of the UK ABWR.

- SSR-2/1 - Safety of Nuclear Power Plant: Design Specific Requirements.
- SSG-2 - Deterministic Safety Analysis for Nuclear Power Plant Specific Safety Guide
- SSG-3 - Development and Application of Level 1 Probabilistic Safety Analysis for Nuclear Power Plant Specific Safety Guide
- SSG-4 - Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plant Specific Safety Guide
- NS-G-1.3 - Instrumentation and Control Systems Important to Safety in Nuclear Power Plants
- NS-G-2.15 - Severe Accident Management Programmes for Nuclear Power Plants

26. Whilst these standards are not HF specific, they have informed my assessment when considering HF in the wider context. My assessment is based primarily upon the SAPs and supporting TAGs.

Use of Technical Support Contractors

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

28. To supplement ONR's internal capability, one contract was placed with Corporate Risk Associates - Synergy (CRA - Synergy) for HF specialists to provide a detailed and independent assessment of Hitachi-GE's qualitative HBSC and quantitative Human Error Probability (HEP) analysis.

29. I sought an independent view on the adequacy and credibility of the substantiation of HBSC. I also requested the generation of independent HEPs using a GB method to establish whether the Hitachi-GE assessments took sufficient account of the relevant qualitative factors and suitably interpreted these in quantitative terms.

30. The final deliverable provided by CRA-Synergy was used to inform my judgements. However, it is important to note that the regulatory judgements reported in this assessment are my own; informed by CRA-Synergy HF technical assessments where indicated.

Integration with other assessment topics

31. GDA requires the submission of an adequate, coherent and holistic generic safety case. Regulatory assessment cannot therefore be carried out in isolation as many aspects of a safety case are cross-cutting in nature. The nature of HF is that it interfaces with almost every topic, however, the following areas are particularly notable.

32. Close cooperation is required between HF and the Probabilistic Safety Assessment (PSA) topic areas. Estimations of the probability of human failure form an integral part of PSA risk models. Therefore, it is necessary for HF to understand the technical context, as described by the PSA models, for the claims being made upon the human. The proper incorporation of human failures within PSA models requires a clear understanding of the dependence between discrete human failure events. Therefore, it has been necessary for me to scrutinise the Hitachi-GE HF analyses of human dependence and provide assurance to my PSA colleagues that suitable treatment of dependence/independence has been undertaken. Further, it is necessary for the PSA assessment to have assurance that probabilistic estimates of human failure are sufficiently accurate for incorporation within the PSA models.

33. The majority of HBSC involves claims on humans interacting with designed control and display user interfaces. These interfaces are predominantly implemented using electrical, electronic or programmable technologies. Therefore, close cooperation has been required with the Control and Instrumentation (C&I) topic area. Areas of common concern have included the availability, category and classification of fall-back user interfaces to be used when instrumentation or plant faults occur, the design and development of a Class 1 computer-based user interface and the requirements, functions and capabilities of alarm systems in the Main Control Room (MCR) and elsewhere.

34. A concern in radiological protection is that a convincing demonstration would need to be provided of the time required, with consequential dose, for personnel to evacuate an area when an unplanned radiological exposure occurs. A convincing demonstration requires the careful task analysis of exposure detection, evacuation decision-making, route selection, route negotiation et cetera to arrive at realistic time estimates. Accordingly I have collaborated with the radiological protection area in the scrutiny of such evacuation claims.

35. The decommissioning of nuclear power plant requires application of different processes equipment and tasks. Accordingly I have collaborated with the assessor covering decommissioning in order to assist in understanding the Hitachi-GE substantiation of decommissioning tasks.

36. I have collaborated with the assessment of the fuel route. In particular, I have supported the Mechanical Engineering assessment of mechanical handling on the operating deck and the Fault Studies assessment of evacuation.

Out of scope items

37. ONR requires sufficient design maturity to enable it to complete the GDA process meaningfully. However, given that the GDA process is undertaken at an early stage and that it only considers the generic design, there are a range of other important aspects of the development of the design and safety case that will need to be addressed before a plant can be constructed and operated. These are accepted by ONR as necessarily falling outside of the scope of GDA.

38. For example, significant evidence and associated confirmatory analysis to support the safety case cannot be gathered until the SSCs have undergone final detailed design by a manufacturer / supplier, or have been manufactured and are in the process of being tested or commissioned. ONR recognises that this is unavoidable.

39. The generic nature of the design considered during the GDA process, and the need for further detailed design and other considerations to be made by the potential operator (as above), means that detailed consideration of the following aspects of the design are out-with the scope of GDA:

- detailed equipment and plan specification;
- aspects of materials specification;
- operational resourcing levels;
- operating technical specifications;
- maintenance schedule;
- procedures (normal operation, emergency, waste management, accident management);
- training programmes;
- emergency preparedness arrangements;
- operating limits;
- radiation protection arrangements for operators;
- plant lifetime records;
- commissioning requirements and records;

40. Specific scope considerations relevant to this this assessment are discussed below:

- Hitachi-GE elected to significantly change the primary HMIs and underlying technology (e.g. main control room) part way through the GDA process. This meant that the design information available, whilst sufficient to reach a judgement on the whether the design could be built, was not sufficient to fully substantiate claims on the operator using these HMIs. I expect a future licensee to continue to develop the design and verification and validation regime to provide this substantiation.

- The level of design detail provided on SSCs was sufficient to provide confidence that the associated HBSCs had been captured and were understood. However, there was insufficient detail to provide confidence that the reliability of the HBSCs had been optimised in relation to the SSC design. Again, I expect a future licensee to continue to develop the design and verification and validation regime to provide evidence that risk-important SSCs have been designed to optimise human reliability.

- The PSA/HRA, whilst appropriate for GDA in that it was sufficient to consider the design against UK risk targets, will require updating post-GDA to reflect the final design and operating regime.Requesting Party's SAFETY CASE

Safety Case Documentation and Structure

41. Hitachi-GE identified the generic PCSR as the key submission within GDA that substantiates the top level claim that the "UK ABWR constructed on a generic site within the United Kingdom, can be operated safely under all operating and fault conditions." (Ref. 17).

42. The PCSR also states that one of the key objectives of the HFI programme was to identify and substantiate any human actions required to achieve the UK ABWR Fundamental Safety Function (FSF).

43. The PCSR has 32 chapters. The following three chapters are most relevant to ONR's HF assessment:

- Chapter 21: Human-Machine Interface (Ref. 18)
- Chapter 27: Human Factors (Ref. 17)
- Chapter 30: Operation (Ref. 19)

44. While the PCSR is clearly a vital and fundamental part of the UK ABWR safety case, it only provides a summary of supporting safety analysis documents. Underpinning the PCSR (and referenced from it) are a large number of basis of safety case documents, topic reports and underpinning analysis reports. It is these references (and supporting references from these reports) that have been the main areas for my assessment during GDA Step 4, and provide the technical basis for majority of the regulatory judgements presented within this report.

45. The key Hitachi-GE HFI references for the UK ABWR design are shown in Figure 1 below.

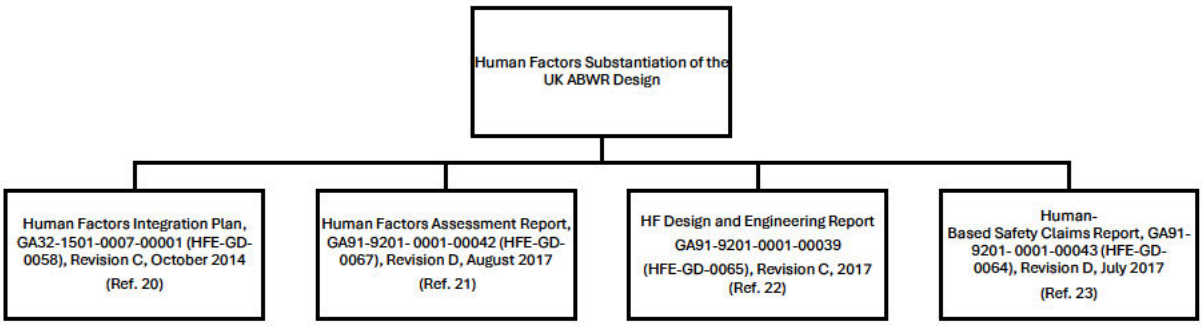

Figure 1

46. The HFI Plan (Ref. 20) is intended to provide confidence that the tools, methods, codes and standards used to integrate HF into the design meets RGP.

47. The Human Factors Assessment Report (Ref. 21) summarises the analysis conducted to substantiate the UK-AWBR design.

48. The HF Design and Engineering Report (Ref. 22) summarises the design assessment activities carried out on the J-ABWR design as well as those conducted to inform the UK AWBR design.

49. The HBSC report (Ref. 23) summarises the substantiation of operator actions that are important for nuclear safety.

50. The following additional reports have been central to ONR's assessment to inform my judgements on the efficacy of Hitachi-GE's HFI process:

- The Baseline HF Assessment Report (Ref. 24), along with the HF Methodology Plan (HFMP) (Ref. 25), describe the HF previously integrated into the J-ABWR reference design. They also describe the programme of HF support that was integrated into the UK ABWR design. Hitachi-GE claims that these demonstrate that suitable and sufficient consideration has been given to HF principles within the design and safety analysis in accordance with RGP.

- The Requirements Compliance Tracking Matrix (Ref. 26) and the Human Factors Issues Register (HFIR) report (Ref. 27). Hitachi-GE claims that these demonstrate that HF requirements that derive from standards and good practice guidance, and the emergent task-based requirements specific to the UK ABWR system, have been met. Where requirements are not met ALARP justification is provided.

- The HF Verification and Validation Plan (Ref. 28) and all the resulting verification and validation (V&V) output, as captured in the HF V&V Report (Ref. 29). Hitachi-GE claims that these provide the demonstration that the assumptions made within the analysis are valid and the recommendations made for the design have been implemented.

- The ALARP Report (Ref. 30) which documents the ALARP justification as it stands at the end of GDA.

51. Many other reports have been referenced by Hitachi-GE and submitted to ONR in the course of GDA Step 4. These have been referenced as appropriate in Section 4 of this assessment report.

Safety Case Submissions Addressing Regulatory Observations

52. During Steps 2, 3, and 4 of the HF GDA assessment of the UK ABWR, ONR raised 4 ROs to ensure that significant gaps in the HFI process and safety case were closed by Hitachi-GE. These are described in full in Annex 1. The ROs comprised:

- RO-ABWR-0005 – Hitachi-GE Nuclear Energy Ltd. Human Factors Specialist Resource and Organisation.
- RO-ABWR-0024 – Human Reliability Analysis – Errors of Commission / Misdiagnosis.
- RO-ABWR-0033 Human Factors Baseline Assessment.
- RO-ABWR-0069 Human Machine Interface: Strategy, Application and Cognitive Issues

53. RO-ABWR-0005 was closed due to a significant increase in Suitably Qualified and Experienced Person (SQEP) resource within Hitachi-GE and its supply chain.

54. Hitachi-GE submitted the following submission to address the requirements of RO-ABWR-0024:

- Error of Commission Analysis Report, Rev. B, HGNE GA91-9201-0003-00815. (Ref. 31)

55. This submission was judged sufficient to close this RO. The accompanying closure statement can be found in Reference 32.

56. Hitachi-GE submitted the following submissions to address the requirements of RO-ABWR-0033:

- Human Reliability Analysis Report (Ref. 33)
- Human Factors Engineering Specification (Ref. 34)
- Allocation of Function Report (Ref. 35)
- Human Factors Methodology (Ref. 36)
  Human Based Safety Claims Report (Ref. 37)

57. RO-ABWR-0033 was closed on the basis that the UK AWBR had departed further from the original J-AWBR than originally claimed so there was less reliance on the J-ABWR substantiation. These submissions also informed my decision to close this RO. The accompanying closure statement can be found in Reference 38.

58. Hitachi-GE submitted the following submissions to address the requirements of RO-ABWR-0069:

- Strategy of Use for HMIs (Ref. 39)
- Cognitive Workload Analysis Report (Ref. 40)
- UK ABWR Alarm Processing and Presentation Strategy (Ref. 41)
- Human Factors Concept of Operations Report (Ref. 42)
- HCI-Induced Cognitive Error Analysis Report (Ref. 43)
- Human Reliability Analysis Report (Ref. 44)
- Alarm Basic Design Specification (Ref. 45)
- Alarm Design Rationalisation and Justification Report (Ref. 46)

59. These submissions provided sufficient supplementary evidence to close RO-ABWR-0069. The accompanying closure statement can be found in Reference 47.

60. To conclude, I am satisfied that all HF related ROs were satisfactorily addressed by Hitachi-GE by the provision of a significant body of additional evidence. This body evidence was also instrumental in my Step 4 assessment as discussed throughout Section 4.

Key Design Features of the UK ABWR

61. The primary means by which plant personnel interact with the UK-AWBR is via multiple Human-Machine Interfaces (HMIs) (Ref. 18). These include the following features and interfaces:

- There are no operator plant intervention actions claimed within the MCR for a period of 30 minutes following any reactor initiating event.

- Reactivity control and short term cooling at the start of a fault transient is assumed to be automatic.

- Manual actions required for long term cooling are simple and comprise:

  - Manual start of Residual Heat Removal (RHR) in Suppression Pool (S/P) cooling mode (assumed to manual in the analysis but proposed to be automatic in the final design

  - Manual switch of RHR back to Low Pressure Core Flooder System (LPFL) mode
  - Depressurisation of the Reactor Pressure Vessel (RPV) by opening 2 SRVs
  - Switch from LPFL mode to RHR shutdown cooling mode
  - Venting of the primary containment during Station Blackout (SBO) events or as a diverse means to the long term cooling methods above.

- Hitachi-GE has performed sensitivity analysis looking at these activities (e.g. late starting or terminating, opening too many valves, etc.). This sensitivity analysis was assessed by fault studies and was judged to be adequate with the conclusion that there is tolerance in the system as to when and how the HBSCs are performed.

- Main Control Room: The MCR is primary control and monitoring location. The main HMIs installed in the MCR are: the Main Control Console (MCC); the Wide Display Panel (WDP); the Safety Auxiliary Panel (SAuxP); and the Hardwired Backup Panel (HWBP).

- Remote Shutdown System Room (RSSR): There are two RSSRs each controlling a separate division. These are segregated but adjacent to each other in the Reactor Building (R/B). The RSSRs are physically separated from the MCR in the Control Building (C/B) and located in different hazard compartment to the MCR. In the event that the MCR becomes uninhabitable, operators will evacuate to a normally unmanned RSSR along an access route. Operators can initiate, monitor and maintain safe shutdown of the reactor from either RSSR. Each RSSR is equipped with a Remote Shutdown Panel (RSP), providing the functionality to bring the plant from a hot shutdown state into a cold shutdown state.

- Backup Building (B/B) Control Room (BBCR): The normally unmanned BBCR is the location for monitoring and operation during certain fault conditions, in particular Severe Accident (SA) conditions, if the MCR and RSSRs have lost required functionality and/or when it is necessary for personnel to evacuate the C/B and R/B. The HMIs installed in the BBCR are the Backup Building Control Panels (BBCPs).

- Radioactive Waste Building (Rw/B) MCR: The C&I and HMIs related to processing of Radioactive Waste (Radwaste) are required to perform the functions related to nuclear and environmental safety. The HMIs in the Rw/B MCR are used to monitor and control the C&I systems and plant associated with the management of Liquid Waste and some parts of the Solid Waste management process. Some information and alarms associated with them are replicated through the HMIs in the MCR.

- Local Control Locations: There are a number of Mechanical and Electrical Engineering systems and equipment in the UK ABWR design that perform nuclear safety functions but which have embedded C&I controlled through local HMIs, i.e., systems not controlled from the MCR through the main C&I (Ref. 48). These systems with local HMIs include:

  - HVAC Emergency Cooling Water System (HECW)
  - Radioactive Waste Management- parts of the Solid Waste Management System (SWMS) in the Solid Waste Facility (SWF) Building, Intermediate Level Waste and High Level Waste (ILW & HLW) Stores

- Fuel Storage and Handling- Fuel Route equipment such as the Fuel Handling and Fuel Preparation Machines (FHM & FPM) and Reactor Building Crane (RBC).

62. The notable feature of the UK ABWR design is the removal of operator actions for reactivity control and short term cooling at the start of a fault transient.

Safety Case Approaches and Principles

63. Hitachi-GE's general approaches and principles for developing its safety case are summarised in Chapter 4 of the PCSR (Ref. 49) and defined in its Safety Case Development Manual (Ref. 50). They are applied throughout the PCSR and safety case documentation, including the HF-relevant reports identified in Section 3.1 above.

64. Hitachi-GE claims that through the application of the framework set out in Chapter 4, and the three supporting references, it has produced a safety case that meets GB expectations for a modern nuclear power plant (i.e. consistent with the expectations set in ONR's SAPs and international guidance).

65. The identification and substantiation of HBSCs flows from the Fundamental Safety Functions, through High Level Safety Functions into basis of safety case and analysis documents where individual HBSCs are identified. HBSCs are also listed within both the PSA (Levels 1, 2 and 3) and the Fault Schedule.

66. The PSA shows there is a comparatively low risk contribution from human error during fault recovery, providing confidence in the basic concept design. Conversely, the automation that underpins this does then necessitate reliable EMIT, highlighting the importance of a good HFI and HBSC identification process to minimise human error in this area. I discuss this in greater detail in section 4.

ONR STEP 4 ASSESSMENT

Introduction

67. This section presents my assessment of the UK-AWBR HF submission as described in section 3 of this report. I have split the assessment as follows into the following logical themes.

- In Section *4.2 Human Factors Integration*, I have assessed the adequacy of the factors needed to ensure that HF is adequately integrated into the design. Within this section I consider: the capability of the resource deployed, the adequacy of the HFI scope, and the methods to analyse and substantiate the design.

- In Section *4.3 Identification and Substantiation of Human Based Safety Claims – Qualitative Human Reliability Analysis*, I discuss the qualitative GDA HF safety case. I have considered the output from the methods used to screen and substantiate those human actions important for safety.

- In section *4.4 Quantitative Human Reliability Assessment*, I discuss the quantitative GDA HF safety case. I have assessed a sample of the output from the application of Hitachi-GE's Human Reliability Analysis method. Within this section I consider whether the analysis is suitably best-estimate. I also consider the human contribution to risk.

- In section *4.5 Design of Human Machine Interfaces*, I have assessed the adequacy of the design of the primary HMIs.

- In section *4.6 Generic Human Factors Engineering*, I have assessed those factors that have widespread effect on human performance, e.g. environmental factors and design for maintainability.

- In section *4.7 Concept of Operations*, I have assessed the adequacy of the command and control philosophy, staffing concept, work organisation and concept of use for the UK ABWR.

- In section *4.8 ALARP*, I have assessed whether Hitachi-GE has been able to construct a cogent and coherent case that the UK ABWR is ALARP with respect to HF.

68. I have considered the adequacy of the PCSR implicitly throughout my assessment of the totality of Hitachi-GE submissions.

Human Factors Integration

Introduction

69. The consideration of HF in design is essential in ensuring nuclear safety. A plant designed in absence of HF consideration is likely to be subject to significantly greater human errors during the operation; with a correspondingly higher risk of accidents.

70. Consequently, ONR pays particular attention to ensuring that HF design principles are integrated into the design and that HF safety analysis methods have been used to provide insight into the risk contribution from human error.

71. A key way in which ONR assures itself that a requesting party has adequately integrated HF into its design and safety analysis programmes, is by checking for the existence of, and testing the efficacy of, the requesting party's HFI programme.

72. HFI is a good practice approach to the application of HF to systems development. As a methodology it provides an organising framework to help ensure that all relevant HF issues are identified and addressed. In addition, the HFI approach has a management strategy that aims for timely and appropriate integration of HF activities throughout the project (Ref. 11).

73. Key to the delivery of effective HFI is the following:

- Sufficient SQEP resources.
- A scope of sufficient breadth to ensure that all areas of the facility, which are important for nuclear safety, receive HF input.
- A scope which includes suitable and sufficient input to the safety analysis areas.
- An effective management process.
- The appropriate use of RGP, codes, standards, and methods.

74. The following sections describe my assessment of the factors that are characteristic of an effective HFI programme.

HF Team

75. To support adequate HFI into a complex socio-technical system design, such as a nuclear power plant, there are four key enablers relating to the HF team. These comprise (Ref. 51):

- Sufficient numbers of SQEP personnel,
- A level of qualification and experience commensurate with the role,
- A suitable level of embedding into the wider project team,
- A suitable level of authority comparable with other engineering disciplines to ensure a balance between HF and other technical considerations.

76. An effective HF team provides both design and safety analysis input. For example:

- Design role:
  - Defining appropriate codes, standards and methods,
  - Developing internal project design guidance,
  - Providing direct design input into SSC that are important for nuclear safety,
  - Conducting operability testing and validation of SSCs that are important for nuclear safety,
  - Managing issues and assumptions for sentencing and future transmission to a licensee.
- Safety analysis role:
  - Identification of all HBSCs,
  - Providing appropriate substantiation of all HBSCs,
  - The assessment of HBSCs to identify human error – in support of the PSA and deterministic analysis,
  - The calculation of human error probabilities.

77. My assessment was limited to the team that Hitachi-GE assembled for the purpose of GDA to support the design and safety analysis activities of the UK ABWR.

78. In 2014, ONR raised RO-ABWR-0005 identifying concerns over a lack of HF Subject Matter Experts (SMEs) then working on the UK ABWR project. It flagged up the project risk of failing to deliver the HF programme of work on time.

79. Hitachi-GE has to be commended for responding positively to this RO, which saw the HF project resource peak at ~ 50 HF personnel split between the UK and Japan. This

level of resource was necessary to address the significant changes in the baseline design from the J-ABWR to the UK ABWR, which substantially increased the originally planned HF work scope. I note that the slow build-up of resource addressing the changes between the J-ABWR and UK ABWR designs did impact upon Hitachi-GE's delivery schedule meaning that critical evidence was supplied late in GDA. I do not consider this to have significantly constrained my judgements.

80. However, I note the importance of a future licensee quickly establishing a suitable and sufficient HF team to perform the necessary follow on work as the project transitions out of GDA. ONR will pay particular attention to the suitability and sufficiency of resource post-GDA.

81. To ensure suitable competency for HF personnel on GDA, Hitachi-GE defined (Ref. 20) three levels of HF SQEP: HF expert, HF specialist and HF-related technical specialist:

82. HF experts were required to have a broader and more extensive background and experience than the HF specialists. Hitachi-GE required experts to have:

- Experience in the nuclear or high hazard industries,
- Experience in meeting UK HF requirements,
- Experience in the development and execution HFI programmes.

83. HF specialists were required to have:

- A bachelor degree in ergonomics, engineering or related science,
- Or, a Bachelor's degree in psychology,
- Or a Master's degree in ergonomics or HF,
- Or four years' experience applying HF principles and concepts usually within high hazard industries.
- The requirement to have experience in high hazard industries is deemed dependent on the specific role within the team.

84. The HF technical specialists were required to have:

- A Bachelor's degree in ergonomics, engineering or related science,
- Four years' experience applying HF principles and concepts usually within high hazard industries.
- The last requirement was deemed dependent on the specific role within the team.

85. I did not examine the academic qualifications of each member of the HF team, nor did Hitachi-GE make these available. However, I am able to comment on competency based on the quality of submissions and via interactions with Hitachi-GE HF personnel during Level 4 meetings during GDA. I am content that the HF personnel deployed on this project were suitably SQEP.

86. With respect to integration and the necessary authority to effect change, I consider that Hitachi-GE put in place reasonably practicable measures to ensure that HF was sufficiently represented in the design process and thus adequately integrated. This judgement is based on the following.

87. The leadership roles of the HF team were established early in GDA Step 3 and remained in place thereafter. The team was led by a British based HF subject matter expert and a Japan-based HF subject matter expert. Both have qualifications in psychology and extensive experience in HF design input and HF design analysis of nuclear power plants. I observed their experience reflected by their ability to

understand the scope and purpose of planned HF activities and by the manner in which they responded to my queries and challenges about the HF work programme.

88. I consider a well-balanced HF programme of work was formulated by the leads. The programme delivered proportionate effort through a risk-informed approach and had suitable coverage to address HF issues that arose. They also developed and managed effective mechanisms for integrating HF inputs and insights into the engineering design and safety analysis processes. Based on the outcomes of this work I consider the HF leads were competent to have managed the HF work programme.

89. Submissions from Hitachi-GE provided evidence that the work programme was effective in integrating HF within both the design and safety analysis areas. For example, HBSCs were specifically identified in the fault schedule, basis of safety case documents and topic reports.

90. I note that Hitachi-GE embedded personnel for the HF specialist roles based upon the consideration of necessary expertise for that role. In instances where specialised knowledge of HF guidance or human error phenomena were required, personnel qualified in HF were selected. In other cases (such as the Hitachi-GE V&V activity), greater onus was placed upon operational expertise in order to formulate suitable assessment scenarios. In such instances, personnel with operational expertise were selected for the role. In some instances, such as the development of Class 1 HMI, an individual was selected with both control and instrumentation as well as formal HF training.

91. To conclude, I am content that Hitachi-GE developed a suitable and sufficient SQEP HF project team for GDA. I consider that this team was suitably tasked and appropriately managed in order to provide:

- HF analytical insights to underpin the wider safety analysis
- Well-informed inputs to the design.

Scope of HFI programme

92. A key enabler for an effective HFI programme is the systematic identification of the interfaces between the human and the technology. In order to proportionately allocate appropriate resource, these interfaces need to be considered in the context of the ability of the human-technology system to cause harm, i.e. a risk based approach.

93. The scope of the Hitachi-GE HFI programme has considered the following (Ref. 20):

- Any HBSCs and HF issues, related to the entire plant, that are within scope for GDA.
- All operating modes.
- All relevant safety case topic areas.
- Process and personnel nuclear safety.
- The environment.
- Plant and site security.

94. Hitachi-GE also applied a screening process to ensure the proportional allocation of HF resource to those areas which pose the biggest risk to nuclear safety. The results of this planning exercise are reproduced below (Ref. 20).

Table 1 – Scope of HF Integration

No.	Topic Area	Potential HF Interface/Impact
1	Management for Safety and Quality Assurance (MSQA)	Medium interface: HF verification and technical quality of deliverables, plus consideration of human in development of organisational arrangements such as management systems.
2	Electrical Engineering	Medium interface regarding electrical safety rules (see also conventional safety) & accessibility/installation of cabling/power especially during installation & decommissioning.
3	C&I	Fully integrated topic: Main focus of HF is to support design of the MCR/local panel HMIs; an area of continuously integrated working.
4	Probabilistic Safety Analysis & Fault Studies	Fully integrated topic: human-related claims (implied and explicit) in safety studies need SQEP HF analysis and/or review. There are multiple chapters that contain elements of HF as well.
5	Fuel and Core Design	Medium interface surrounding fuel handling and refuelling tasks. Use of automated core loading software and design of core components for ease of independent verification following reloading require particular consideration.
6	Security	Some interface: Security systems and arrangements make implied claims on human response/action and also have human-system interfaces that require support/assessment.
7	Conventional Safety/ Fire Safety	Medium interface: HF includes the consideration of human capabilities within design for reduction of conventional health & safety risk (in addition to nuclear safety and process risk reduction). Also, fire safety strategy often makes implied claims on human action for alarm response, fire-fighting, successful evacuation within time periods etc. Wayfinding (human cognitive capability in directional & plant layout mental model) & panic response impact evacuation arrangements.
8	Turbine Island	Medium interface relating to plant layout and accessibility/ maintainability/ constructability.
9	Project	HFI programme must be completely linked to project overall schedule and milestones to demonstrate that HF was applied early and at the right time for the related design activity.
10	Generic Site Envelope & External Hazards	Medium interface: response to external hazards has HF element.
11	Internal Hazards	Medium interface: Internal hazards (dropped load, leaks, etc.) can relate to human errors and claims (i.e. human failure events during EMIT, administrative controls).
12	Civil Engineering	Some interface: structural integrity often relies on inspection which has an implicit human-related claim. Also, Construction (Design and Management) Regulations (CDM) and constructability are part of HF scope.
13	Mechanical Engineering	Some interface: as above regarding inspection and EMIT reliability and other claims. Particularly valves, pumps, etc. equipment accessibility, maintainability, and cranes/nuclear lifting.
14	Structural Integrity	See civil engineering above.
15	Reactor Chemistry	Some interface: surveillance & testing reliance on human actions.
16	Radiological Protection	Medium interface: administrative arrangements and plant design for reducing and monitoring dose uptake must include

No.	Topic Area	Potential HF Interface/Impact
		consideration of human capabilities. Managing dose during planned EMIT.
17	Decommissioning	Some interface: consideration of HF in decommissioning and interim storage facilities necessary during design stage. HF issues arising in current UK decommissioning were captured by HF Subject Matter Expert (SME); HF considerations for stores contained within Nuclear Decommissioning Authority (NDA) industry guidance document.
18	Rad-waste	Medium interface: design of fuel handling & rad-waste plant and systems must include consideration of HF as per operating plant design.
19	General Environmental Permit	As above for security & internal hazards, interface to support design/assessment of human-related environmental protection claims.

95. HF concerns itself with the how people interact with technology and the environment and is thus extremely wide ranging in scope. I welcome that Hitachi-GE recognised the cross-cutting nature of the topic and identified a comprehensive list of technical areas where HF support was necessary. I consider that the prioritisation work done appears to have come up with a sensible set of risk-based priorities. HBSCs were also comprehensively identified within the fault schedule and within the level 1, 2 and 3 PSAs, which informed where HF effort should be focussed (see section 4.3 for full discussion).

96. Over the course of Step 4, I observed evidence, either via Level 4 meetings or via submissions, that Hitachi-GE had actively deployed its resource in each of these areas.

97. Examples of integration include (Ref. 30):

- *"Improvements to the Allocation of Function: examples include implementing automation for functions where human capability was challenged such as Standby Liquid Control System (SLC) initiation, RHR, Suppression Pool cooling mode switching, Fuel Handling Machine operation (full automation and semi automation dependent on mode of operation), as well as automation support (i.e. sequential automation) of manually-initiated functions such as certain RHR modes, etc.*

- *Developments to the Fuel Route design including aspects such as Reactor Building Crane attachment modifications to reduce error potential, as documented in the Topic Report on Lifting Attachment.*

- *Improvements to the strategy for alarm presentation within the MCR, particularly the rationalisation and suppression of certain alarms in certain plant modes or states in order to ensure effective alarm processing, as per the Alarm Processing and Presentation Design Strategy Report.*

- *Improvements throughout the plant to plant layout and plant equipment design such that they comply with UK and international modern standards for consideration of human capabilities and limitations within the design (i.e. physical dimensions for access and clearance, working environment, etc.). A key example is the design of the Hydraulic Control Unit (HCU) where the accumulator has been raised to facilitate checking during refilling tasks that form part of the reactor pressure boundary."*

98. To conclude, I am satisfied that the scope of the Hitachi-GE HFI programme for GDA meets RGP. I consider it supports the development of a design to minimise the risk from human error. The scope is comprehensive, and the HF resource available appears to have been deployed with pragmatism, based on:

- Where the greatest risk to nuclear safety lies.
- Gaining the biggest insight into the human contribution to nuclear safety, thus potentially influencing the design for the better.

99. I consider that a similarly comprehensive scope, recognising the additional scope items necessary for licensing and permissioning hold points, will be necessary for the development of the UK AWBR beyond GDA.

Methods

MANAGEMENT OF ISSUES AND ASSUMPTIONS

100. On any complex socio-technical project, a Human Factors Issues and assumptions Register (HFIR) is necessary to manage the emergent issues and deficiencies across the scope of the design. It plays a key role in recording, sentencing, and resolution by providing an auditable trail for QA purposes.

101. ONR expects no different for GDA; it is expected that a requesting party will establish an effective management tool for capturing, sentencing and (where reasonably practical) resolving HF deficiencies for the scope of GDA.

102. ONR also expects that assumptions about future operation or licensee arrangements are captured for later validation by a future licensee as the information becomes available.

103. It will be necessary for a future licensee to either adopt the same HFIR process used for GDA or develop one of equivalent functionality to manage issues / deficiencies identified as the design progresses post-GDA.

104. It will also be necessary for a future licensee to establish a programme to either validate the assumptions made during GDA, or provide updates to the safety analysis reflecting the implications of assumptions which have proven to be invalid.

105. For their effective resolution, HF deficiencies often require consideration by a number of disciplines. Therefore, it is necessary to:

- Identify HF issues when they arise,
- Make a recommendation for its resolution,
- Record the method by which they can be resolved,
- Record the individual or team with prime responsibility for its resolution,
- Provide an auditable record to show if, when and how the issue has been satisfactorily resolved.

106. Hitachi-GE recognised the importance of managing HF issues as they arose on the UK ABWR project and set-up an HFIR as part of its HFI process.

107. Hitachi-GE provided ONR with regular updates on the status and output of the HFIR during Level 4 progress meetings.

108. My assessment is based upon the Human Factors Issues Register (Ref. 52), which is a snap-shot of the HFIR as of January 2016, and my experience of Hitachi-GE feedback at progress meetings. Hitachi-GE transferred the HFIR to a proprietary AIRIS database in Step 3, when the AIRIS database was first created. The HFIR was maintained in an integrated fashion with the other design and analysis issue registers.

I also considered whether this had any implications for my assessment. I examined all of the tabulated entries in the last formal issue of the HFIR.

109. Each issue was uniquely identified and was clearly described. The early issues recorded outcomes from the Baseline HF Assessment (Ref. 24) and therefore these were broad in nature. As the list matured, so the issues became more specific in character. I am satisfied that HF issues were clearly and adequately described when they arose.

110. Each issue had a recommended form of resolution and an associated risk rating if the matter was not resolved during GDA.

111. Both the proposer of the action and the owner of the action were recorded together with an expected closure date and current status.

112. This content was sufficient to provide an auditable trail through to resolution so met my expectations. I consider the HFIR provided a satisfactory mechanism for recording HF issues and generating a proposed pathway to their resolution for GDA.

113. In order to assess progress with the resolution of issues, I requested regular updates at Level 4 progress meetings. Hitachi-GE provided presentations showing the level of closure to date and forward projections for future closure. Hitachi-GE also presented and discussed a sample of HF issues to illustrate how they were recorded and resolved. This occurred during L4 progress meetings in February 2017 (Ref. 82) and April 2017 (Ref. 83). As GDA Step 4 progressed, I observed a steady reduction in the number of outstanding issues.

114. I was pleased to note that, notwithstanding the impending end of GDA Step 4, Hitachi-GE was willing both to add new issues to the register and to reopen ones where new information had emerged that in-validated the previous closure decision. This provided clear evidence that Hitachi-GE was using the HFIR in a proper fashion.

115. Hitachi-GE transferred the HF issues from the HF-only register to the proprietary AIRIS® database. I examined a printout from the AIRIS® database (Ref. 53) and compared it with the structure and content of the HFIR. I noted that AIRIS® column headings remained the same as those of the HFIR. Therefore, I did not see much likelihood of transcription errors or omissions being entailed through the transfer process.

116. I was assured by Hitachi-GE that issues open at the end of GDA would not be consolidated simply to reduce their numbers. I consider this appropriate because the HF issues I have examined appear to be set at a level of description that consistently matches the generality or specificity of their application to UK ABWR.

117. To conclude, I consider that the HF issues register has captured issues at a suitable level of detail and that Hitachi-GE has demonstrated suitable sentencing and resolution of issues.

HF DESIGN PROCESS

118. ONR expects that HF is adequately and systematically integrated into all lifecycle phases of the design and safety assurance of a Nuclear Power Plant (NPP); this is the key intent of SAP EHF.1 (Ref. 8) which requires that:

119. "*A systematic approach to integrating HF within the design, assessment and management of systems should be applied throughout the facility's life-cycle.*"

120. To meet this SAP, a requesting party must demonstrate that it has a robust design process in place that takes account of HF modern standards and good practices. Such a process should:

- integrate HF into all areas of the design,
- take account of all stakeholder positions,
- clearly specify HF requirements,
- provide a robust iterative process for the resolution of HF issues identified during the evolution of the design.

121. Figure 2 shows Hitachi-GE's Design and Engineering Process for the UK ABWR.

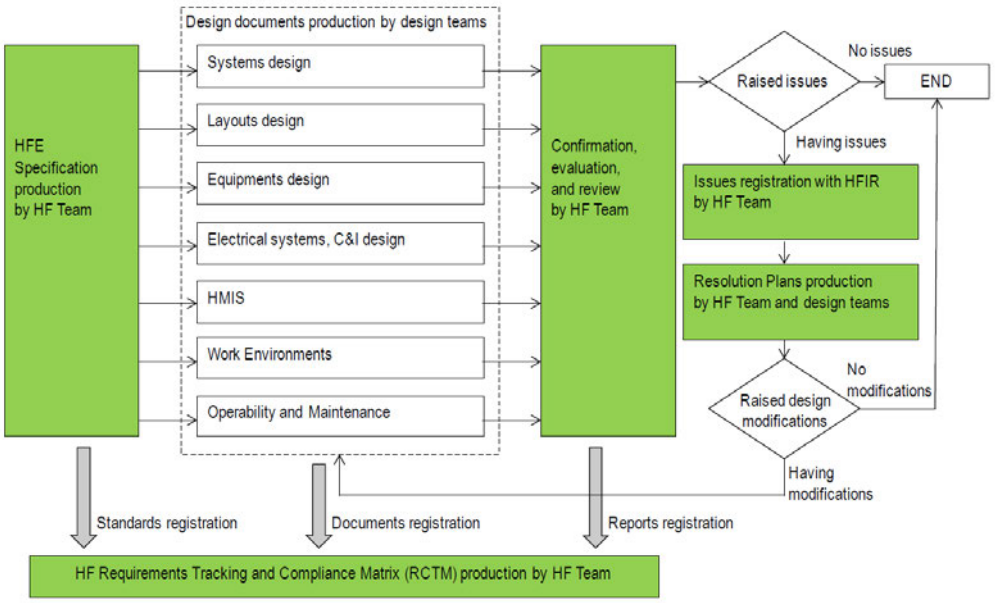

Figure 2 - Hitachi-GE Design and Engineering Process for the UK ABWR.

122. This process has, sensibly, been specifically designed to target those areas where J-ABWR is not suitable for the British operational context. This targeting has been achieved by means of the gap analysis contained in Baseline Human Factors Assessment Report (Ref. 24). To support the design programme, the HF engineering specification (Ref. 34), which provides the UK ABWR technical HF specifications for the following areas, was developed:

- Access and Egress
- Work Postures and Positions
- Equipment Layout for Operability and Maintenance
- Electrical, Control & Instrumentation (EC&I) Equipment Installation
- Main Control Room and Supplementary Control Points
- Displays and Controls (Non-Control Room)
- Alarms
- Digital System Design
- Materials Handling
- Labelling and Signage
- Working Environment

123. The HF engineering specification (Ref. 34) has been continuously updated based on engineer / designer feedback and at the end of my assessment stood at revision D.

124. The application of the HF engineering design process was enhanced by two HF led training sessions. These sessions were aimed at design and engineering teams working on the UK ABWR to provide a basic level of HF awareness and support to the application of the HF engineering design process. The first session focussed on HF principles and fundamentals and the second focussed on the implementation of the HF engineering specification (Ref. 34). This was aimed at the HF-responsible engineers from each UK ABWR design team.

125. Hitachi-GE expanded upon its HF engineering design process and guidance over the course of Step 4. At the end of step 3, ONR concluded that the HF engineering design process had suitable depth and breadth.

126. I can conclude that the progress made in this area is adequate for the closure of GDA. It constitutes one of several Hitachi-GE mechanisms for ensuring that human error during human-technology interactions is reduced so far is reasonably practicable.

127. My judgement is based on the fact that the process meets ONRs expectations in that it is being demonstrably applied to all the areas where risk-important human interactions may occur with technology and is delivering results. I have seen evidence of this first hand during an HF inspection of Hitachi in Japan (Ref. 54). During this inspection I was shown how the UK ABWR design has been modified over the Japanese design to provide additional work-space for UK operators and the relocation of local plant controls to facilitate better access.

128. The application of the Hitachi-GE HF engineering design process is discussed throughout sections 4.3 to 4.7

DESIGN GUIDANCE, CODES AND STANDARDS

129. The use of recognised guidance, codes and standards (RGP) is a key element in demonstrating that the risk associated with operating the design has been reduced so far as is reasonably practical; a requirement of UK Law. In some cases, ALARP can be judged on the basis that it can be demonstrated that RGP has been followed - highlighting the importance of guidance, codes and standards followed.

130. It was established at Step 2 and confirmed in Step 3 that Hitachi-GE had developed (Human Factors Engineering Specification, Ref. 34) a comprehensive listing of relevant and current HF and HF-related modern standards and guides. Hitachi-GE has iterated this listing throughout the GDA.

131. Given that ONR's Step 2 and Step 3 GDA assessments concluded the guidance, codes, and standards encapsulated in Hitachi-GE's Human Factors Engineering Specification was appropriate, I have chosen not to revisit this part of the assessment. I consider such an exercise would be disproportionate and for little benefit. I note only that the revisions enhance the scope of the guidance.

132. The scope of the guidance, comprised the following, adequately meets my expectations :

- Access / Egress
- Work Postures and Positions
- Equipment Layout for Operability and Maintenance
- Electrical, Control & Instrumentation Equipment Installation
- Main Control Room and Supplementary Control Points
- Displays and Controls (Non-Control Room)
- Alarms
- Digital System Design
- Materials Handling

- Labelling and Signage
- Working Environment

133. I discuss the application of guidance in later sections of this report.

DESIGN BASIS ANALYSIS METHODS

134. This section is confined to describing the adequacy of the qualitative HF analysis methods used to identify and analyse HBSCs. The application of these methods is discussed in later sections. It discusses:

- Operating Experience Review,
- Allocation of Function Methodology,
- Task and Error Analysis approach,
- The analysis of Type-A (Pre-initiator) errors,
- The analysis of Type B (Operator) errors,
- The analysis of Type C (Post-Fault) errors,
- The analysis of errors of commission / misdiagnosis,
- The analysis of cognitive errors in the control room,
- The analysis of cognitive workload.

135. Probabilistic methods are discussed in Section 4.4.

Operating Experience Review

136. ONR expects that, where reasonably practicable to do so, Operational Experience (OPEX) be taken account of to inform both the design and risk modelling (Ref. 51).

137. The ABWR reactor design has existed in various forms since the late 1990s. It is also an evolution from earlier Boiling Water Reactor (BWR) designs so considerable OPEX does exist. Early in the GDA process, ONR raised a RO-ABWR-0033/RO-ABWR-0045 concerning the failure of Hitachi-GE to adequately demonstrate that it had taken account of OPEX in design and risk modelling.

138. Subsequent to these ROs being raised, Hitachi-GE has addressed this and these ROs have been closed (Ref. 55). I have therefore kept this section brief.

139. During Step 3, ONR commissioned two reports investigating Operational Experience Feedback for BWR NPP in Europe and the United States (US) (Refs. 56 & 57). The two reports (developed by separate TSCs) considered the nature of events and issues arising on BWR plants to inform ONR's regulatory knowledge on the fundamental technology. In doing so, this recognised the lack of a BWR NPP within the UK at this time. The two ONR commissioned reports were passed to Hitachi-GE for consideration under a wider OPEX related programme of review (including OPEX from Japanese BWR).

140. In response to cross cutting RO (RO-ABWR-0045), Hitachi-GE produced an OPEX report which reviewed all OPEX. The HF specific elements of this review are contained within Reference 24. The review considered operational data from the US, Japanese and European BWR experience, along with other major nuclear events (Three Mile Island, Chūetsu Offshore Earthquake, Chernobyl, and Fukushima).

141. Hitachi-GE enhanced this OPEX review by performing some simulator analysis of the J-ABWR MCR design (Ref. 24). The review comprised the testing of scenarios containing HBSCs taken from the J-ABWR along HBSCs of interest for the UK ABWR. The scenarios spanned, normal operations, design basis accidents, and 'severely faulted conditions'. The results were used to inform the design and provide confidence in the HF safety analysis.

142. The review identified design change recommendations that had come out of the major events and showed that the UK ABWR design had incorporated these features.

143. Many of the findings collated related to the importance of safety culture, which, whilst important, is a consideration for a future licensee.

144. More useful was the identification of human error related events that have occurred on European and American BWR plant designs. The majority of the events identified relate to maintenance and testing errors (Type A). Hitachi-GE took these data and used it to underpin its assessment of Type A errors using the Standardised Plant Analysis Risk Model – Human Reliability Analysis (SPAR-H); particularly in relation to identifying appropriate performance shaping factors to apply to the base human error probabilities. I consider this is an appropriate approach.

145. One apparent omission I noted was the failure to translate these data into Initiating Event Frequencies (IEF). This does not affect my overall conclusions regarding GDA as I have confirmed that the HEP data used in the PSA appear suitably conservative (see section 4.3). A similar observation on the wider use of OPEX to inform IEF was raised in the Fault Studies assessment. An Assessment Finding (AF-ABWR-FS-03) was raised, which I consider bounds my expectation that: a future licensee should review the human error related OPEX data to determine appropriate IEFs / HEPs. This is considered RGP and an effective method of providing additional confidence in the HRA method generated HEPs.

Allocation of Function

146. Allocation of Function (AoF) is the process by which functions and responsibilities are assigned to either the human or the technology within a complex socio-technical system. In the context of nuclear safety case, the functions of concern are those that support nuclear safety.

147. ONR expects that safety should be secured primarily via engineered safeguards (SAP EKP.5). Where it is not reasonably practicable to engineer passive or automatically initiated active systems, it may be appropriate to use manually activated systems or rely on administrative controls to secure safety. The AoF process directly informs this human-technology split. Substantiation of this human-technology selection is expected (SAP EHF.2). ONR Safety Assessment Principal ERL. 3 sets an expectation that the dependence on human action to maintain a safe state should be minimised when rapid or reliable action is required. Safety Assessment Principal ESS. 8 expands upon this principle by setting the expectation that a safety system implementing a protective action should be automatically initiated and, normally, requiring no human intervention. ESS. 9 sets the criterion for rapid action by stating that no human intervention should be necessary for approximately 30 minutes following the start of a requirement for protective action.

148. The Hitachi process for performing AoF analysis is presented in Allocation of Function Report (Ref. 58).

149. The Hitachi-GE scope of analysis for GDA comprised those systems important to safety and any safety-related functions within all other systems. This included safety important human actions as identified by the deterministic safety case or the PSA. Thus the analysis consider the full range of SSCs for GDA, for example, reactor systems, fuel route, turbine building. The full scope of the review can be found in Reference 58.

150. I consider this to be a proportionate approach. It is derived from the US Nuclear Regulatory Commission (NRC) and IAEA guidance, which I consider suitable source material and RGP (Refs. 59 & 60).

151. The AoF process considers:

- time available,
- reliance on fault recovery in short timescales
- level of information processing,
- complex or repetitive operations,
- required level of human – machine reliability,
- task completion in a hostile environment,
- decision-making demands,
- concurrent task demands.

152. Each of these factors is considered in turn and a score given reflecting the potential level of challenge for human performance/reliability. All scores are combined to give an indication of the overall level of likely challenge to human performance. Feedback from Japanese ABWR operators has also been considered.

153. At the close of Step 3, the HF assessment report concluded that the Hitachi-GE process for AoF "*…broadly aligns with RGP [and] has been applied by Hitachi-GE to progress the design from the J-ABWR to the UK ABWR…this process has the capacity to positively influence AoF in favour of HF related criteria. However, it remains that this process may not always lead to reconsideration of AoF decisions across and between systems and therefore the implementation of such AoF decisions within the detailed design process will be an area for further consideration at GDA Step 4."*

154. Thus in the interest of proportionality and pragmatism, I elected to not revisit the method in my Step 4 assessment, but focussed my regulatory effort on testing the output of Hitachi-GE's AoF process to determine whether it delivered logically sound AoF determinations.

155. In the interest of clarity, and to preserve the scope of this section to assessing Hitachi-GE's general HF methods, I discuss the application of the AoF method and its role in substantiating the design in section 4.3.

Verification and Validation Methodology

156. ONR TAG 058 Human Factors Integration guides that: "*An appropriate validation and verification programme should be sought for the HF elements of the project that aligns with general validation and verification activity on the project. The activity should be appropriate to the scope and safety significance of HF to the project. Activities may range from verification against standards and good practice, and draw upon the output of any design reviews, to functional validation involving drawing walk-throughs, the use of mock-ups or simulators and the testing of HF aspects during wider project activities such as during a Factory Acceptance Test (FAT).*"

157. Integrated System Validation (ISV) trials are used to test and validate all of the HFI elements (training, procedures, human-technology interfaces, environment, staffing levels, etc.) that in concert make up a human-systems interface. Their purpose is to test how each of these elements interact together and to either validate the system performance or identify limitations in any of the HFI elements. They are an effective error analysis tool as they can and do show up adverse complex interactions leading to poor system performance beyond the imagination of the analyst.

158. A modern standard validation trial is characterised by a number of features, which I have considered during my assessment. These comprise:

- The scope of the scenarios chosen to test the HMI design is representative of the range of events that could be encountered during the plant's life-time. For example, includes all plant modes, and a range of bounding fault conditions.

- The fidelity of the HMI is such that it accurately presents all the HMI displays and controls.
- The physical environment is representative of the final design.
- The trial participants are representative of the user-population and are appropriately SQEP.
- Procedures, sufficiently representative of the final design, are available and followed.

159. The lack of design maturity of the key HMI designs on the UK ABWR for GDA meant that it was not possible to conduct formal ISV or V&V trials for the HMI design. This has meant that scope of testing has been at the operability level to inform the design rather than validation of final design performance. The testing has been confined to using low fidelity representations of the HMI; either non-interactive layout mock-ups or discrete control and display studies.

160. I do not consider this unduly detrimental to the findings of my assessment as it is important to consider the purpose of GDA: to provide confidence that that no significant safety, environmental or security issues have been identified that cannot be resolved.

161. Thus in this context, they key aim of trials is to ensure that the basic layout is correct, as is the basic technological solution. The detailed HMI design can develop post-GDA, although this does increase project risk as a finalised control room is a critical path item in an NPP design.

162. Informed by my level 4 interactions, discussing how testing was performed (Refs. 61 and 62), I am able to conclude that whilst I can only consider the trials as operability trials, and not formal validation trials, what was done was suitably informative with respect to demonstrating that a suitable and sufficient design could be achieved. This judgement is based on the following:

- Each trial is recorded using multiple video sources: two static cameras, and operator head-cameras,
- Following the completion of each scenario, the MCR crew are formally de-briefed using a structured interview / questionnaire,
- Successive trials involving HMI have represented the Hitachi-GE design intent for that HMI and, where engineering designs have been updated in the interim, subsequent trials have taken the benefit of HF recommended design changes stemming from earlier validation trials on MCR design has followed a logical and progressive process. This started with trials looking at the placement of HMI on workstations, to ascertain whether tasks involving multiple interfaces could progress in smooth sequences or whether undue task interruption occurred through to post fault scenario-based trials following J-ABWR procedures in order to demonstrate the support of combined workstation and HMI designs for operations in more challenging scenarios.
- I have observed that recommendations have been made for design improvement stemming from these trials. Examples include:
  - the optimal placement of new HMI required for UK ABWR in the MCR layout;
  - changes in the layout of controls and displays to improve overall visual clarity and functional associations between controls and displays;
  - The transfer or duplication of individual controls and or displays between different places in the control room layout to minimise the need to transfer between work surfaces.
- The ‘V&V’ trials considered the following scenarios:
  - Start-up and shut-down; surveillance tasks and post-fault recovery using step by step and ‘flowchart’ emergency operating procedures (EOP); with and without automatic sequences

- Tasks requiring access to and operations at the SAuxP and HWBPs including:
    - Reactivity Control
    - Water Level Recovery
    - Emergency Depressurization
    - Anticipate Transients Without SCRAM (ATWS)
    - SBO
    - Venting
- Some scenarios also assumed loss of digital systems
- Preliminary validation of functional HBSCs categorised as 'A' and 'B' - step by step and EOP-based exercising all HMIs within the MCR
- Specific exercise of tasks requiring the use of the RSPs

163. I consider that the process that Hitachi-GE has developed meets RGP in terms of method. However, there remains a significant amount of work to be progressed post-GDA with respect to the full verification and validation of the interfaces and equipment supporting reliable HBSCs. I also note the limitation of what was tested; there are other risk-important interfaces that could prejudice nuclear safety, e.g. fuel route equipment and remote shutdown interfaces which were not trialled during GDA.

164. However, I can take confidence from:

- The basic human-technology allocation of function for the UK ABWR and J-AWBR designs has been reviewed and confirmed (See section 4.3), which minimises the risk of foreclosing any future design changes (Ref. 58).
- The design features high levels of automation (e.g. no plant intervention claims on the operator for the first 30 minutes of a fault) which minimises the risk of foreclosing any future design changes.
- Much of the MCR interface design will be duplicated in remote or secondary HMI locations, so are somewhat bounded by the MCR testing.
- The entirety of the HMI suite on the plant has benefitted from HF good practices as documented in Hitachi-GE's design guide (Ref. 34)
- Considerable paper-based analysis has been performed on the control room design, during Hitachi-GE's programme of human error analysis, including the use of Commission Errors Search and Assessment (CESA) and Technique For The Retrospective And Predictive Analysis Of Cognitive Error (TRACEr), which have identified issues, and driven tangible improvements to the design (e.g. Refs. 33, 31, 35, 37, 40, 43).

165. This area will be an important focus for ONR post-GDA, to ensure that the licensee provides sufficient V&V for all safety-important interfaces. Accordingly, I expect trials to be undertaken as a matter of course by a future licensee and I would expect the degree of realism in such trials to have progressively greater fidelity in representing the intended finished MCR design. In particular, I would expect that trials should become dynamic with active representations of intended user interface designs.

Task and Error Analysis Method

166. The safety of nuclear installations often requires claims on human action. Where safety important human actions and administrative controls are required and their need is justified, the feasibility and reliability of the actions should be demonstrated qualitatively using task analysis. This qualitative modelling should be used to substantiate any HBSCs and the quantitative modelling of the probability of the associated human errors. It is considered necessary to carry out task decomposition and analysis of sufficient depth in order to understand what is being assessed, the demands and influencing factors on personnel and to assist with the identification of reasonably practicable design options or improvements to support human reliability. If this is not done, the HRA risks being superficial. ONR therefore considers HRA to be

more than just quantification of human error. It is this holistic task analytical process that ONR considers as HRA. (Ref. 14).

167. ONR expects fault analysis (comprising DBA, PSA and SAA as appropriate) to be performed to enable both a qualitative and quantitative assessment of the risk arising from plant design and operation. The fault analysis must account for the impact of human activities affecting safety in order for it to be considered complete and to ensure that adequate protection against faults is provided.

168. Task analytical methods should be used to support the DBA, PSA, and SAA and should adequately identify safety important operator actions, demonstrate their feasibility, identify influencing factors and error mechanisms, and determine reasonably practicable improvements (Ref. 14).

169. Although task and error analyses are not new task-analytical approaches, to conform to modern standards, additional information is required above what is suggested by older task analysis guide references. It is important to relate all the relevant task influencing factors, provide a comprehensive 'story', and if any issues are identified, provide information about how these will be resolved and tracked.

170. Hitachi-GE has employed a number of iterations of its task-analytical method, and I am content that the final iteration of this methodology (Ref. 25) meets modern standards. Future applications of this methodology post-GDA should provide a suitable and sufficient analysis of safety important tasks. If an alternative method is selected for use post-GDA, I expect that – as a minimum - it captures and analyses the information identified below.

171. My judgement is based on the method comprehensively capturing all the task-relevant information and linking any human engineering deficiencies to possible solutions and the associated HF issue register unique identification number. Its method captures the following information:

- Task step
- Task description
- Personnel involved
- Location
- Interface required
- Operator cues
- Familiarity with task
- Related procedure
- Potential error mechanisms
- Performance Influencing Factors (PIFs) (Also known as performance shaping factors)
- Time available / Time Required
- HMI adequacy
- Recovery opportunity / dependency
- Consequences
- Error reduction measures
- HFIR Identification Number.

Type A Error Analysis Method

172. Type A errors typically relate to maintenance or calibration errors which, should they occur, could prejudice the later functioning of a safety system. Thus it is important that they are covered within the scope of the safety case. However, for a comprehensive assessment, there needs to be a number of task design features established, which for GDA is not typically the case. These include, manning arrangements, procedures, training, etc. These features are out of scope of GDA and thus Type A error analysis

is typically limited by a lack of relevant information. Practically this means that any analysis focusses on the design of equipment and the layout of the plant.

173. The Hitachi-GE analysis of Type A errors has been confined to those with the potential to make a necessary safety system unable to work when called upon.

174. The population of such errors is very large therefore Hitachi-GE sought to confine its analysis to errors on safety-important systems, thereby inferring that relevant errors would have the greatest potential impact upon nuclear safety. I consider the focus on safety-important systems to be appropriate for GDA.

175. The process of identifying errors with the greatest of importance has been informed by examining the Risk Achievement Worth (RAW) of systems contained within the PSA models (RAW of a modelled plant feature (usually a SSC) is the increase in risk if the feature is assumed to be failed at all times. It is expressed in terms of the ratio of the risk).

176. The following safety important systems were selected by Hitachi-GE for Errors Of Commission (EOC) assessment (Ref. 31):

- Flooding System of Specific Safety Facility (FLSS),
- HVAC,
- HVAC Normal Cooling Water System (HNCW),
- Control Rod Drive (CRD),
- Reactor Building Cooling Water System (RCW).

177. I consider that this scope of study has been reasonable for GDA. Whilst the scope could have been broadened to include more systems, it will be necessary to revisit and expand upon the work undertaken to date post-GDA as details on training and procedures are established. I also take confidence that Hitachi-GE has:

- Considered Type A errors as part of UK ABWR Failure Modes and Effects Analysis (FMEA) and PSA
- Developed, and is following, a comprehensive suite of HF guidance that captures a significant amount of RGP in the area of designing for maintainability (Ref. 34).

178. Recognising the large number of components with which humans might interact during maintenance, Hitachi-GE chose to analyse generic classes of components, such as pumps and valves, heaters, filters, etc. across the five systems identified to be safety-important. I consider this to be a proportionate use of HF resources for the examination of Type A errors. This is because the main focus at Step 4 GDA is upon considering HF within the concept engineering design.

179. The Type A error analysis comprised a workshop which was directed by guiding questions which informed the examination of the maintainability of the components of interest. The workshop utilised British-based NPP maintenance specialists and two SQEP HF specialists. I have assessed the questions involved and a description of how the workshop was undertaken and I consider this to be the application of a suitable method.

180. My judgement is based on the fact that the HF involved in maintenance of equipment can be complex and the method exploits the in-depth experience of maintenance specialists. This experience can thus be focused on the specific risk-important Type A errors and offers useful insight into maintenance error that could affect engineering design.

181. There is a small amount of published RGP for this kind of Type A error analysis and I consider that Hitachi-GE has applied suitable methods in a proportionate way – given the design maturity - to this difficult area of error identification. In the absence of design detail to support a more in-depth analysis, I draw significant confidence in the HFI process applied across the GDA plant design, which has informed the design to its current maturity levels. I expect that HFI will continue along with error identification post-GDA as the design maturity increases along with details of the operating regime. I also note Hitachi-GE's recognition of the need for further work in this area post-GDA (Ref. 17)

182. I consider Hitachi-GE's consideration of Type A errors within the HRA in section 4.4.

Type B Error Analysis Method

183. Type B errors describe those human errors with an immediate and significant consequence. Hitachi-GE has followed the same basic task analytical and quantitative modelling approach as per Type A and C errors as they are functionally similar – error occurs due to similar task design, equipment design, administrative control design, deficiencies, etc. It has also screened based on RAW. I consider this to be appropriate.

184. Type B errors are unlikely to occur in isolation within the control room during normal at power operations due to the high levels of automation and reactor protection present on the UK ABWR. However, it would be sensible to assess Type B errors within the control room during future validation trials.

185. Type B errors with conventional and nuclear significance are more likely to occur outside of the control rooms, e.g. fuel route and waste management, or where there is less automation and protection. Areas for which little design detail existing for GDA. Post-GDA, ONR expects that HF input is provided where necessary to FMEA and Hazard and Operability (HAZOP) analyses of these areas. Or if necessary, as standalone HRA.

186. I consider Hitachi-GE's treatment of Type B errors within the HRA section 4.4

Type C Error Analysis Method

187. Type C errors describe those human errors that occur during fault recovery activities.

188. For Type C omission errors, Hitachi-GE followed the approach outlined above in the 'Task and Error Analysis Method' section. I consider this approach to meet RGP.

189. For Type C EOC, Hitachi-GE has used a different approach; an adapted version of the Commission Errors Search and Assessment (CESA) method (Refs. 63 and 64).

190. The CESA method relies upon the existence of established procedures to identify where procedures might induce an EOC. The examination of procedures looks for the existence of opposite actions at different procedural points (e.g. open a valve versus close a valve). As it is not necessary for procedures to be available at GDA, the CESA method was modified by Hitachi-GE to take account of this. This was done by experienced operators and a HF professional considering the postulated EOCs and seeking potential mechanisms for their occurrence rather than relying on the identification of contrary instructions in procedures.

191. The key benefit of CESA is that the method-originators have spent considerable time developing a comprehensive manual, unlike many other methods which are either propriety or simply published in academic papers. In addition, the method proposes specific means to interface qualitative EOC analysis with structured risk models. Accordingly, I consider this an appropriate method for interfacing HF based insights

with risk assessment given the context. Whilst there are limitations in doing any kind of paper-based EOC analysis, it should also be noted that errors of commission are also typically picked up during ISV and operability trials of the human system interfaces. Hitachi-GE has also performed trials of MCR interfaces, which I consider adequately mitigates the deficiencies in the CESA method, given the scope of GDA.

192. I consider Hitachi-GE's treatment of Type C errors within the HRA in section 4.4

Cognitive / Misdiagnosis Errors Analysis Method

193. The introduction of Human-Computer Interfaces (HCI) into MCR designs results in a greater diversity of forms and types of user interface. This change in interface design may induce cognitive error unless it is identified and either eliminated or minimised.

194. RGP for the identification of error potential in HCI does not appear to be well-reported in the open literature. However, HCI literature acknowledges the significant role of cognition when humans interact with computer-based user interfaces. Accordingly, I would expect good practice to have the following characteristics:

- An established method for predicting human error potential is applied,
- The chosen method should provide mechanisms for identifying cognitive error,
- It should be possible to use the chosen method for qualitatively recommending improvements to design.

195. HCI constitutes a significant proportion of the available HMI in the UK ABWR MCR. Because of the low levels of achievable HCI systems integrity, Hitachi-GE has chosen not to claim the use of such interfaces during post fault scenarios, instead preferring claims on actions undertaken on Class 1 interfaces comprised of hardwired indicators and controls. As HCI forms a central part of the normal user interfaces –especially for monitoring – it will have a role because (unless unavailable) it will influence MCR operators' understanding of the plant prior to the commencement of the fault scenario.

196. To analyse cognitive error within the MCR, Hitachi-GE has employed a two-part method combining two complementary techniques.

197. The first method was a desktop study (Ref. 43) using the 'lite' version of the Technique for the Retrospective and predictive Analysis of Cognitive Errors (TRACEr), known as TRACEr-lite.

198. In the case of MCR HMI, the tool was applied by SQEP HF personnel in consultation with two UK NPP operators. To provide context, the method was applied by stepping through one post fault scenario and applying the TRACEr-Lite guide words to each stage of that scenario. This was done in a static MCR mock-up with drawings of control and display surfaces laid out on the intended sizes and shapes of consoles and panels.

199. The second method (Ref. 43) of the analysis was a live study using a PC-based emulator of the HCI being tested, called the HCI Test Tool (HCITT). The HCI Test Tool provides a dynamic feature where Hitachi-GE can test usability of HCI user interfaces

200. Judged on the criteria, I set out at the start of this section, I consider the use of TRACEr-Lite to be an appropriate method to analyse cognitive error. I consider the application of this method in section 4.3.2

Cognitive Workload Analysis Method

201. Cognitive workload has been implicated in many high profile accidents globally. Too high a level of workload and errors of omission and commission are much more likely. Too little, and boredom and a lack of attention can result. The error data used in

current HRA methodologies reflect this, as high workload factors tend to result in very high human error probabilities being calculated. For example, the Human Error Assessment and Reduction Technique (HEART) method increases the probability of error by a factor of 11 where high workload is identified as likely.

202. ONR thus expects "the workload of personnel required to undertake…[safety important]…actions and controls should be analysed and demonstrated to be reasonably achievable" (SAP EHF.5 Para 452). The optimisation of cognitive workload is key in ensuring good human reliability.

203. Despite the difficulties of predicting cognitive workload in the absence of a simulator or finished facility, Hitachi-GE has nevertheless attempted to do what is practicable given these circumstances. Thus, it has applied the reasonably well-validated Pro-Subjective Workload Analysis Tool (Pro-SWAT) method. Pro-SWAT does not enjoy the same validation of its contemporary method National Aeronautics and Space Administration – Task Load Index (NASA-TLX), but is considerably less resource intensive to apply and given the afore mentioned context I judge this to be acceptable.

204. Pro-SWAT uses three constructs to measure mental workload:

- Time-load – how long do you have.
- Mental load – attentional or mental demands
- Stress load – how stressed you would be during this task

205. Participants rank each of the construct's combinations from 1 to 27 which provides a scale tailored to each participant.

206. Participants then rate each task step against each of the constructs from 1 to 3 and the results are calculated using the above scale.

207. The method was applied in a single workshop involving one Japanese operator and one UK operator with 43 years combined experience of control room operation. During the workshop, five fault scenarios, already previously subjected to human reliability assessment for PSA support purposes, were evaluated.

208. The results are reported in Hitachi-GE's Cognitive Workload Analysis Report (Ref 40).

209. I consider that the use of the Pro-SWAT method is appropriate given the context in which it was applied. However, moving forward post-GDA, it may be more appropriate to use a better validated method such as NASA-TLX.

Conclusion to Section 4.2

210. I consider Hitachi-GE has:

- Developed a suitably competent HF team.
- Identified and developed a comprehensive suite of task-analytic methods to support GDA.
- Identified an appropriate set of codes and standards.

211. I consider that these methods meet ONR's expectations with respect to meeting RGP.

212. The application of these methods goes a long way in providing confidence that the UK ABWR can be built within GB in a way that is acceptably safe and secure. It is therefore important that, to maintain this confidence, a future licensee applies an equally rigorous approach to HFI as the design matures, as well as identifying new methods needed to underpin the development of those areas outside of GDA.

213. I discuss Hitachi-GE's application of these methods during GDA and how they substantiate the design and HBSCs within sections 4.3, 4.4, and 4.5.

Identification and Substantiation of Human Based Safety Claims – Qualitative Human Reliability Analysis

214. It is a fundamental tenet of the SAPs that duty holders must demonstrate effective understanding and control of the hazards posed by a site or facility through a comprehensive and systematic process of safety assessment (SAP FP.4).

"The safety case should list all initiating faults that are included within the design basis analysis of the facility" (Para 628).

"Initiating faults identified in Principle FA.2 should be considered for inclusion in this list" (SAP FA.5).

"The process for identifying faults should be systematic, auditable and comprehensive and should include (c) …internal faults from plant failures and human error…" Para 618 to SAP FA.2.

"DBA should provide an input to…...the identification of requirements for operator actions" (SAP FA.9).

Identification and Screening

215. HRA is underpinned by the identification and understanding of those human activities that are important to safety and how these may fail. This process should employ task analysis to an appropriate degree and draw on the fault schedule, fault analysis (e.g. fault and event tree) and operational experience data (Ref. 14). To be effective for GDA, and to recognise the typically incomplete nature of both the Fault Schedule and the PSA, the requesting party should consider not just explicit claims within the safety analysis, but also any implicit claims that feature within the lower level safety analysis documentation (for example, claims on personnel performing surveillance activities). The screening process should consider both quantitative and qualitative criteria to be defined by the requesting party.

216. Failure to follow a method which exhibits these characteristics risks any analysis of HBSCs being superficial. Unless subjected to appropriate testing and assessment it becomes possible that claims may be made upon the human that cannot be reliably fulfilled in practice.

217. In this section I consider whether Hitachi-GE's has employed effective methods for the identification and screening of the HBSCs important for nuclear safety. The appropriateness of Hitachi-GE's task analytical methods is discussed in detail in section 4.2.4.

218. Hitachi-GE chose to manage its HBSCs via a database. This was a live tool so was constantly updated during the course of GDA. The latest 'snapshot' of the HBSC database was submitted at the end of GDA in Revision E, September 2017 (Ref. 65).

219. This iterative nature is appropriate for the GDA process, because as the design evolves, better understanding is obtained concerning what the human may need to do outside of the initial allocation of function. Whilst the late nature of the HBSC analysis has constrained my assessment somewhat, I do consider that Hitachi-GE's HF team has taken a pragmatic approach as they have also been dependent on the availability of design, PSA and DBA information. This does mean, however, that ONR will need to revisit this analysis post GDA as part of its normal regulatory business as the design progresses.

220. Hitachi-GE has had to make assumptions in order to undertake some HBSC assessments. This is because analysis of tasks would not be feasible without assumptions being made about procedure design or roles, responsibilities and organisational structure. I am satisfied that these assumptions have been properly recorded and, therefore, should those assumptions be challenged by a licensees design intentions for procedures, staffing etc. then the assessment can be revisited.

221. The HBSC database contained 206 HBSC entries at the end of GDA. To ensure the best use of the HF resource available, this necessitated the application of screening methods to ensure that the HF resource was focussed on those human actions with the greatest impact to nuclear safety.

222. To screen HBSCs, Hitachi-GE applied a method similar to an engineering category and classification assessment. It is described in Reference 65. It uses the following categories to inform the ranking process:

223. I consider this approach to be appropriate and in line with ONR's expectations (SAP ECS.2, Para 164, "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").

224. To screen PSA HBSCs, Hitachi-GE has developed a Risk Achievement Worth (RAW) and Cut-set based method (Ref. 65).

225. RAW values provide insight into the importance of a human action with respect to plant risk. They show what increase, in core-damage frequency or large radioactive material release, would be expected if the task of interest was assumed to fail. For example, if a RAW value of 2.0 is revealed when an error probability is set to one (failure), this shows that if it failed, the result would be a doubling (100% increase) in plant risk. Hitachi-GE used a three-point rating scale based on a combination of RAW, Cutset and task novelty criteria.

226. I consider the criteria applied to be appropriate in reducing the number of HBSCs for further analysis to a manageable number. Whilst there is no universally agreed RGP in this area, the values do align with previously used criteria on other GDAs.

227. There is a down-side of using risk as a dominant criteria in the screening process. This is that it can narrow the analysis too much. Typically, cut-sets and RAW values tend to identify similar tasks, all centred on a few key locations or components.

228. Although ONR expects that a GB nuclear safety case be developed proportionate to the risk posed by the plant, it also expects that it be 'complete' (Ref. 14). That is, it is comprehensive of the activities performed on the plant. In the case of GDA complete would mean within the scope of GDA and not the full operational safety case.

229. Thus, for an HF case to be considered complete, it should not just focus on purely those few high risk contribution human actions. It should also proportionally assess a fully representative range of HBSCs.

230. I welcome the fact that Hitachi-GE has considered this and required the screening-in of HBSCs that do not easily fit into the above schemes, but are nevertheless considered to be important. The rules / criteria can be found within Reference 65, but for example considers things like engineering class and to identify the most important HBSC.

231. The output from application of any of the above methods is fed into a Hitachi-GE proprietary substantiation level decision matrix. This determines the level of analysis / substantiation required.

232. Analysis Level 1: Detailed Tabular Task Analysis (TTA) and qualitative human error analysis (HEA), with full HRA (i.e. quantification of Human Error Probability (HEP), if PSA-related); specific reference to consideration within analysis regarding allocation of function, workload, and other Performance Influencing Factors (PIFs); HF task-based support to the design; generic verification for the related SSCs/HMIs and specific verification of the design features supporting the claimed actions, with preliminary validation of the HBSC (on a representative basis – may be considered validated by a similar HBSC test) (Ref. 65).

233. Analysis Level 2: Higher level (i.e. less detail) task and error analysis (where appropriate); general consideration within HF analyses regarding PIFs; HF task-based support to the design where new; generic HF verification of SSC/HMI design and, where SSC/HMI is new, specific verification of design features to support the task. For HBSCs derived from PSA HFEs, justification must be provided that to demonstrate that an appropriate bounding case has been subject to Level 1 Substantiation, for any HBSCs that are judged to be similar to other assessed task(s) (Ref. 65).

234. Analysis Level 3: Simple task-based analysis or other means to show “achievability” of task, taking into account specific PIFs that might impact achievability (Ref. 65).

235. Hitachi-GE has performed a comprehensive review of a wide range of material where explicit and implicit claims on the human may be made. These sources (Ref. 65) include:

- Reference plant and previous ABWR PSA HFE review (J-ABWR records within Hitachi-GE, and US ABWR Design Certification Document (DCD); used for the preliminary HBSC listing only).
- OPEX Report for UK ABWR
- DBA related human action claims, from the fault assessments, which includes actions required for design basis faults (DBFs) and beyond-design basis faults (BDBFs).
- PSA claimed human actions (from HFEs) analysed in the Human Reliability Analysis Report (HRAR).
- Review of UK ABWR PCSR chapters, Basis of Safety Case (BSC) and Topic Reports (TRs) for implied and ALARP HBSCs, particularly those related to system topic area claims not identified in bullet 2 and 3 above.
- Review of BWR owners group guidelines for producing EOPs and SAGs for any required operator actions not already identified through bullets 2 through 4 above.
- Various HF analyses in support of design and safety case development activities, particularly allocation of function, task and error analysis and testing activities supporting design requirements development; for example that to support the HMI topic area given in PCSR Chapter 21 Human Machine Interfaces.

236. In total, ~ 60 documents were reviewed.

237. Hitachi-GE claimed that the full scope of human actions required to achieve safe operation across all the system design analysis topic areas have been explicitly identified and clearly described. It also claimed that this work has been performed proportionate to the risk importance of the human actions, which I consider to be a sensible approach and in-line with ONR’s expectations.

238. I tested these claims in conjunction with my fault studies and PSA colleagues and consider it valid.

239. With respect to the scope of HBSC identification in the PSA, the HRA is fully integrated into all levels: 1, 2, and 3. Operator actions are considered in level 1 and 2, which are detailed logic models. Level 1 and 2 are 'linked' which allow dependencies to be considered. All modes of operation are considered, along with fuel route and the most significant hazards. Operator actions are included in all aspects. The HRA considered within the PSA is all recorded in the single HRA report (at the end of GDA the PSA was aligned to revision D, with hazard PSA specific actions in revision F). Hitachi-GE conducted a sensitivity analysis of the changes to the HRA data on the at-power, shutdown, and spent-fuel pool PSAs. The impact of these changes, although significant in a couple of areas, is explicable, and understood by the ONR PSA team and does not challenge their regulatory judgement on the adequacy of the PSA for GDA.

240. With respect to deterministic analysis, the FMEA included in UE-GD-0071 (Ref. 74) to identify initiating events is adequate / auditable and specifically identifies HBSCs including operator and maintenance errors. It clearly identifies the SSCs required to deliver the functions of reactivity control, short and long term cooling (plus other functions), and states whether the actuation of those SSCs is automatic or necessitate an operator intervention.

241. Based on the outcome of the PSA and HF assessments it can be concluded that the current HRA supplemented by the internal hazards PSA refinement and the Internal Events At Power (IEAP) sensitivity analysis to reflect the most recent HRA values is sufficient to support the UK ABWR 'generic' PCSR.

242. I judge that Hitachi-GE has developed a sensible and risk-proportionate approach to the identification and screening of HBSCs. My judgement is based on the fact that, whilst there is no industry-wide consensus on how to identify and screen HBSCs for proportionate analysis, the methods selected by Hitachi-GE have their origins in sound engineering Category and Classification practices. They also align well what has been applied before in previous GDAs.

243. I consider that, noting where the UK-AWBR design is with respect to maturity, that Hitachi-GE has applied a proportionate and fit-for-purpose process for the identification of HBSCs. I welcome the fact that Hitachi-GE has not limited its search to only explicitly claimed operator actions within the PSA and DBA, but has instead taken a more holistic approach by expanding its analysis to explicitly search for implicit claims within design and engineering reports. I note that whilst not claimed, Hitachi-GE has also informed its review by OPEX as evidenced in some of the analysis workshops.

Substantiation

244. Substantiation of HBSCs is achieved through a combination of V&V activities and analysis. ONR does not prescribe a single approach. The optimal combination of evidence is determined by the maturity of the design undergoing GDA.

245. Substantiation activities include:

- Task Verification
- Design Verification
- Validation

246. Task verification is the analytical process that verifies that the design provides the necessary features to support reliable human-technology system performance. It is

performed by comparing the controls, instrumentation, alarms, tools, etc. identified as required in the task analysis with what is provided in the design.

247. Design verification is the audit process by which the requesting party demonstrates that the design meets the relevant codes, standards, and criteria.

248. Validation is the analytical process by which the human –technology performance is demonstrated to support safe operation of the plant. This can range from full scope high fidelity ISV trials, to paper based task and error analysis.

249. The higher the fidelity the validation approach, the more reliable the evidence. For example, the best evidence is provided by ISV trials – where SQEP operators, using representative procedures and a fully representational control room are tested against a full range of normal, abnormal and emergency conditions.

250. It is typical to provide substantiation evidence in each of the V&V areas, which as stated above, is predicated on the availability of design information. When judged in concert, data from each process provides compelling evidence that the HBSCs are valid (or not).

251. The level of design detail required for GDA need only be sufficient to demonstrate that the design does not foreclose on possible future changes that may be needed if future design and safety analysis identifies that HBSCs cannot be supported without changes to the technology. Thus it is advantageous to have a relatively mature plant design for GDA as it can de-risk future design change impact but it is not essential.

252. The original intention for the UK ABWR GDA was that it would closely match the J-ABWR in design. However, as the GDA progressed, it became apparent that, amongst other things, the user interfaces in centralised control locations would require modification relative to J-ABWR to meet ONR expectations for diversity in C&I and user interfaces. These design changes for the UK ABWR had a significant impact on the maturity of some elements of the design and the timely delivery of submissions by Hitachi-GE.

253. Thus my assessment of HBSC substantiation has needed to draw from a wide range of analytical and topic areas, and is done so without the benefit of having seen evidence from high fidelity control room trials as per previous GDAs. This means that although I am confident in my conclusions, there remains significant design effort required post GDA to completely substantiate the UK ABWR HBSCs.

254. Hitachi-GE has developed a claims, arguments, evidence structure for its safety case. To implement this approach, it has used the following concepts.

255. The UK ABWR has five fundamental safety functions (FSFs):

- FSF 1 - Control of reactivity
- FSF 2 - Fuel cooling,
- FSF 3 - Long term heat removal
- FSF 4 - Confinement/Containment of radioactive materials
- FSF 5 - Others

256. These are further divided into uniquely numbered high level safety functions (HLSFs). For example, FSF 1 (control of reactivity) is broken into 10 HLSFs:

- HLSF 1-1 - Functions to prevent excessive reactivity insertion
- HLSF 1-2 - Functions to maintain core geometry
- HLSF 1-3 - Emergency shutdown of the reactor

- HLSF 1-4 - Functions to maintain sub-criticality, etc.

257. The UK ABWR fault schedule specifies the HLSFs provided by the SSCs claimed to have a role in ensuring safety following an individual fault. The requirement to provide the specified HLSF identified in the fault schedule becomes a safety functional claim (SFC) for that SSC. SFCs are those actions performed by an SSC to directly implement the safety function; for example insert control rods, open a valve, start a pump, etc. An SFC may comprise a human action.

258. In addition, an SSC may also have a number of safety property claims (SPC) associated with it, which are claims that provide the safety justification that the UK ABWR is compliant with Hitachi-GE's Nuclear Safety and Environmental Design Principles.

259. Hitachi-GE defines HBSCs as those operator actions which are required to achieve the SFC and SPCs. They are grouped separately from, but directly linked to the SSC SFC and/or SPC, to enable a more systematic assessment of their credibility and take account of wider performance shaping factors.

260. HBSCs are split into three levels:

- Level 1 and Level 2 HBSCs capture (respectively) the fundamental system design and ensure that UK HF RGP is captured and implemented.
- Level 3 HBSCs support achievement of the SFCs (operational actions) and SPCs (EMIT actions) for each relevant system, specific-action claims were designated by PCSR topic area and the safety analyses.

261. This approach permits the tracing of SPC and SFC HBSCs from the fault schedule, to individual basis of safety case or analysis reports, through to the PCSR. Thus it should be possible to follow the claim through to the supporting arguments and ultimately the evidence demonstrating the claim. Note: This approach was changed later during GDA so that HBSCs were divided into Functional HBSCs & HF SPCs. I do not consider this affects my assessment and consider this approach equally valid.

262. The PCSR presents the complete listing of all the HBSCs – supporting both SPC and SFC. It shows the relationship between the fundamental safety function, the supporting high level safety functions, the fault schedule, the system, system state, and the HBSCs. Each HBSC is allocated a unique identification number.

263. An additional document, the functional HBSC summary report (Ref. 65), supports the PCSR and provides a claims, arguments, evidence substantiation summary for every HBSC.

264. Below I illustrate how this process works using an example HBSC.

265. It is claimed that the control room operator "*manually initiates containment venting, prior to core damage and containment failure in DBFs, using the Atmospheric Control (AC) System controls on the MCC*". This HBSC can be found in the list of functional HBSCs table within PCSR Chapter 27 Human Factors.

266. This table shows that this HBSC supports the "*function of alternative containment cooling and decay heat removal*" the high level safety function, which in turn supports the fundamental safety function of "*long term heat removal*". It also shows the fault group in the fault schedule where this comes from and the system used to perform the function.

267. From the unique identification number it is possible to drill down further into the functional HBSC summary report (Ref. 65). This provides the following information:

- HBSC ID
- Generic type (Functional or Property)
- Claim
- Context
- Location of operation
- Human failure event type
- Ranking
- Remark for ranking
- HBSC substantiation (Arguments)
- HBSC substantiation (Evidence) (These two boxes present all the arguments and then list the relevant evidence demonstrating that the arguments are valid)
- Evidence references
- ALARP discussion
- Remark
- Source

268. For the chosen example, a number of arguments are made. Each argument is identified by an "A-*n*" number. Examples are shown below:

269. The arguments relate to design review, HF analysis and V&V, which is important for robust substantiation.

270. Below is reproduced a small sample of the corresponding evidence summary statements. The bracketed E number provides a further reference to the document containing the evidence.

[redacted]

271. Whilst I found the quality of the documented evidence variable in its level of detail, ultimately I am satisfied that the approach taken by Hitachi-GE is sensible and meets RGP.

272. Using the HBSC example above, when attempting to confirm that the argument regarding task performance was valid, I was unable to fully do so in either the BSC document for the Primary Containment Vessel (PCV) gas control systems (Ref. 81) or within the Human Factors V&V report (Ref. 29).

273. The BSC report identified the HBSC but did not provide any demonstration of performance. However, other more HF focussed BSC documents do attempt to link the claim to performance evidence e.g.:

- HGNE, UK ABWR, GA91-9201-0002-00109 - 3E-GD-A0166 - Rev.1 - Basis of Safety Cases on Overall Human-machine Interface. (Ref. 86)
- HGNE, UK ABWR, GA91-9201-0002-00060 - 3E-GD-A0029 - Rev.2 - Basis of Safety Cases on Main Control Room Human-machine Interface. (Ref. 87)
- HGNE, UK ABWR, GA91-9201-0002-00061 - 3E-GD-A0030 - Rev.2 - Basis of Safety Cases on Remote Shutdown System Human-machine Interface. (Ref. 88)
- HGNE, UK ABWR, GA91-9201-0002-00062 - 3E-GD-A0031 - Rev.2 - Basis of Safety Cases on Backup Building Human-machine Interface. (Ref. 89)

274. The V&V report, where I would expect many of the HMI based HBSCs to be validated, based on the evidence summary within the HBSC report (Ref. 38), was insufficiently detailed to provide confidence that all MCR based HBSCs were fully substantiated. For example, key information such as time available versus time taken for each HBSC tested was not included within the report.

275. The report concluded the following without explaining as to how the evidence related to the HBSCs listed in the HBSC report (Ref. 38): *The overall result was that the trials provided clear evidence to show that all tasks were successfully completed in a timely and effective manner. Participants reported no difficulties in carrying out the tasks as required hence it can be concluded that the layout and inventory of the HMI as depicted in the mock-up is fit for its intended purpose and requires no major modification based on the current level of design maturity although it is recognised that the design will be confirmed and verified through the detailed design activities after GDA.*

276. Whilst this is a significant gap with respect to providing a clear claims, arguments and evidence route to substantiation, when considering the wider safety submissions provided by Hitachi-GE, I conclude that HBSCs are sufficiently substantiated to avoid foreclosing on options as the design progresses beyond GDA.

277. Hitachi-GE has provided additional substantiation evidence via supplementary analysis. This includes, but is not limited to, the following references:

- A baseline J-ABWR assessment (Ref. 24)
- An allocation of function Review (Ref. 15)
- Strategy of Use for HMIs (Ref. 39)
- Human Reliability Analysis Report (Ref. 66)
- HCI-Induced Cognitive Error Analysis Report (Ref. 43)

- Human Factors Concept of Operations Report (Ref. 42)

278. Hitachi-GE undertook a comprehensive gap analysis to identify where the baseline design had shortfalls in HF design inputs and analyses relative to modern HF RGP and GB regulatory expectations. This review was systematically informed by the identification of relevant regulatory expectations, HF standards, and guidelines. The identified gaps and recommendations are summarised in the revised HF Baseline Report (Ref. 24). These gaps could be seen to be addressed by the Hitachi-GE HF work programme, which was fully integrated with the relevant engineering and safety case activities by means of a Human Factors Integration Plan/Programme (HFIP) (Ref. 20). I considered that the developed programme fully integrated HF within the design and safety assessment processes. Whilst I cannot be satisfied that HF has been fully integrated within J-ABWR design, I can be confident that the HF activities undertaken for GDA have ensured that HF has been adequately integrated into the UK AWBR design & safety case for this point in the design maturity/phase of project. It will be important for a future licensee to maintain similar levels of integration post GDA.

279. This assessment contributes to the substantiation of HBSCs by identifying where the baseline design was considered to meet RGP and identifying improvements for the UK-AWBR, thus providing an element of design verification.

280. The gap analysis identified that there was insufficient evidence to show that dependency on human action for nuclear safety had been systematically assessed. Hitachi-GE re-assessed the J-ABWR allocation of function (Ref. 35) to provide this confidence and to show that the reliance on operator input for nuclear safety has been reduced so far is reasonably practicable. The output of this analysis was evidence that the allocation of function is fundamentally sound – which aligns with the views ONR's PSA and Fault Studies analysis. The analysis also identified candidates for an additional 15 automated tasks. This has resulted in improvements to the UK-AWBR design and includes the following additional automated features:

- SLC initiation;
- Exchange water source of High Pressure Core Flooder System (HPCF) and Reactor Core Isolation Cooling System (RCIC) from Condensate Storage Tank (CST) to S/P;
- Flooding System of Specific Safety Facility (FLSS) initiation and valve arrangement for core injection;
- SCRAM by S/P temperature high;
- Initiation of S/P cooling by RHR;
- Initiation of standby RCW/Reactor Building Service Water System (RSW) by S/P temperature high;
- Inhibit of Automatic Depressurisation System (ADS) automatic initiation at ATWS;
- Initiation of diverse ADS;
- Initiation of Diesel Generators (DGs) of B/B

281. I consider the allocation of function analysis supports the substantiation of HBSCs by demonstrating that the basic allocation of function is sound, i.e. those tasks allocated to the operator are within the capability of human limitations. If the detail of these tasks is informed by good HFI, then reliable human performance should follow and my assessment of the HFI process has shown it to be RGP.

282. Hitachi-GE submitted a HMI usage strategy document (Ref. 39), which supplements the evidence provided by the V&V trials. It considers permutations of partial and full failures of Class A1 and A2 SSCs by describing how:

- Failures would be detected,
- The role of the operator in monitoring automated backup system activity,

- Or in detecting the need for manual action to reinforce failed automation.

283. As part of this work, Hitachi-GE has demonstrated that:

- An operator would be able to detect that a cue had been lost and how the related parameter could be determined through alternative indications. This has shown that suitable substitute indications will be available.
- Following a single failure, an alternative means of control would be available on the same interface system in some instances and otherwise control will be available on an alternative HMI system.
- To the extent practicable at GDA Step 4, systemic failures will be detected and the operator will transfer their monitoring or control activity to another HMI, as appropriate.
- That smooth transition between HMIs can be achieved with minimised task disruption in the event of single point or systemic failures.

284. I consider the HMI usage strategy, within the limitations afforded by the design maturity, supports the substantiation of HBSCs by demonstrating that the MCR operators can adequately detect that the HMI has failed and effectively migrate to alternative means of control. I expect that this topic will be revisited by a future licensee as the wider plant HMI develops. I consider this to be part of the normal HMI development process.

285. Hitachi-GE submitted Reference 40, Cognitive Workload Analysis Report to address the requirement within RO-0069. This report considers a small sample of potentially high workload MCR based post fault actions and also includes within scope the issue of distraction within the MCR.

286. The report confirms that the analysed initial responses following a fault are typically very high workload, which is unsurprising and typical of most nuclear power stations when the automation / engineered safety systems have failed. However, I can take confidence from the fact that no typically low / medium workload tasks were identified as high, which would indicate issues with the concept design. It is also important to note that:

- The design features no plant intervention claims on the operator for 30 minutes following a fault.
- Immediate reactivity control and short term cooling at the start of a fault transient is claimed to be automatic.
- Where manual actions are required for long term cooling, these are typically simple in nature and error tolerant. ONR fault studies reviewed Hitachi-GE's sensitivity study on these activities and considered that the sensitivities illustrate that there is plenty of time to perform the necessary actions, and substantiating them in the future should not be a problem.

287. Based on the analysis a number of recommendations were made to help optimise workload post fault. However, I consider the major benefit from workload analysis is realised when measured during simulation studies, which was not practicable during GDA.

288. In addition, the analysis has provided some verification of the Technique for Human Error Rate Prediction (THERP) based human reliability estimates used in the UK ABWR PSA, which increases the confidence that can be placed on the HRA assessments that support the safety case. HRA is discussed in section 4.4.

289. The distraction assessment identified no distractors specific to the UK ABWR and provides confidence that the basic control room layout is sound. The majority of

distractions identified arise from, and can be managed by, organisational and task design – outside of the scope of GDA.

290. Overall, I consider that the assessment of cognitive workload and distraction has been undertaken to the extent practicable for GDA Step 4. I note the limitations of this assessment work due to design maturity and consider it will be necessary for a future licensee to revisit the topics of cognitive workload and possibly distraction as the design progresses. It may also need to include within scope, the HBSCs made on field operators.

291. Hitachi-GE submitted HCI-Induced Cognitive Error Analysis Report (Ref. 43) which describes an assessment of the UK ABWR MCR design using the two-part study (desktop TRACEr-lite analysis and live emulator study). This was submitted to:

- Substantiate that the HCI and demonstrate that cognition errors were not disproportionately contributing to plant risk.
- Substantiate the use of computerised interfaces during post fault operations. This claim was later rescinded.

292. In the first phase of the analysis, the method considered the HMI within the MCR as a whole. It was applied by a qualified HF analyst to 28 HFEs previously subjected to HRA analysis and, following verification by discussion with operators having previous UK Pressurised Water Reactor (PWR) and J-ABWR experience, six potential issues for HMI design within the MCR were identified.

293. The second phase of work involved eight subjects interacting with the Hitachi-GE HCI Test Tool (HCITT). The test tool simulates screen-based interactions with the flat displays to be located in the MCR. A HF professional observed eight test participants undertake a number of dynamic navigation tasks. The second phase resulted in the identification of 12 design issues and corresponding recommendations for the HCI used in the study.

294. The insights gained from this analysis were used to inform the quantitative HRA, which in later iterations (Ref. 44) considers errors of commission associated with the use of the MCR HMI.

295. I consider this analysis provides useful additional substantiation of the HBSCs tested. Where issues were identified, sensible improvements were suggested. However, the analysis performed was dictated by the maturity of the design and the availability of SQEP operators. I note that those participants with the greatest UK ABWR / J-ABWR experience made the lowest number of errors. Given the design maturity, I expect a future licensee to continue with the analysis of the HCI as the design progresses. I consider this to be normal business.

296. The concept of operation for the UK ABWR is presented in Reference 42. This report presents the baseline set of assumptions concerning:

- Job roles,
- Operational responsibilities,
- Competencies for the MCR crew performing the majority of claimed HBSCs; This same crew would be involved in operations in the RSSR and the B/B.

297. The concept of operations was derived from the J-ABWR and modified to reflect the UK NPP operational practices. It draws from the experience and knowledge of a UK future operations team. I consider this to be a sound basis for demonstrating feasibility of claimed human based safety actions through HF analysis.

298. The concept of operations report describes the expected staffing levels and roles for MCR-based personnel and elsewhere on the plant where claims might be placed upon individuals performing those roles. This includes processes for supervision and checking intended to improve overall performance of human based safety actions.

299. I was able to verify that the operational concept is being consistently applied in practice to the task analysis of HBSCs and the logical and probabilistic modelling of those actions. This is demonstrated in:

- The derivation of HEPs presented in the Human Reliability Analysis Report
- (Rev E, July 2017) (Ref. 66), which covers Internal Events at Power (IEAP) Level 1 and Level 2 PSAs; SFP Level 1 and Level 2 PSAs; and Shutdown Level 1 PSA.
- Hazards HRA Addendum, (Ref. 67)
- Task Analysis in Support of HBSC Report, (Ref. 68).

300. The proposed crewing structure is not explicitly referred to in the majority of HBSCs but only on those supported by documented task analysis. However, through my discussions with Hitachi-GE HF personnel I am satisfied that the operational concept has consistently influenced their thinking when analysing the deterministic human based safety claims.

301. I judge that Hitachi-GE has developed a valid concept of operations applicable to British operation of the UK ABWR. It provides a credible description of assumed operational roles and an appropriate allocation of function between personnel for the execution of safety actions and the checking that those safety actions have been correctly executed. The operational concept has been applied in a consistent fashion to probabilistic and analyses. It supports the substantiation of HBSCs. The future licensee will need to verify that the concept of operations remains valid as the HMI design matures. It will also need to translate the concept of operations into a formalised and validated conduct of operations. I consider this to be part of normal business.

302. Whilst I consider the UK ABWR HRA within Section 4.4 below, it is important to consider its role with respect to the deterministically substantiating the HBSCs. The current iteration of the HRA substantiates those HBSCs within the PSA via limited task verification. It clearly identifies those design features – interfaces, cues, etc. – that need to be available for the task to be reliable. It also identifies the time-related success criteria from the PSA and demonstrates (Ref. 66 - Time Line Analysis Table) that there is sufficient time for the HBSC to be performed. Or where design feature or time available have been found to be inadequate, the specific HBSC has either been withdrawn and the PSA model modified accordingly, or clear recommendations have been made to ensure resolution post GDA. I consider this to be conservative approach which meets RGP.

Conclusion to Section 4.3

303. The HBSC substantiation has been confined by the design maturity of the risk important SSCs. This can be viewed both positively and negatively: it has limited the level of substantiation possible for GDA, but provides opportunities to accommodate design changes taking into account the wider out of scope GDA areas and licensee preferences regarding operational regimes.

304. I consider the level of detail provided was sufficient for my assessment and the methods are appropriate for the level of design maturity.

305. When I consider the suite of submissions provided by Hitachi-GE it is difficult to identify what other analysis could have been reasonably performed given the availability of design information. From what has been submitted, I consider that:

- The most important HBSCs have been identified and considered within the design and safety analysis.
- The allocation of function between the human and technology appears fundamentally sound.
- Few claims are made on the operator within the design basis.
- What claims are made appear relatively straight forward with reasonable time available to respond, with a number of exceptions which Hitachi-GE recognises itself.
- There is strong evidence that the HFI programme has demonstrably influenced the design.

306. The positive role the major HMIs play in providing assurance that risk from operator action or inaction is reduced so far as is reasonably practicable is discussed in section 4.5.

307. I judge that for the purposes of GDA that the HBSCs are sufficiently substantiated; thus minimising the risk of foreclosing on future design options.

Quantitative Human Reliability Assessment

308. ONR's expectations concerning human reliability analysis are set out in a number of SAPs. However, the primary reference is SAP EHF.10, which states:

"*Human reliability analysis should identify and analyse all human actions and administrative controls that are necessary for safety".*

309. TAG 030 PSA, guides that the scope of the HRA should account for contributions to risk including:

- pre-fault human errors (e.g. misalignments and mis-calibrations),
- human errors that lead to initiating faults,
- human errors during the course of the fault sequences including those required for repair or recovery actions,
- and potential dependencies between separate human activities (either by the same or by different operators).

310. When models are used for the calculations of input probabilities then the methodologies used should be justified, and should account for all key influencing factors (SAP FA13).

311. This section presents my assessment of the application of Hitachi-GE's quantitative analysis of human error.

312. In it, I consider whether:

- Hitachi-GE has carried out a review of human reliability that aligns with the expectations set out above.
- The level of analysis carried out and the HEP data generated are sufficient and appropriate to support the UK ABWR PSA.

313. For GDA, I do not expect a fully developed quantitative HRA to be in place as there are likely to be many uncertainties concerning design maturity and also significant assumptions made about future licensee arrangements.

314. My expectation is that:

- The methods used were sound,
- The scope, within the constraints of design maturity and future licensee inputs, is adequate.
- Where uncertainties or assumptions exist, these were captured for future resolution or validation.

Scope of HRA

315. The HRA for the UK ABWR is presented in the Human Reliability Analysis Report. This submission has received multiple revisions to accommodate the ongoing HRA analysis. At the close of GDA Rev F (Ref. 66) was issued. I discuss how the various issues relate to the PSA.

316. I can confirm that HBSCs are fully integrated into all levels of the PSA 1, 2, and 3. Operator actions are considered in level 1 and 2 comprising detailed logic models. Level 1 and 2 are 'linked' which allow human-dependencies to be considered.

317. All modes of operation are considered, along with fuel route and the most significant hazards. HBSCs are included in all areas.

318. The HRA considered within the PSA is recorded in the single HRA report (Ref. 66) (at the close of GDA, the PSA was aligned to revision D, with hazard PSA specific actions in revision F). I consider that the assessment of operator actions in the hazards PSAs met RGP as it followed the standard task analytic and takes into account both scenario and task specific factors related to the hazards that could significantly impact upon human performance.

319. Hitachi-GE conducted a sensitivity analysis of the changes to the HRA data on the at-power, shutdown, and spent-fuel pool PSAs. The impact of these changes, although significant in a couple of areas, is explicable, and has been assessed in the ONR PSA assessment and does not challenge its regulatory judgement on the adequacy of the PSA for GDA.

320. The summary above refers to Hitachi-GE's consideration of Type C errors. Both errors of omission and commission are considered.

321. Type A errors are also considered in the PSA. However, the lack of design detail, and licensee arrangements have confined the analysis to a higher, generic task, level. This is not unusual for GDA as many of the factors significantly affecting task performance, such as job design, training and procedures, are not mature or available during GDA. I consider that Hitachi-GE took a proportionate approach to assessing and quantifying Type A errors for GDA given the design and licensee arrangement detail available at the time.

322. Type – A errors were categorised into 4 basic types:

- Mis-calibration of pressure transmitters.
- Mis-calibration of water level transmitters.
- Mis-alignment of manual valves.
- Failure to restore circuit breakers (leaving equipment isolated). Based on errors that have been assessed and quantified for four generic EMIT classes.

323. These were subject to generic task analysis and subsequently quantified to provide conservative screening data for use in the PSA. The quantification of these generic HEPs reflected an appropriate application of the THERP HRA method. I consider that that Hitachi-GE has applied this approach proportionately and with intelligence, as evidenced by the fact that two discrete tasks where identified where the 'fit' of the

generic error was not close enough. In this case, specific analysis was performed. These tasks comprised:

- Invasive maintenance of a motor operated valve
- Invasive maintenance of an air circuit breaker.

324. The consideration of Type B errors is similar to that for Type C. Type B errors are included within:

- The Internal Events Shutdown Level 1 PSA;
- The Spent Fuel Pond PSA (Level 1 and 2).
- The IEAP Level 1 PSA.
- Fuel Route and Dropped Loads PSA

325. Type B errors are typically rare on a reactor plant during normal at-power operations, as considerable international effort has been expended upon developing reactor protections systems, which provide protection against human errors (with single failure consequences). Unsurprisingly, there appears to be no risk significant Type B human errors identified for MCR based at-power operations. However, 13 Type B errors were identified and quantified in relation to maintenance type activities. These comprise mainly errors that that can directly lead to leakages or LOCAs. Given the level of design and licensee arrangement detail available for GDA, I consider this proportionate to the current stage of the UK ABWR project.

326. To conclude, whilst there are some limitations with respect to detail, these are commensurate with the design detail available during GDA. I consider the current scope of the HRA sufficient and proportionate to support the UK ABWR PSA and PCSR for GDA. A conclusion supported by my PSA colleagues.

327. The limitations can be attributed to a combination of a lack of design detail and the fact that much of the HRA was performed late in the GDA. I expect that a future licensee will continue to develop the HRA in support of the PSA to reflect the evolution of the design and to reflect future licensee operating and arrangement assumptions. This expectation is bounded by the following key PSA Assessment Findings:

- AF-UKABWR-PSA-001
- AF-UKABWR-PSA-002

328. It is important to note that some HF input may be required to resolve the other PSA assessment findings.

Quantitative Human Error Probability Method

329. ONR expect that “When models are used for the calculations of input probabilities, for example, in human errors….then the methodologies used should be justified, and should account for all key influencing factors” (Para 657, SAP FA.13)

330. This section presents my assessment of Hitachi-GE’s approach to the quantitative analysis of safety important human actions and whether the method used is adequately justified.

331. An important enabler to the suitable and sufficient analysis of HBSCs is the close integration between the PSA, the HRA and HFI design process which delivers a design that supports reliable human performance. A failure to adequately integrate the HRA into the PSA and consider the human performance effects of the design, can lead to an unrealistic and superficial estimate of facility risk.

332. Hitachi-GE has explicitly identified HBSCs within the basis of safety case documentation linking the design to the associated HBSCs. The HBSC report (Ref. 65) links the HBSC with specific design property claims – as discussed in section 4.3.

333. Both the PSA and HRA were completed in parallel and late in the GDA process and therefore this meant that Hitachi-GE did not have time to fully integrate the HRA into the PSA for GDA. In lieu of this, Hitachi-GE performed a sensitivity study to determine the impact of this on the facility risk. The study showed that risk will increase significantly when the revised HRA is integrated, particularly during plant shutdown and for spent fuel pool operations. However, Hitachi-GE claimed that overall risk remains low and the extant PSA still contains significant conservatisms, which will be gradually removed by best estimate models. This topic is discussed in greater detail within the PSA assessment report, Reference 69.

334. I concur with my PSA colleagues in this area, that whilst not optimal, this approach is sufficient for GDA. I also note that both the HRA and the PSA will require significant revisions post-GDA. ONR will monitor the development of the HRA as part of the normal regulatory process.

335. Whilst ONR does not prescribe HRA methods, it does take into consideration the SAPs governing the methods and data used in safety case analyses when judging the adequacy of HRA methods not typically used within GB. The SAPs of relevance comprise:

- SAP AV.2 Calculation Methods: Calculation methods used for the analyses should adequately represent the physical and chemical processes taking place. Models should be validated for each application made in the safety analysis.
- SAP AV.3 Use of data: The data used in the analysis of aspects of plant performance with safety significance should be shown to be valid for the circumstances by reference to established physical data, experiment or other appropriate means.

336. An option open to Hitachi-GE was to adopt more straight forward techniques, for example an unmodified THERP approach or the alternative HEART method; both of which are recognised in GB but with acknowledged weaknesses concerning the ability to model human-computer interaction.

337. I welcome Hitachi-GE's ambitions to address some of the methodological constraints in these methods by developing a hybrid approach to obtain better estimates of human reliability, and ultimately for the benefit of an improved, more balanced PSA model.

338. Hitachi-GE selected THERP modified by the SPAR-H method as the basis for its assessments. Given the novelty of the adopted approach, I commissioned CRA-Synergy to independently model a sample of Hitachi-GE's HEPs (Ref. 70). This is discussed later in this section.

339. ONR recognises that limited information is available for estimating human error probabilities at GDA. Often detailed designs are not available and the fundaments to reliable human performance such as HMIs are incomplete and other factors such as procedures, staffing structures and organisational design are beyond the scope of GDA. Accordingly it would be disproportionate and potentially misleading to use a method which requires a detailed consideration of all these factors at this stage.

340. SPAR-H provides two baseline human error probabilities for undertaking an assessment. One baseline is the probability of error in decision-making whilst the other is error probability during the execution of actions. Consistent with other methods, decision-making is considered less reliable than the skill-based execution of actions. However, these baseline probability estimates are derived by taking an

average from a range of more precisely described probability estimates that are provided in the THERP method (I return to this feature later as it has been the subject to modification by Hitachi-GE).

341. The analyst selects an appropriate baseline and modifies this using PIFs. In this method, modifiers can improve or degrade the baseline probability. This modification is achieved by the PIF multiplying the baseline probability. The chosen multiplier for each PIF is selected based upon a corresponding qualitative description that constitutes part of a scale. If the effect of the PIF is neutral, i.e. it neither improves nor degrades the error probability then the PIF multiplier is 1 and the baseline probability remains unaffected by that PIF.

342. The following PIFs are included in the SPAR-H method:

- Time Margin
- Stress
- Complexity
- Experience/Training*
- Procedures*
- Sufficiency of Human – System Interface Design
- Fitness for Duty*
- Work Processes*.

343. The PIFs marked with an asterisk address factors that are beyond the scope of GDA and are therefore, I consider, appropriately excluded from the Hitachi-GE assessments. However, as the detail associated with these factors becomes available post-GDA, the licensee will need to revisit the HRA and determine their impact.

344. In addition, where assumptions were made for the purposes of GDA, the impact of any later invalidated assumptions will need to be considered. These assumptions/exclusions were recorded in the Hitachi-GE assumptions log for onward transmission to the future licensee. E.g. “Comprehensive list in GDA for requirements and assumptions to be transferred to operating regime, XD-GD-0049, Revision 1, September 2017” (Ref. 71).

345. I have compared the PIF multipliers with those of the original SPAR-H method. I note that maximum multiplier for stress has been changed (Ref. 25). This has been done by adding a further qualitative anchor point to the stress scale. Accordingly, the previous maximum multiplier was associated with ‘high stress ‘and it is now associated with the descriptor ‘Extreme stress’. Given the levels of uncertainty and qualitative information at GDA I consider this change appropriate.

346. When compared with the original THERP method, the inclusion of the SPAR-H PIFs provides a wider and more precise scope for modifiers to baseline reliability estimates than those contained within THERP. I consider this to be an enhancement because it ensures a wider consideration of qualitative factors that can affect human reliability outcomes.

347. Returning to the baseline multipliers, Hitachi-GE has reverted to the use of the THERP baseline multipliers that are contained within that method. These are more precisely defined by qualitative description than the SPAR-H method.

348. Within THERP, baseline multipliers of five fundamental classes are provided for the probability of:

- Making an error of detection or diagnosis;
- Omitting a procedural step;
- Omitting a required action;

- Executing a required action erroneously;
- Interacting with a different control or display done that required to be used.

349. Within each class, different probabilities are provided according to the characteristics of the task and/or the interface device with which an interaction is required.

350. I am satisfied that the Hitachi-GE reversion to the THERP originating baseline data averaged in the SPAR-H method is appropriate.

351. One weakness I note is that Hitachi-GE has not addressed the fact that the THERP and SPAR-H databases are drawn operational data based on traditional analogue panel based HMIs. The UK ABWR design uses both panel and screen based HMIs which means that the databases from current HRA methods may not be fully appropriate. This is not unique to Hitachi-GE and has been an issue on every GDA to date due to the paucity of human reliability data on human-computer interaction.

352. In previous GDAs, this issue has been mitigated by taking into consideration the output from simulator and ISV trials. This is not an option for Hitachi-GDA given the relative maturity of the MCR. Thus a future licensee will have to specifically consider the impact of screen based interfaces on human reliability post-GDA.

353. To conclude, Hitachi-GE could have simply used either the THERP or the HEART technique – both are recognised techniques in GB. However, it has attempted to address some of the methodological constraints in both these methods, and has developed a method that should offer a better estimate of human reliability, ultimately leading to a better PSA.

354. I judge that the approach adopted Hitachi-GE has its merits, and the logic behind the modifications to be sound. To provide a measure of independent validation of this method, I used an independent consultancy to re-model a sample of Hitachi-GE derived HEPs, which used a hybrid method. The consultancy found that the HEPs were sufficiently similar to those calculated using traditional methods. There was certainly no unfounded optimism in the data identified. I thus consider that the basic tenets of SAPs AV. 2 and AV. 3 to have been met; the Hitachi-GE output shows reasonable validation against existing methods and the underpinning analysis adequately captures the factors that determine the human reliability probabilities. However, I note the need for further work in this area post-GDA to consider the impact of screen based interactions on the HRA.

Dependency modelling

355. Dependency considers the extent to which a human error in one task might or will influence the probability of error in another. ONR expects that dependencies between human actions must be accounted for to avoid underestimation of risk. The potential impact of dependency between separate activities (either by the same or by different persons) should be assessed (Ref. 14).

356. Hitachi-GE initially incorporated HFEs into PSA models as independent events. However, to analyse the dependency between HBSCs, Hitachi-GE then identified cut-sets with the greatest contribution to risk, and reviewed them against a set of dependency factors:

- Are the actions for each HFE carried out close in time?
- Are the actions fulfilled with similar tasks?
- Are the same cues used to prompt the actions of each HFE?
- Are the actions carried out by the same personnel?

357. This list was derived from various US NRC NUREG documents which discuss the qualitative modelling of human dependency. I consider these encapsulate good practice.

358. However, there are other sources of HF dependence and Hitachi-GE has taken the above factors and expanded upon them to include the dependency factors within the THERP HRA method. These include for, for example, higher tier contingent actions (e.g. the same mind-set affecting HFEs associated with the same higher level safety function). Again I consider this to be good practice.

359. From these considerations, Hitachi-GE derived judged levels of dependence which were translated into a conditional probabilities using dependency calculations contained within the THERP method; again, this constitutes good practice.

360. Other human factors exist that can affect judged levels of dependence. These factors stem from: training, procedures, crewing structures and organisational design etc. These are beyond the scope of GDA but I would expect a future licensee to revisit assessed levels of dependency during updates to the HRA/PSA.

361. Hitachi-GE has systematically included initial diagnostic HFEs within its PSA models. It has described these as “cognitive common cause failures”. I have examined the evaluation of these failures and I find that they properly recognise the detection of an initial cue or cues that prompt the need for subsequent functions to be completed, the failure of which I represented by HFEs in a sequence.

362. Also included is the consideration of the error probability for failures in confirmation that a situation does exist where functions need to be fulfilled. In consultation with my PSA specialist assessor colleagues, we concluded that these failures have been suitably incorporated within PSA models as so-called “higher tier contingent failures”. I consider that Hitachi-GE has followed RGP in the identification and assessment of human dependencies.

363. I conclude that Hitachi-GE has adequately represented issues of potential human dependency, within, and between, HFEs. It has also taken account of common cause failures (failures that could affect multiple HFEs).

364. In the light of the inevitably limited HF information available during GDA, the estimation of the human contribution to risk due to dependency is somewhat conservative. Despite this, I note that the estimated human contribution to risk remains acceptably low.

Quantitative Human Reliability Assessment

365. ONR expects that human reliability analysis is performed for all human actions that are necessary for safety (SAP EHF.10). It also expects that best-estimate data have been used, or where this is not practicable, that suitable conservatisms have been used in lieu (Ref. 14).

366. This section focusses on whether Hitachi-GE has appropriately and proportionately applied its HRA method to produce HRA data that is suitably best-estimate, taking account of the design and licensee operation / arrangement uncertainties.

367. The interface between the Hitachi-GE HRA process and each PSA model is called a Human Failure Event. A HFE describes the human-failure associated with the failure to deliver nuclear safety function. For example, “Failure of manual operation of RHR”. In order to manually operate RHR, a number of discrete tasks are required to be successfully completed if RHR is to operate successfully. Failure of a subtask equals failure of the HFE. Therefore, a HFE comprises a number of human error

assessments and considers the probability of failure for each of the relevant constituent tasks (i.e. HEPs).

368. HFEs thus present the aggregate reliability for the task set. HEPs present the probability of error for a given task within a particular functional set.

369. I have scrutinised a sample of HFEs as they have become available (e.g. Ref. 65) and find that they consistently identify the constituent tasks that need to be assessed for error probability. In general terms I observe that the pattern of a qualitative HFEs consists of the following:

- The detection or recognition of alarms indicating a need to do something;
- Confirming that what is believed to have been detected is valid;
- The formulation of the decision to act, based upon available user interface indications and procedural instructions;
- Undertaking the, almost invariably more than one, necessary action(s);
- Checking the success (or otherwise) of one or more actions;
- Checking the overall functional success (e.g. getting RHR working);
- Consideration of any subsequent diagnosis or actions necessary to recover any errors or failures revealed by the cheque that have been made.

370. In my scrutiny of task analyses I have found all of these tasks have been considered in each human failure event. This has been achieved by Hitachi-GE applying a consistent pattern as above.

371. In order to assess whether estimated human reliabilities for HFEs are suitably best estimate, it is necessary to consider how qualitative HF information has been identified or captured by task analysis and the process by which that is translated into a human error probability.

372. As discussed in sections 4.2 and 4.3, I have scrutinised Hitachi-GE's qualitative analysis methods and the results and consider they provide sound basis to underpin any quantitative analysis. The methods provide detailed analytical insights into those factors that negatively affect human reliability.

373. To inform my judgement on the reliability of Hitachi-GE's HRA method and its application, I secured the services of specialist technical support in the area of HRA to perform an independent review. The purpose of this review was to confirm that the method was sound and that the output was suitably 'best-estimate'. I also sought confirmation that 'best-estimate' was suitably conservative given the uncertainties relating to design maturity and assumptions relating to future operation and licensee arrangements. The results of this independent review are presented in Reference 70.

374. The independent review comprised the re-modelling of a selection of HEPs using an alternative HRA methodology (HEART). The review was constrained by the phased delivery of safety case documents containing the HEP models.

375. The review attempted to sample based on:

- Selecting actions from the different PSAs,
- Selecting a mixture of both risk significant and risk insignificant HEPs.
- Selecting actions to cover a wide range of HEP values (from 5.5E-04/demand to 2.37E-01/demand).
- Selecting a broad range of the different operator tasks (e.g. initiating systems, manual injection, and manual shutdown).

376. The application of these criteria resulted in 12 discrete HFEs being re-modelled using the same qualitative input data, as used in the original Hitachi-GE analysis. These HFEs spanned the following PSAs:

- At power,
- Shutdown,
- Spent fuel pool.

377. The results of this re-modelling exercise are summarised in table 2 below. The table provides direct comparison between the HEPs derived by Hitachi-GE's SPAR-H / THERP hybrid method and those calculated independently via the HEART method.

Table 2 - Comparison between HEPs derived by Hitachi-GE HRA method and the HEART method.

No.	Human Failure Event	Description	THERP/SPAR-H HFE (/demand)	HEART HFE (/demand)
1.	[redacted]	[redacted]	[redacted]	[redacted]
2.	[redacted]	[redacted]	[redacted]	[redacted]
3.	[redacted]	[redacted]	[redacted]	[redacted]
4.	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
6.	[redacted]	[redacted]	[redacted]	[redacted]
7.	[redacted]	[redacted]	[redacted]	[redacted]
8.	[redacted]	[redacted]	[redacted]	[redacted]
9.	[redacted]	[redacted]	[redacted]	[redacted]
10.	[redacted]	[redacted]	[redacted]	[redacted]

11.	[redacted]	[redacted]	[redacted]	[redacted]
12.	[redacted]	[redacted]	[redacted]	[redacted]

378. The two sets of HFE data in table 2 show reasonable correlation at the order of magnitude level. A bigger sample size would have provided greater confidence, but the size was limited by availability of both technical support resource and Hitachi-GE derived HEP data.

379. The TSC notes that the task times proposed by Hitachi-GE appeared to be conservative, and in some cases several conservative assumptions were compounded to result in a significantly conservative assessment. Whilst the PSA, and therefore the HRA, should be best estimate, the results of the TSC assessment provides confidence that the risk contribution from operator actions in the PSA is conservative, and that refinement could be achieved in the site specific phase.

380. This supports the finding in ONR PSA assessment report that the documentation does not provide sufficient clarity on the timing estimates for operator actions. I am not concerned over this for GDA as the timings appear conservative* rather than optimistic but consider it will be a necessary update by the future licensee. *Excluding those associated with evacuation – subject of assessment finding AF-ABWR-RP-08 (Ref. 78)

381. A further minor finding from of the independent assessment was that the supporting material for the HEPs was not always particularly cogent and coherent in its presentation. I agree with this point and note the same in section 4.3. It is something that I would expect a future licensee to address as submissions at the 'evidence' level are updated to reflect future design changes and validation of licensee assumptions. I would expect a clear link between the claim and the evidence, i.e. a clear statement within each basis of safety case document or analysis report that sets out what HBSCs are being substantiated and how. Then a clear conclusion that demonstrates that the HBSCs is substantiated, i.e. those factors that could potentially make the HBSC unreliable have been assessed and shown to be optimised.

382. However, I do not consider this to prejudice the findings of my assessment and is issue of clarity rather than a fundamental failing.

383. Based on this comparative review I can conclude the following:

384. The re-modelled HFEs provide confidence that the task analysis methods deployed by Hitachi-GE have effectively identified performance shaping factors.

385. The close correlation between the Hitachi-GE HFE data and that calculated by the HRA specialist provides confidence that the HFE data used in the PSA is suitably best-estimate – taking into account the uncertainties associated with GDA.

386. Based on the position that:

- all key HBSCs appear to have been identified and are represented within the appropriate PSAs (See sections 4.3 and 4.4),
- HFE/HEP data has been shown to be 'best-estimate',
- human-dependency modelling appears sound (See Step 4 PSA Assessment Report).

387. I can be confident the human contribution to risk is well understood by Hitachi-GE – as far as can be reasonably practical within limitations of GDA.

388. I note that the PSA and HRA remain work in progress at the close of GDA and therefore expect a future licensee to update both accordingly as the design matures and assumptions regarding operations and arrangements become confirmed.

Human Contribution to Risk

389. Given the lack of maturity of both the PSA and the UK ABWR design at the start of Step 4, I have focussed my attention on the Internal Events at Power (IEAP) Level 1 PSA (events that lead to core damage) in an attempt to understand the human contribution to risk. Given that core damage can lead to large release fractions and ultimately off-site release, I consider this appropriate for GDA.

390. Reference 72, Topic Report on the IEAP Level 1 PSA, reports the top 10 human based risk contributors to core damage frequency (CDF) for both Type A (Maintenance) errors and Type C (Post fault recovery) errors.

391. An important measure of the risk contribution from either the human or the technology is the measure of Risk Achievement Worth (RAW). RAW measures the amount the total risk would increase if the human or technology were to definitely fail on demand.

392. Obviously there is artificiality to this concept, as people and technology are far more reliable than this. However, it is a useful indicator that shows the relative importance of HBSCs or equipment with respect to their contribution to overall risk.

393. Tables 3 and 4 below show the top ten and top eleven RAW value listings for the Type A and Type C HFEs. One would not expect to find Type B errors for at power operations due to the high levels of protection afforded a modern reactor design. Type B errors are present within the shutdown PSA but were outside the scope of my assessment. I expect a future licensee to revisit this process post-GDA as the design evolves and licensee specific information becomes available.

394. These data show that the UK AWBR design appears well protected from human error during fault conditions. It supports the deterministic claims that:

395. "*Regarding the manual operation necessary to be performed by the operator, appropriate and sufficient time for that operation is considered. In any case, it is conservatively assumed that no operator action is taken for a period of 30 minutes following any initiating event". (*Ref. 73 - PCSR Chapter 24)

396. The UK ABWR fault schedule (Ref. 74) also shows that: for reactor faults from power operations, design basis safety claims of reactivity control and (short term) fuel cooling functions can be delivered by automatic SSCs.

397. ONR's fault studies assessment (Section 4.3.6) (Ref. 75) considered these claims within its scope and concluded that: "*The necessary operator actions will need to be substantiated once these are developed, and I would expect the thermal hydraulic analysis discussed above to be reviewed or repeated to demonstrate that the procedures are effective. However, I consider this to be all part of normal business for site licensing. For the purposes of GDA, it is my judgement that sensitivities illustrate that there is plenty of time to perform the necessary actions, and substantiating them in the future should not be a problem."*

398. The highest contributing HFE (HFE-DF-TR) during fault recovery accounts for a 97% increase in total risk if it completely fails; in PSA terms, 97% is a small contribution as risk increase / decreases are often measured in hundreds or thousands percent increase. I was able to compare the RAW values for these HFEs against previous reactor designs that have passed through GDA and note that they are comparable.

399. Conversely, these data do show that, in risk terms, the biggest human contribution to risk for the UK ABWR design lies in the area of EMIT for those SSC that provide post fault protection. This is typical of all highly automated plants as EMIT errors, if undetected, can result in the failure to actuate on demand. In contrast to the Type C risk contribution, the highest type A HFE increases overall risk by 8200% if it fails. Whilst significantly higher than that for the Type C HFEs, it also comparable with contemporary reactor designs. This is due to the simple fact that modern designs employ technological solutions to provide active (and passive) protection against design basis faults. If the technology fails, then the onus is on the operator to recover from the fault. The operator is the final remaining barrier.

400. In the case of the UK ABWR, the operator actions required if the technology fails are typically quite simple in nature; if important in risk terms.

Table 3 Top eleven RAW Pre-Initiator HFEs (Ref. 72)

Rank	Human Failure Event	Risk Achievement Worth	Description
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			

Table 4 Top ten RAW Post-Initiator (Type C) Human Failure Events (Ref. 72)

Rank	Human Failure Event	Risk Achievement Worth	Description
1.	[redacted]	[redacted]	[redacted]
2.	[redacted]	[redacted]	[redacted]
3.	[redacted]	[redacted]	[redacted]
4.	[redacted]	[redacted]	[redacted]
5.	[redacted]	[redacted]	[redacted]
6.	[redacted]	[redacted]	[redacted]
7.	[redacted]	[redacted]	[redacted]
8.	[redacted]	[redacted]	[redacted]
9.	[redacted]	[redacted]	[redacted]
10.	[redacted]	[redacted]	[redacted]

401. I judge that the current HRA supplemented by the internal hazards PSA refinement and the IEAP sensitivity analysis to reflect the most recent HRA values is sufficient to support the UK ABWR PCSR

402. My assessment, supported by the TSC review (Ref. 70), provides confidence that methodology selected for the HRA and its implementation meets most of the expectations in ONR's HRA TAG, with well documented task analysis and structured methods for dependency identification.

403. From the risk contribution data, I can conclude – noting the maturity of the PSA and design – that the UK ABWR is comparable to other contemporary reactor designs with respect to human contribution to risk.

404. I consider that the RAW values for Type A errors highlight the importance of providing robust substantiation of human actions relating to EMIT activities on nuclear important SSC. As discussed above in previous sections, the consideration of HF in the design of plant systems has been limited by design maturity in these areas. I consider this a matter of importance for a future licensee to progress in relation to both design and safety analysis.

Conclusion to Section 4.4

405. I judge that Hitachi-GE has developed a suitable method for the quantification of HEPs for GDA noting the maturity levels of the design. The method is based on existing methods and attempts to address some of the limitations of both. Via independent confirmatory analysis, I consider that the method used was suitable for GDA producing appropriately conservative HEP data. Hitachi-GE has also used established RGP for the modelling intra-HFE dependencies.

406. I judge the scope of the HRA presented by Hitachi-GE to be adequate for GDA. HFEs are appropriately captured in the Level 1, 2 and 3 PSAs. Operator actions are considered in Level 1 and 2 comprising detailed logic models. Level 1 and 2 are 'linked', which allow human-dependencies to be considered. All modes of operation are considered, along with fuel route and the most significant hazards. All types of HFE are appropriately considered (Type A, B, and C). The underpinning task analysis is suitably descriptive and contains sufficient information to substantiate the claims within the limitations of the information available at GDA.

407. However, the methods used do not adequately address the modelling and quantification challenges associated with the use of human computer interaction – of which no suitable method is currently validated. I expect a future licensee to develop the HMI in parallel with method/s to model and quantity the interactions between the operators and the major control interfaces.

408. To conclude, I consider it will be necessary for a future licensee to update the HRA as design, operation, and arrangements detail becomes finalised. The ONR PSA assessment originated assessment findings relating to the need to update and maintain the PSA in the future bound this requirement (e.g. AF-UK-ABWR-PSA-001)

Design of Human Machine Interfaces

Main Control Room

409. The MCR is the principal mechanism through which personnel interact with and control the plant. It provides the facilities for this interaction in the form of instrumentation, displays, alarms and controls. It supports the delivery of nuclear plant safety functions related to detection, diagnosis, decision-making and action. It also needs to provide a habitable environment during all design basis events, to ensure that any safety-important human actions can be performed reliably. Habitability is discussed in section 4.6.

410. The ONR SAPs relating to the design of control rooms establish the following guidance:

- "Suitable and sufficient safety-related system control and instrumentation should be available to the facility operator in a central control room, and as necessary at appropriate secondary control or monitoring locations." (ESR.1)

- "The systems should provide for control, monitoring and data recording in normal operations, fault conditions and severe accidents. The extent of these provisions should be consistent with the fault analysis and justified in the safety case." (Para 778, EHF.7)

- "The user interface should:
  a) provide sufficient, unambiguous information for the operator to maintain situational awareness in all operating modes and in fault and accident conditions (e.g. the behaviour and status of the automated plant control systems);

b) provide a conspicuous early warning of any changes in parameters affecting safety;
c) provide a means of signalling safety system challenges and of confirming that the safety system has initiated and achieved its safety functions;
d) support effective diagnosis of plant deviations; and
e) enable the operator to determine and execute appropriate actions including those needed to overcome failures of automated safety systems or to reset a safety system after its operation; and
f) support communication between personnel located in the same or different operating locations, including locations external to the facility or site.

411. To meet the requirements of applicable C&I design codes (e.g. International Electrotechnical Commission standards), Hitachi-GE elected to redesign the UK ABWR C&I architecture part way through the GDA process. This required the implementation of new diverse technologies for controlling functions important to safety, and physical separation of different C&I platforms and systems of different safety classification.

412. As a result of these changes, there was a requirement to modify existing and design new diverse HMIs to allow required manual functions for monitoring and control to be undertaken on the new or newly separated systems (Ref. 76).

413. Due to this redesign, Hitachi-GE were only able to present outline designs for the:

- Main control room,
- Remote shutdown room,
- Backup building
- Alarm system

414. These locations contain HMI matched to the classification and requirements of the C&I equipment that is being controlled. The HMI maintains independence between C&I systems, and avoids influence of lower class systems on higher class systems. I judge this to be adequate.

415. This has resulted in an MCR design which is predominantly based on the J-ABWR design at the functional level but with UK specific additions / modifications; although these additions typically replicate functionality for diversity/segregation reasons. The UK specific additions comprise:

416. The extension of the Main Control Console (MCC) to accommodate the Safety Auxiliary Control System (SACS). This functionality was embedded in the System Logic and Control System (SSLC) for the J-ABWR, but they are separated for the UK ABWR, to comply with the requirements of the C&I SPC on segregation of systems of different Safety Classifications.

417. The Hard-Wired Back-Up Panel / Hard-Wired Back-up System, Safety Auxiliary Panel and the Backup Building Control Panels / Severe Accident C&I are newly designed for the UK ABWR.

418. Touchscreen soft switches, which are used on the J-ABWR, are replaced by an on-screen command that is actuated by a hardware-based input device for Class 1 digital HMI.

419. Hitachi-GE has not been clear with respect to exactly what level of similarity exists at the detailed interface level and has not been able to demonstrate that the baseline J-ABWR MCR design benefitted from a HFI programme (Ref. 38).

420. However, I can confirm that Hitachi-GE has taken cognisance of international BWR OPEX when evolving the UK design (Ref. 38).

421. Hitachi-GE undertook a comprehensive facility wide gap analysis to identify where the J-AWBR baseline design had HF deficiencies relative to modern HF standards and UK regulatory expectations. The identified gaps and recommendations are summarised in the "Baseline Human Factors Assessment Report", (Ref. 24). I have sampled the sentencing of these gaps and can confirm that they have been suitably sentenced by the HF work programme (Ref. 38)

422. Supplementary to the review of OPEX, Hitachi-GE also performed an analysis of the facility J-ABWR baseline design allocation of function (using NUREG 3331). This analysis evaluated "*264 functions. As a result of AoF analysis, the number of functions assigned to Automatic was 166 and the number assigned to Manual was 98. Of the 98 that were manual, most were supporting functions for systems that were safety-related (i.e. identified within the safety case as making a contribution to safety by not necessarily UK Class 1 or 2 SSCs, claimed directly in the design basis safety case), but where the manual functions were not themselves safety-related. In addition, some of the automatic functions were actually "sequential" automation, where the human acts as "supervisor" to direct the start or continuation of operations, but with the repetitive or complex elements being performed automatically by the system. This ensures there is continued situational awareness and that the operator maintains a sense of responsibility for the plant, without burdening the operator in ways that are not optimal for overall effective and safe plant performance.*

The AoF analysis identified there were fifteen functions where the allocation had changed from the baseline design or where new functions were planned for UK ABWR. As a result of existing allocation of the reference plant design functions and additional considerations through the UK ABWR AoF analysis, the overall automation level during the initial fault and accident sequences analysed in GDA is almost complete automation, with back-up safety functions also allocated to the technology. The operator in UK ABWR maintains an alert monitoring role and has specific functions that are related to acting as a "supervisor" for the plant equipment and providing control when more dynamically flexible responses for operational functions are needed within normal plant conditions." (Ref. 35). The output of this report, and previous iterations, closed RO33 (Ref. 38).

423. It is thus possible to summarise that the UK ABWR functional design has a sound allocation of function basis and has used OPEX to inform the design, which should underpin reliable human performance as the design progresses.

424. Noting the outline nature of the MCR design detail, Hitachi-GE, has performed a series of V&V activities to test and evaluate the MCR performance to ensure that the "overall layout, the functionality and the feasibility of developing a fully detailed design are specified and assured" (Ref. 76).

425. These activities include (Ref. 17 and Ref. 76):

- Trials using experienced NPP operators (Japanese and UK) performing a sample of risk important HBSCs in a static mock-up of the MCR. The mock-up being constructed to adequately depict the layout, size, shape and inventory of each element of the HMI: WDP, MCC, SAuxP, HWBPs and RSPs – all of which were exercised in the trials.
- Computer Aided Design based analysis of the anthropometric elements of the MCR (e.g. sightlines).
- Link analysis of interface element layout designs.
- Early input and review of the functional display layouts

426. The output of these activities did not identify any significant HFE deficiencies with the MCR design and associated interfaces (Ref. 17). Based on the available information, I can conclude that: user testing to date and Hitachi-GE's material submitted as part of the RO-0069 closure, has revealed no major operability concerns with the C&I platform. Workload appears to be broadly acceptable within the main control room. The interface designs in the main control room, and by extension other locations where the HMI is replicated, are control failure tolerant; that is, the operators can clearly detect control system failures, and in the event of failure, a smooth transition between interfaces can be achieved with minimised task disruption.

427. Hitachi-GE "*aims to present a generic plant design that will, without any further major design changes, eventually be able to be licensed in the UK. However, it is not intended to result in a fully detailed design that is able to be constructed. Further design development and safety analysis iterations are required to arrive at a design that is suitable and approved to be built at a particular UK site. As such the design maturity at the end of GDA is that of "basic" design, where the overall layout, the functionality and the feasibility of developing a fully detailed design are specified and assured*" (Ref. 76).

428. Given this aim, my above conclusions, and the statement that further design development and iterations will be required prior to build, I consider that the design of MCR is suitably HF informed given that it is under design evolution. I have consulted with the ONR C&I Specialist and I am content that there is sufficient contingency in the MCR design to provide assurance that HMI design options have not been foreclosed. However, it is important to note the significant amount of additional design and evaluation required of the UK ABWR MCR and other risk important interface designs before they will be sufficiently substantiated for nuclear operations.

Basic Layout

429. Hitachi-GE states that the UK ABWR MCR has minimal layout differences between the reference Japanese design. These difference comprise:

- The functions to be implemented in the Safety Auxiliary Control System (SACS) for the UK ABWR were embedded in the Safety System Logic and Control System (SSLC) for the J-ABWR, but they are separated for the UK ABWR, to comply with the requirements of the C&I SPCs on segregation of systems of different Safety Classifications,
- The Hardwired Backup Panel / System (HWBP/HWBS), Safety Auxiliary Panel (SAuxP) and the Backup Building Control Panels / Sever Accident (BBCP/SA) C&I are newly designed for the UK ABWR, and
- Touchscreen soft switches which are used for the J-ABWR are replaced by on-screen commands which are actuated by a hardware-based input device for Class 1 digital HMI.

430. The ABWR design has benefitted from OPEX from an existing fleet of reactor designs, which have offered insight into the operability of the MCR; as reported in the HF Baseline Assessment Report (Ref. 24). Hitachi-GE took this insight, differences in GB regulatory expectations, differences between GB and Japanese user populations and conduct of operations and used it to inform the UK ABWR C&I design.

431. The User Interface Strategy Report (Ref. 39) provides the demonstration that alternative HMI's are available when the first choice HMI is not. I judge that it provides sufficient evidence to show that the basis for choosing an alternative interface are

logical and consistent, when the HMI of first choice or that currently being used is not available. This is presented in the form of an logic flowchart showing how transfer to a different HMI(s) will be undertaken. The scope of the description includes HMIs within the MCR and the use of HMIs for fall-back positions when relocation becomes necessary.

432. Failures of HMI systems can be complex and their manifestation not obvious, however Hitachi-GE has shown that cues are available for the loss of a single control or display and also for systemic HMI failures.

433. Hitachi-GE has undertaken a series of well-structured trials involving experienced nuclear power plant operators both to test the usability of the overall MCR layout, and the usability of particular user interfaces within it. The trials have progressed from gathering initial opinions from experienced NPP operators on proposed panel layouts, through to simulating post fault scenarios with video and text recording. This has provided a level of HF integration into design which I judge acceptable for GDA. I am thus content that basic layout is unlikely to change between GDA and licensing.

Class 1 Flat Panel HMI Development

434. During Steps 2 and 3, ONR identified that Hitachi-GE intended to use lower classification HMI to support human interactions with Class 1 safety systems. The function of this HMI is to undertake routine surveillance and testing of Class 1 safety systems.

435. ONR advised Hitachi-GE to assess the impact of the failure of the lower Class MCR HMI systems on the plant Class 1 safety systems. In performing this assessment, Hitachi-GE identified the need for a Class 1 HMI.

436. A lower integrity design of HMI already exists on the Japanese ABWR for undertaking the necessary surveillance and testing. This consists of a human computer interface with a flat panel screen that has been shown to be operable in practice. Therefore, Hitachi-GE has a strong motivation to maintain the levels of usability afforded by that pre-existing but lower integrity user interface. In meeting class 1 requirements, the design uses Field Programmable Gate Array (FPGA) technology.

437. A number of interaction methods, suitable for implementation in FPGA technology, were trialled by Hitachi-GE to evaluate the most suitable interaction methods. An eight person trial was performed to test and evaluate alternative design options for navigating between display pages and interacting with on-screen controls.

438. I, along with my C&I colleague, assessed Hitachi-GE's submissions (e.g. Refs 29, 45, 46, and 48) in this area. I am satisfied that the usability trials were undertaken have identified an adequate design option based on the J-ABWR design requirements. The requirements remain in development. I consider that Hitachi-GE has done enough in this area to support the completion of GDA. However, I note the necessity of the future licensee continuing with this work to arrive at an optimised and usable solution; one that works in concert with other interface types contained with the control room.

Alarm Design

439. An alarm is an automatic visual or audible indication to personnel of when a specific plant variable or condition has reached a pre-set limit or state. There are multiple SAPs which address the use of alarms, but for brevity, these can be summarised as the need for them to be suitable and sufficient. Reference 77, EEMUA publication 191, usefully defines what suitable and sufficient is with respect to alarms and ONR consider it to be RGP in the development of alarm systems. I welcome that Hitachi-GE has used this reference to inform the design of the UK ABWR alarm system.

440. EMUA set out five key design principles:

- Each alarm should alert, inform and guide.
- Every alarm presented to the operator should be useful and relevant to the operator.
- Every alarm should have a defined response.
- Adequate time should be allowed for the operator to carry out the defined response.
- The alarm system should be explicitly designed to take account of human limitations.

441. It also defines the characteristics of a good alarm:

- Relevant
- Unique
- Timely
- Prioritised
- Understandable
- Diagnostic
- Advisory
- Focussing

442. These principles and characteristics have guided my assessment.

443. Hitachi-GE's principal submission regarding the UK-AWBR alarm system is Reference 46. It describes the method to be used to develop the MCR and supporting HMI alarm systems. It provides a proof of principle that the intended Hitachi-GE alarm rationalisation will be effective.

444. Hitachi-GE has measured the difference in the number of alarms that would be displayed following a normal reactor scram without and with rationalisation. The scope of the document is limited to this one scenario. For this purpose the defined alarm population is taken from the Taiwanese ABWR, because the alarms within this population are described in English.

445. The report describes an alarm rationalisation process, described as a logical flow chart that follows the RGP given in EEMUA 191.

446. As a means of illustrating the effectiveness of the rationalisation process, Hitachi-GE has depicted the number of alarm tiles that would be illuminated on the Japanese ABWR alarm interface for reactor scram without and with rationalisation. The rationalisation process saw a ~ 90% decrease in discrete alarms.

447. I have scrutinised the basis for the proposed Hitachi-GE rationalisation process and am satisfied that it follows the RGP given in EEMUA 191. In addition, the setting out of the decision-making process within a logical flowchart gives me confidence that the process will be well controlled and repeatable across different individual alarms and across potentially multi alarm scenarios. I cannot comment on the adequacy of the Alarm HMI design at this stage as it is not sufficiently developed. However I see no limitations in what has been shown so far that could foreclose on future design options.

448. The proof of principle demonstration applied to a normal reactor post scram situation is a logical starting point for a future process that must be continued. I consider that the Hitachi-GE report forms a sound basis for that continuation of process. However, a future licensee will need to further develop the alarm system until it can be proven that it is fit for purpose. My C&I colleague has raised an assessment finding in this area.

449. AF-ABWR-CI-017: In GDA, Hitachi-GE provided outline information describing alarms. ONR's expectation is that as more detailed design information becomes available the design is adequately substantiated, in particular considering claims and engineering requirements. The licensee shall:

- Identify the engineering requirements for each alarm considering appropriate factors (such as impact on risk, aversion to alarm flood, fault detection, HF).
- Justify the adequacy of the alarm design against the requirements (including the use of normally open or normally closed contacts), considering RGP in the UK and relevant guidance.

Remote Shutdown System Room

450. There are two Remote Shutdown System Room (RSSRs) each controlling a separate safety division. These are located in different rooms that are separate safety divisions but located next to each other.

451. The purpose of these rooms is to provide the capability to shut-down the reactor outside of the MCR and provide the ability to monitor critical safety function parameters important for accident management. However, they share similar HMI technology to the MCR.

452. The principal HMI in these rooms is the Remote Shutdown Panel (RSP) which provides the functionality to bring the reactor form a hot shutdown state to a cold shutdown state following an automatic or manual reactor scram.

453. Hitachi-GE have systematically identified the safety functional claims for the RSP and the C&I systems necessary to meet them. The claims comprise:

- FSF2 – Fuel cooling,
- FSF3 – Long term heat removal,
- FSF5 – Others (including the monitoring of key plant parameters).

454. The RSP interfaces with the Residual Heat Removal (RHR), High Pressure Core Flooder (HPCF), Reactor Core Isolation Cooling (RCIC) and Nuclear Boiler (NB) systems, plus their required water supply and electrical power supply supporting systems, including the Emergency DGs (EDGs).

455. At the close of GDA, the RSP design had not been finalised and thus not validated. It is an area that the future licensee will need to progress post-GDA.

456. Hitachi-GE stated that it anticipates that "the operators will be provided with an alternate control for manual reactor scram along the access route to the RSSRs or within the RSSRs themselves." (Ref. 18). It will be necessary for a future licensee to validate this assumption.

457. Whilst I have not been able to gain sufficient confidence that the RSS / RSP design meets RGP with respect to HF informed layout, I do have confidence in Hitachi-GE's design and testing process. I expect that the design of the RSS / RSP will follow the same or equivalent process and guidance as that used for the MCR so I do not consider this lack of maturity to be sufficient to prejudice the closure of GDA. I also consider there is sufficient scope within the layout to accommodate any necessary changes.

458. Given the immature nature of the RSS / RSP design for GDA, ONR will pay particular attention to this area post-GDA to ensure that the licensee develops a safe and operable design solution.

Backup Building Control Panel Room

459. The Backup Building Control Room (BBCR) provides a remote location which provides monitoring and functionality from the Backup Building Control Panel (BBCP) to support the following safety function claims:

- FSF2 – Fuel cooling: Alternative means using the Flooding System of Specific Safety Facility (FLSS), Reactor Depressurization Control Facility (RDCF),
- FSF3 – Long term heat removal: Through the Filtered Containment Venting System (FCVS),
- FSF4 – Confinement/Containment of radioactive materials: Using FLSS, and
- FSF5 – Others: Especially the monitoring of key SA plant parameters during accidents.

460. Hitachi-GE have systematically identified these safety functional claims and the C&I systems necessary to meet them.

461. At the close of GDA, the BBCR/BBCP design had not been finalised and thus not validated. It is an area that a future licensee will need to progress post-GDA as part of the evolution of the HMI.

462. Whilst I have not been able to gain sufficient confidence that the BBCR/BBCP design meets RGP, I do have confidence in Hitachi-GE's design and testing process. The design of the BBCR/BBCP design will follow the same process and guidance as that used for the MCR so I do not consider this lack of maturity to be sufficient to prejudice the closure of GDA. The safety functions are identified and there is sufficient contingency to accommodate the design evolving post-GDA.

463. Given the immature nature of the BBCR/BBCP design for GDA, ONR will pay particular attention to this area post-GDA to ensure that the licensee develops a safe and operable design solution.

Conclusions to Section 4.5

464. It is clear that the design of the principal HMIs for the UK ABWR is immature at the close of GDA. This limits the conclusions that can be drawn with respect to the role of the HMI in substantiating HBSCs in these locations.

465. Based on my assessment described in this and other sections I can conclude the following in relation to the principal HMIs on the UK ABWR:

- The process followed for the design to date is adequate (Conclusion of section 4.2).
- The design team are SQEP (Conclusion of section 4.2).
- The codes, standards, and methods used to inform the design are appropriate (Conclusion of section 4.2).
- Whilst I cannot comment on discrete panel design, the basic functional allocation between the human and the technology has been derived logically and appears to meet GB RGP. For example, there are no operator plant intervention claims within 30 minutes of a fault and reactivity control and short term cooling at the start of a fault transient is assumed to be automatic (Conclusion of section 4.3).
- There is indication that operators can adequately detect HMI failures and migrate control to alternative means of control (Conclusion of section 4.3).
- I consider that there is sufficient contingency in the layout and panel and interface sizing to accommodate future requirement that may arise as the design progresses (Conclusion of section 4.5).

466. I expect that the future licensee will continue to develop the principal, and other, HMIs to a state where they can be subjected to formal V&V activities, sufficient to fully

substantiate the HBSCs performed at these locations. I also expect that the future licensee will follow the guidance and methods demonstrated for GDA, or develop equivalents.

467. Whilst not sufficient to prejudice the issue of a DAC due to the judgement that there is sufficient accommodation within the concept HMI and control location designs, the lack of HMI design detail is sufficient to raise an assessment finding in this area. However, I consider that C&I assessment finding AF-UKABWR-CI-001 sufficiently captures the need to develop the HMI to a level where its human-system performance can be fully substantiated. Plant wide HMIs that play a role in nuclear and conventional safety will be a future focus for ONR post-GDA.

Generic Human Factors Engineering

468. This section presents my assessment of the wider factors that affect human performance across the design of UK ABWR. Hitachi-GE's principal reference for generic HF engineering is the Human Factors Engineering Specification (Ref. 34) which synthesises the RGP in this area into a single guidance document.

469. My assessment comprises the following:

- Thermal
- Lighting
- Access / Egress / Evacuation
- Decommissioning
- Examination Maintenance Inspection Testing

Thermal

470. Optimal temperature levels are defined by British Standards (BS) and Charted Institution of Building Service Engineers (CIBSE) guidance. Whilst there is no legal requirement to comply with British Standards, the relevant legislation often draws upon them. British Standards are typically viewed as RGP, which is a consideration in the determination of whether risk is reduced so far as is reasonably practicable.

471. Hitachi-GE has selected the following standard and guidance for control rooms and wider plant thermal environments.

- BS EN ISO 11064-6 Section A2
- CIBSE Guide A

472. The specification for the MCR temperature is presented in the HF engineering specification (Ref. 34). It specifies a winter / summer temperature range of 20 – 24 and 23 – 26 degrees respectively – drawn from the relevant ISO standard 11064-6. However, I consider the summer range to be on the high side as the typically reported comfort temperatures for the UK tend to be around 20-21 degrees. I note within the basis of safety case for the heating and ventilation system (Ref. 84) that the temperature can be controlled down to 20 degrees in normal conditions and 26 degrees in faulted conditions, which spans the reported UK comfort levels.

473. I note that ONR's mechanical engineering assessment of the HVAC system found the system design to be adequate for GDA and recognised that further development of the HVAC system design will occur during the detailed design phase. The assessment raised a number of assessment findings relating to the future development of the system (Ref. 85)

474. I was unable to identify any assumptions with respect to occupancy levels within the HVAC basis of safety case report in relation to the any underpinning thermal

modelling. However, I consider it is appropriate for a future licensee to explore the effects of occupancy on MCR heat-up post-GDA, as the necessary design information becomes available and the mechanical engineering assessment findings are addressed.

475. I consider that Hitachi-GE has provided sufficient confidence that thermal comfort can be maintained within the MCR and RSSR during normal and fault conditions.

Lighting

476. Optimal lighting levels are defined by British Standards, whilst there is no legal requirement to comply with British Standards, the relevant legislation often draws upon them. British Standards are typically viewed as RGP, which is a consideration in the determination of whether risk is reduced so far as is reasonably practicable.

477. Hitachi-GE has stated that the UK ABWR will meet the appropriate British Standards:

- BS EN 12464-1:2011 Light and Lighting – Lighting of Work Places – Indoor Work Places
- BS EN 12464-2:2014 Light and Lighting – Lighting of Work Places – Outdoor Work Places
- BS EN 1838:2013 Lighting Applications - Emergency Lighting
- BS EN 60964:2010 Nuclear Power Plants – Control Rooms – Design
- BS EN ISO 11064-6:2005 Ergonomic Design of Control Centres – Environmental Requirements for Control Centres

478. As Hitachi-GE's specifications are based on British Standards, I consider they meet RGP.

479. I welcome the fact that the UK ABWR lighting system has been classified in accordance with Human Based Safety Claims report (Ref. 65), and received HF input into the design. It is comprised of three systems:

- The SC3 lighting system provides lighting in emergency response areas. These are areas where operators are required to work to support nuclear safety such as MCR and RSSR.

- The non-safety class lighting system provides lighting in normal operations areas such as the Turbine Building.

- The escape route lighting system provides a safe egress route from buildings for site personnel in case of loss of alternating current power. The escape route lighting system is classified as SC3 in emergency response areas and non-classified in normal operation areas.

480. However, I note that I have not seen any lighting analysis or finalised designs for the UK ABWR plant to make a judgement of adequacy. Thus it will be necessary for the future licensee to provide evidence of compliance post-GDA. I do not consider a lack of evidence at GDA to be of sufficient concern to withhold the DAC.

Noise

481. There are two levels of acceptable noise specified in standards and regulations. The first is the legal limit which is defined by the Control of Noise at Work Regulations. Hitachi-GE has stated that its design will comply with these regulations or that it is assumed that the licensee will provide suitable hearing protection as required under its legal duties.

482. The second limits relate to the effects on human performance, and in this case Hitachi-GE has stated that its design will comply with BS EN ISO 11064, which provides limits beyond which communication is affected and distraction likely.

483. I consider these specifications to meet the UK legal requirements. However, I note that I have not seen any acoustic analysis of the UK ABWR plant to make a judgement of whether the plant actually meets these requirements. Thus it will be necessary for the future licensee to provide evidence of compliance post-GDA. I do not consider a lack of evidence at GDA to be of sufficient concern to withhold the DAC.

Access / Egress / Evacuation

484. Adequate access and egress at the person or limb level is important to ensure that EMIT can be performed reliably and that personnel can move freely around the facility.

485. Reference 34, section 2 provides comprehensive guidance on the minimum allowances to facilitate personnel movement around the facility. The data contained within is based on that contained within recognised RGP, e.g. BS ISO standards, and US NRC guidance. I consider these sources to be appropriate RGP.

486. Given the lack of design detail relating to maintenance I have not explored access / egress in relation to EMIT any further as there is little to assess in this area. It is a subject that I follow up beyond GDA when sufficient design detail is available to perform meaningful assessment.

487. The assessment of evacuation is predominantly covered in ONRs fault studies assessment (Ref. 75) and also discussed within the Radiological Protection assessment report (Ref 78). I have provided specialist support to this area with respect to the credibility of the evacuation claims.

488. In summary, I consider that:

- Hitachi-GE has used the fault analysis to clearly identify where evacuation is necessary. Evacuation is claimed within the design basis safety case.
- The claims on immediate and rapid evacuation are a challenging issue to accept within a design basis safety case. Under such circumstances, human behaviour can be highly unpredictable and it is known that maladaptive behaviours can result, i.e. moving towards the hazard instead of rapid evacuation. Due to such uncertainties, evacuation should only ever be claimed where engineered solutions are demonstrated to not be ALARP.
- Hitachi-GE has included the basis for its time estimates (including initial location of workers, the location of exit, the speed on ladders and moving through floodwater) in the submission.
- However, without a complete redesign of the UK ABWR and its outage operations (it would no longer be an ABWR), workers will need to be in vulnerable areas doing essential work during shutdown operating states, and there is no way to avoid a need for rapid evacuations for the most limiting faults.

489. I conclude that whilst this position is not ideal, Hitachi-GE has identified the vulnerable activities that will enable a future licensee to manage these risks ALARP. This provides a sound basis from which a future licensee can consider further risk reduction measures to manage the residual risk.

490. ONR will consider this topic, and wider personnel movement around the plant during all plant and fault states, further post-GDA, as details on operational complements mature. This is partially covered by Radiological Protection Assessment Finding:

- AF-ABWR-RP-08 (Ref. 78)

Examination Maintenance Inspection Testing

491. ONR expects that: "Workspaces in which operations (including maintenance activities) are conducted should be designed to support reliable task performance. The design should take account of the physical and psychological characteristics of the intended users and the impact of environmental factors." (SAP EHF.6 Workspace design).

492. With respect to EMIT, this means that ONR expects that the design of safety important equipped is designed to minimise errors during disassembly and reassembly (The Poka Yoka or mistake proofing concept) and that consideration is given to the need for inspection activities.

493. Hitachi-GE acknowledge that the detail design and task information necessary to assess EMIT tasks was not available during GDA. It commits to further development in this area, which I expect a future licensee to follow-up. I therefore cannot consider that the risks from EMIT activities have been reduced ALARP.

494. What I can conclude based on evidence assessed within sections 4.2, 4.3, and 4.4 above is:

- All SSC important for safety have been identified in the fault schedule providing a list of important EMIT activities.
- Maintenance specific HBSCs that relate to ensuring that the systems or components are restored to their pre-EMIT state have been identified.
- Type A and B errors relating to maintenance are modelled in PSA.
- In lieu of design detail, Hitachi-GE produced a set of conservative screening maintenance error data based around 4 error types.
- Hitachi-GE also sensibly conducted discrete analysis of two discrete maintenance errors which did not fit the generic models.
- There is evidence that in those areas of the design that are more mature, that HF was considered.
- There is evidence of HF training being given to the designers of plant equipment.
- Hitachi-GE has developed a comprehensive HF engineering guide to ensure that HF RGP is integrated into the design of the plant.

495. Outside of my HF assessment, EMIT has been considered within other ONR assessment reports and I provided technical support in these areas:

- Mechanical handling and fuel route operations for defueling and refuelling, (Ref. 3)
- HF involved in the inspection of vessel or structural integrity. (Ref. 79)

496. In addition, I have not considered areas where very specialised and well-established HF considerations apply such as the ergonomics of inspections of structural integrity or pressure vessel condition. These areas are supported by well-codified standards and guidance that is well understood by ONR inspectors, involved in those fields.

Decommissioning

497. Specific HF considerations relating to decommissioning were not considered as part of this assessment.

Conclusion to Section 4.6

498. The detailed design for the wider plant was not defined for GDA, which constrained my assessment. This is not unusual during GDA

499. However, I do not consider this to be of concern for two reasons.

- The design maturity levels mean that adequate HFI is not foreclosed.
- A lot of the wider HF engineering design can be resolved late in the design process without compromising other elements of the design.

500. What I can conclude in this area is:

- There is significant work required beyond GDA by a future licensee to adequately meet regulatory expectations, for example:
  - Thermal analysis of the control room
  - Acoustic analysis of the control room
  - Detailed design input into the design of SSCs to support reliable EMIT
  - Analysis of evacuation and wide plant personnel movements during normal and fault conditions
  - HFI into design for decommissioning
- The HBSCs applicable to the wider plant are well understood, which provides a mechanism for targeting future work. HEP data for these HBSCs appears suitably conservative and supportable if a modern standards HFI process is adopted by the future licensee.
- The guidance developed to underpin the wider HF engineering programme was based on and meets RGP and there was evidence that it was followed; albeit within the limitations of the design maturity.

Concept of Operations

501. A concept of operations defines the goals and expectations for the new system from the perspective of users and other stakeholders and defines the high-level considerations to address as the detailed design evolves. It includes (Ref. 11):

- Statement of operational purpose of the system
- Consideration of the command and control philosophy
- Staffing concept and their capabilities and responsibilities
- Basic details of the working environment
- Work organisation and design
- Concept of use – how the HMI is used by the operators to support the safe operation of the plant.

502. The concept of operation for the UK ABWR is presented in Reference 42, the scope of which is based on the scope defined in Reference 11 above.

503. The concept of operations has been derived from the J-ABWR and modified to reflect the UK NPP operational practices. It draws from the experience and knowledge of a UK future operations team. I consider this to be a sound basis for demonstrating feasibility of claimed human based safety actions through HF analysis.

504. The concept of operations report describes the expected manning levels and roles for MCR-based personnel and elsewhere on the plant where claims might be placed upon individuals performing those roles. This includes processes for supervision and checking intended to improve overall performance of human based safety actions.

505. I was able to verify that the operational concept is being consistently applied in practice to the task analysis of HBSCs and the logical and probabilistic modelling of those

actions. This is demonstrated in: the analysis of tasks and errors undertaken to support estimations of human failure probability given in Reference 44, which covers Level 1, Level 2 Shutdown and Spent Fuel Pool Probabilistic Safety Assessments.

506. It should be noted that the manning structure is not explicitly referred to in the majority of human based safety claims but only on those supported by documented task analysis. However, through my discussions with Hitachi-GE HF personnel I am satisfied that the operational concept has consistently influenced their thinking when analysing the deterministic human based safety claims.

507. I judge that Hitachi-GE have developed a valid concept of operations applicable to British operation of the UK ABWR. It provides a credible description of assumed operational roles and an appropriate allocation of function between personnel for the execution of safety actions and the checking that those safety actions have been correctly executed. The operational concept has been applied in a consistent fashion to probabilistic analyses.

508. I conclude that the concept of operations underpins the wider substantiation of HBSCs. I also conclude that it appears to be based on a credible set of operational assumptions.

509. It will be necessary for a future licensee to validate the assumptions made during GDA relating to the concept of operations. Or where changes are made, consider the effects of any changes on the risk analysis.

As Low As Reasonably Practicable (ALARP)

510. It is required under UK law (Health and Safety at Work etc. Act 1974) that workplace risks are reduced so far as is reasonably practicable (SFAIRP). When this legal requirement is met, risk is determined to be reduced ALARP. As nuclear facilities are classed as places of work, they are subject to this requirement. It is thus important for a requesting party to provide evidence that its design meets this requirement as far as is reasonably practicable for GDA.

511. Using the “reasonably practicable” concept allows ONR to set goals for duty-holders, rather than be prescriptive. This flexibility is a great advantage as it allows a flexible approach to reducing risks ALARP thus supporting innovation. However, there are drawbacks to this approach in that it requires duty-holders and ONR to exercise judgment.

512. There are two ways in which ONR determines whether a design acceptably reduces risk ALARP:

- A comparison against RGP. That is, control measures have been used that are recognised by consensus (i.e. the nuclear industry and the regulator) to be the best way of controlling the risk.

- A first principle computation. That is, the quantum or risk reduction is compared against the sacrifice in terms of time, effort and cost. Where the balance is grossly disproportionate, then the risk is considered to be reduced ALARP.

513. This section presents my assessment of whether ALARP has been demonstrated in the HF topic area for the UK ABWR. My judgements and conclusions should be viewed in concert with the wider ONR overall assessment of the UK AWBR design, e.g. Reference 75, ONR Fault Studies Assessment Report.

514. The Hitachi-GE Human Factors ALARP case was presented in the HF ALARP Report (Ref. 6). The ALARP method is described within the GDA ALARP Methodology (Ref. 80).

515. As I have already stated in sections above, I am content that Hitachi-GE has applied appropriate modern standards and RGP, where appropriate. Where there is no consensus regarding "good", I consider that Hitachi-GE has taken a logical and sensible approach and gone back to first principles or adapted existing methodologies, codes and standards. Hitachi-GE has then implemented a system of verification (Ref. 28) to ensure that the output from the design process complies with these codes and standards, and a system of validation (Ref. 28.) to ensure that the end result demonstrably reduces risk.

516. As part of my wider assessment, I have sought evidence that the programme of HFI has demonstrably informed the design with respect to risk reduction.

517. The UK ABWR is an evolution of the baseline J-ABWR design. Hitachi-GE claims that the baseline design has benefitted from HFI informally and formally in its design. It provides evidence against this claim in the "Baseline Human Factors Assessment Report" (Ref. 24). I consider that this claim is largely supported. Reference 24, described a design review of the J-ABWR design and shows that it does largely meet modern HF standards, with some exceptions. These exceptions are identified and were added to the HFIR for resolution during the course of GDA.

518. The Baseline Human Factors Assessment served as a foundation on which to build a focused programme of HF work to not only to address the identified shortfalls but also to address UK regulation or operational requirements.

519. Within that programme, the scope of professional HF involvement in the GDA design has taken two forms: inputs to the engineering design, with a view to minimising human error so far as is reasonably practicable, and undertaking analysis of engineering designs to establish whether the risk of error is indeed minimised ALARP.

520. Hitachi-GE claims that the design input and analytical effort has been proportionate and informed by risk. I consider this claim to be substantiated. The HF and PSA teams have worked together to identify those systems which are vulnerable to human error and the most important HBSCs. I discuss this in more detail in section 4.3

521. Within the HF ALARP report (Ref. 6), Hitachi-GE has identified design improvements aimed at reducing the risk from human error. These comprise:

- Increased automation of systems relevant nuclear safety by allocation of function;
- HMI improvements identified via the HRA;
- Implementing a strategy for improved alarm presentation;
- Plant layout improvements relative to J-ABWR;
- Improvements in process and layout in specific areas e.g. fuel route.

522. HFI can only lead towards an ALARP position if recommendations are made for design improvement and appropriately sentenced. In all of the documents I have assessed in considering the substantiation of HBSCs, each one does contain recommendations. I have followed the life-cycle of some of these recommendations and can confirm that recommendations are being appropriately sentenced and that there is evidence of direct HF influence on the design. I note that, despite impending closure of GDA Step 4, Hitachi-GE has been willing both to add new issues to the HFIR and to re-open closed ones where new information has emerged that affect the previous closure decision. This strongly suggests that Hitachi-GE is using the HFIR in a proper fashion.

523. As I am satisfied that the analyses have been risk informed, then it is possible to conclude that design recommendations, within the scope of GDA, will lead towards ALARP position in the case of those human based safety claims that have been assessed. However, I do note that the HBSC continue to be identified and their substantiation continues to be developed as I write my assessment.

524. Demonstration of ALARP will be an ongoing objective for future safety cases as the design and organisation develops. Inevitably a number of assumptions have needed to be made regarding the future design and operating organisation. However, it is possible to judge whether the work done to date will lead towards an ALARP position. I judge this to be the case here. I consider that the HF-based recommendations that have stemmed from the analyses I have assessed, are driving the design towards minimising risk ALARP.

525. My expectation, post-GDA, is that the UK-AWBR will continue to evolve towards a position where risk is reduced ALARP. The future licensee will need to consider how any post GDA design changes and the operating organisation and safety-management systems impact upon the ALARP position.

CONCLUSION

526. This report presents the findings of the ONR assessment of HF for the Hitachi-GE UK ABWR GDA Step 4.

527. The UK ABWR has changed from the original J-ABWR baseline design. This evolution has required a significant effort in the HF area by Hitachi-GE. It was necessary to grow a significant HF capability and embark upon a complex and wide ranging design and safety analysis campaign. This has born both, significant risk-insights and demonstrable improvements over the baseline design. I note the considerable effort that was required to do this.

528. I have assessed Hitachi-GE's HFI programme of design and safety analysis work against the applicable expectations of ONR's SAPs and TAGs.

529. In doing so I have considered whether:

- The PCSR and supporting references provides a suitable and sufficient safety case to demonstrate that the UK ABWR is capable of being built and operated in Great Britain on a site bounded by a generic site envelope, in a way that is acceptably safe and secure.
- Taken together in concert, the totality of the design and safety submissions is sufficiently adequate to recommend issuing a DAC.
- Hitachi-GE has identified and understands the risk contribution from the HBSCs on the UK ABWR design.
- There has been adequate consideration of the HF contribution to an overall ALARP position.
- The HFI programme, including consideration of the codes and standards used, the methods applied, and the competency of the HF team delivering the programme of work were acceptable.
- Hitachi-GE has provided sufficient evidence to substantiate the HBSCs on the UK ABWR design to an appropriate level for GDA.

- Hitachi-GE has arrived at a balanced design with respect to the allocation of function between the human and the technology.
- The design has been demonstrably informed by the HFI programme.
- Residual issues and assumptions relating to a future operating organisation are being managed in a manner suitable for future resolution / validation.

530. To conclude, the early difficulties in securing HF resource to establish a credible HFI capability, and the maturity level of the UK variant of ABWR design, limited what was practicably achievable by Hitachi-GE during the GDA. At the completion of GDA only conceptual designs existed for the major HMIs and many of the risk important SSC. Whilst I commend what was achieved, given the above factors, there remains significant work remaining in the HF area post-GDA.

531. Despite these constraints, I consider that Hitachi-GE did sufficient work in this area. I am satisfied with the claims, arguments and evidence laid down within the PCSR and supporting documentation for HF. On this basis I consider that the UK ABWR is capable of being built and operated in GB on a site bounded by a generic site envelope, in a way that is acceptably safe and secure and thus support issuing a Design Acceptance Confirmation (DAC).

532. I judge that, within the purposes of GDA, Hitachi-GE has:

- Provided a PCSR and supporting references sufficient for GDA and taking account of the design maturity to demonstrate that the UK ABWR design is capable of being built and operated in Great Britain (GB), on a site bounded by a generic site envelope, in a way that is acceptably safe and secure.
- Developed a clear initial claims and arguments structure in which it is possible to trace each Human Based Safety Claims (HBSCs) identified in the basis of safety case document all the way up through safety functional / property claims, into high level safety functions and fundamental safety functions.
- Identified a comprehensive list of HBSCs, which are identified / modelled in both the fault schedule and PSA. The PSA considers Type A, B, and C errors and includes consideration of errors of omission and commission. It also appropriately models dependency.
- Applied its HRA method with suitable conservatism taking account the lack of design maturity and assumptions associated with future licensee operation and arrangements. Noting the need for a future licensee to look specifically at how HCI is modelled in the HRA.
- Demonstrated that the risk contribution from the human is proportionate within what is considered practical for GDA.
- Provided sufficient evidence to substantiate that the HBSCs are credible within the limitations of GDA and without licensee input.
- Provided sufficient evidence demonstrating that the UKABWR design submitted for GDA is balanced and minimises the risk from human error via the appropriate allocation of safety functions between technology and operators. The UK ABWR features high levels of automation. There are no claims made on the operator within 30 mins of a fault occurring with automatic reactivity control and short term cooling. Other operator claims are typically simple responses to failed automatic safety system.

- Provided sufficient confidence that the HMI design is sufficiently mature for GDA, with sufficient contingency to mitigate the risk of foreclosing on future options.
- Identified a comprehensive set of domestic and international standards appropriate to inform the UK ABWR design.
- Identified an appropriate suite of tools and methods that meet GB regulatory expectations with respect to RGP.
- Provided cogent evidence that these codes, standards, tools and methods are being appropriately and proportionately applied.
- Developed a suitable process for capturing and sentencing HF engineering deficiencies.
- Developed a suitable process for capturing future operating and licensee arrangement assumptions.

533. There remains a significant amount of HF work required post GDA to reflect the evolving nature of the design, to accommodate the licensee's chosen operating regime, and items that were out of scope for GDA. This will require the future licensee to revisit the HBSC analysis for the UK ABWR to ensure that they reflect the increased understanding of the design and operation. In particular, I consider the following areas are of key importance for a future licensee:

- Whilst the maturity of the design was adequate for GDA, there remains considerable HFI effort required to fully substantiate the design for operation. It is important that the future licensee recognises the extended timescales associated with fully substantiating some of the more complex areas of the design (e.g. control rooms / major HMIs) or those long lead items that need to be ordered years in advance of delivery (e.g. RPV, or Decommissioning Considerations).
- On a modern nuclear plant design with high levels of protection and automation, the probabilistic model shows that much of the human risk contribution comes from human error during EMIT activities leading to the failure of an systems, structures or components. This is the same for the UK ABWR design. Noting again the lead times of nuclear important equipment, a future licensee will need to provide early assurance of the ability to reliably examine, maintain, inspect, and test prior to signing off on the design. There is recent industry learning in this area showing the significant cost / schedule impact of not providing this assurance before procuring the equipment.
- A weakness in all current generation HRA methods that has not been addressed for GDA is the fact that the database of reliability is drawn from human interactions with traditional analogue panel based HMIs. In previous GDAs, this issue has been mitigated by taking into consideration the output from simulator and ISV trials. This was not an option for this GDA given the relative maturity of the MCR. A future licensee will have to consider the impact of screen based interfaces on human reliability post-GDA, either through improved HRA modelling or through simulator input – or combinations of both.
- At the claims and arguments level, I consider Hitachi-GE to have developed the beginnings of a modern standards HF safety case. However, my assessment of the evidence base (basis of safety case and analysis documents) has often shown a lack of connection to the claims and arguments, i.e. it should be explicit in all evidence submissions, what the evidence is substantiating and

how. The failure to do this at this level significantly impacts the coherency of the safety case.

REFERENCES

1	ONR, Step 4 Assessment Plan for Human Factors, ONR-GDA-AP – 15 –006, 9th November 2015
2	ONR, Step 4 Assessment of Radiation Protection for the UK ABWR, ONR-NR-AR-17-021, Revision 0, December 2017
3	ONR, Step 4 Assessment of Mechanical Engineering for the UK Advanced Boiling Water Reactor, ONR-NR-AR-17-022, Revision 0 December 2017
4	ONR, Step 4 Assessment of Structural Integrity for the UK Advanced Boiling Water Reactor, ONR-NR-AR-17-037, Revision 0, December 2017
5	ONR, Step 4 Assessment of Severe Accidents for the UK Advanced Boiling Water Reactor, ONR-NR-AR-17-015, Revision 0, December 2017
6	Hitachi-GE Nuclear Energy, Ltd., Human Factors ALARP Report, GA91-9201-0003-02210 (HFE-GD-0524), Revision A, July 2017
7	ONR, ONR Guidance on Mechanics of Assessment, TRIM 2013/204124
8	ONR, Safety Assessment Principles for Nuclear Facilities. 2014 Edition Revision 0, ONR, November 2014, www.onr.org.uk/saps/saps2014.pdf
9	ONR, NS-TAST-GD-005 Guidance on the Demonstration of ALARP (As Low As Reasonably Practicable)
10	ONR, NS-TAST-GD-030 Probabilistic Safety Analysis
11	NS-TAST-GD-058 Human Factors Integration
12	NS-TAST-GD-059 Human-System Interface
13	NS-TAST-GD-062 Workplaces and Work Environment
14	NS-TAST-GD-063 Human Reliability Analysis
15	NS-TAST-GD-064 Allocation of Function between Human and Engineered Systems
16	■ SSR-2/1 Safety of Nuclear Power Plant: Design Specific Requirements. ■ SSG-2 Deterministic Safety Analysis for Nuclear Power Plant Specific Safety Guide ■ SSG-3 Development and Application of Level 1 Probabilistic Safety Analysis for Nuclear Power Plant Specific Safety Guide ■ SSG-4 Development and Application of Level 2 Probabilistic Safety Analysis for Nuclear Power Plant Specific Safety Guide ■ NS-G-1.3 Instrumentation and Control Systems Important to Safety in Nuclear Power Plants. Safety Guidance ■ NS-G-2.15 Severe Accident Management Programmes for Nuclear Power Plants
17	Hitachi-GE Nuclear Energy, Ltd., Generic PCSR Chapter 27 : Human Factors, GA91-9101-0101-27000 (HFE-GD-0057), Revision C, August 2017
18	Hitachi-GE Nuclear Energy, Ltd., Generic PCSR Chapter 21 : Human-Machine Interface, GA91-9101-0101-21000 (3E-GD-A0060), Revision C, August 2017

19	Hitachi-GE Nuclear Energy, Ltd., Generic PCSR Chapter 30 : Operation, GA91-9101-0101-30000 (QGI-GD-0012), Revision C, August 2017
20	Hitachi-GE Nuclear Energy, Ltd., Human Factors Integration Plan GA32-1501-0007-00001 (3E-UK-0121), Revision C, October 2014
21	Hitachi-GE Nuclear Energy, Ltd., Human Factors Assessment Report, GA91-9201- 0001-00042 (HFE-GD-0067), Revision D, August 2017
22	Hitachi-GE Nuclear Energy, Ltd., Human Factors Design and Engineering Report, GA91-9201-0001-00039 (HFE-GD-0065), Revision C, August 2017
23	Hitachi-GE Nuclear Energy, Ltd., Human-Based Safety Claims Report, GA91-9201- 0001-00043 (HFE-GD-0064), Revision D, December 2016
24	Hitachi-GE Nuclear Energy, Ltd., Baseline Human Factors Assessment Report, GA91- 9201-0001-00032 (HFE-GD-0068), Revision B, August 2015
25	Hitachi-GE Nuclear Energy, Ltd., Human Factors Methodology Plan, GA91-9201- 0001-00033 (HFE-GD-0059), Revision E, January 2017
26	Hitachi-GE Nuclear Energy, Ltd., “Human Factors Requirements Compliance Tracking Matrix”, GA91-9201-0001-00038 (HFE-GD-0062), Revision C, August 2017
27	Hitachi-GE Nuclear Energy, Ltd., Human Factors Issues Register, GA91-9201-0001- 00036 (HFE-GD-0061), Revision C, August 2017
28	Hitachi-GE Nuclear Energy, Ltd., Human Factors Verification and Validation Plan, GA91-9201-0003-01353 (HFE-GD-0232), Revision A, October 2016
29	Hitachi-GE Nuclear Energy, Ltd., Human Factors V&V Report, Revision A, HFE-GD-0525, August 2017
30	Hitachi-GE Nuclear Energy, Ltd., Human Factors ALARP Report, Revision A, HFE-GD-0524, July 2017
31	Hitachi-GE Nuclear Energy, Ltd., Error of Commission Analysis Report, GA91-9201- 0003-00815 (HFE-GD-0157), Revision D, March 2017
32	ONR, Closure Assessment Note RO-ABWR-0024 Human Reliability Analysis – Errors of Commission / Misdiagnosis - 2017/422023
33	Hitachi-GE Nuclear Energy, Ltd., Human Reliability Analysis Report, Revision C, GA91-9201-0001-00041 HGNE, March 2015
34	Hitachi-GE Nuclear Energy, Ltd., Human Factors Engineering Specification, Revision. B, GA91-9201-0001-00037 HGNE, March 2015
35	Hitachi-GE Nuclear Energy, Ltd., Allocation of Function Report, GA91-9201-0001-00040, April 2015
36	Hitachi-GE Nuclear Energy, Ltd., Human Factors Methodology, Revision C, GA91-9201-0001-00033 HGNE, March 2015
37	Hitachi-GE Nuclear Energy, Ltd., Human Based Safety Claims Report, Revision. A, GA91-9201-0001-00043 HGNE, March 2015
38	ONR, Closure Assessment Note RO-ABWR-0033, Human Factors Baseline Assessment, 2017/422031
39	Hitachi-GE Nuclear Energy, Ltd., Strategy of Use for HMIs, GA91-9201-0003-01462 (HFE-GD-0360), Revision A, December 2016
40	Hitachi-GE Nuclear Energy, Ltd., Cognitive Workload Analysis Report, Revision A, HFE-GD-0415, February 2017
41	Hitachi-GE Nuclear Energy, Ltd., UK ABWR Alarm Processing and Presentation Strategy, Revision A, HFE-GD-0474, March 2017
42	Hitachi-GE Nuclear Energy, Ltd., Human Factors Concept of Operations Report, Revision E, HFE-GD-0060, April 2017

43	Hitachi-GE Nuclear Energy, Ltd., HCI-Induced Cognitive Error Analysis Report, Revision B, HFE-GD-0416, Jun 2017
44	Hitachi-GE Nuclear Energy, Ltd., Human Reliability Analysis Report, Revision E, HFE-GD-0066, July 2017
45	Hitachi-GE Nuclear Energy, Ltd., Alarm Basic Design Specification, Revision 0, 3E-GD-A0137, March 2017.
46	Hitachi-GE Nuclear Energy, Ltd., Alarm Design Rationalisation and Justification Report, Revision A, HFE-GD-0417, July 2017.
47	ONR, Closure Assessment Note RO-ABWR-0069 Human Factors Baseline Assessment, 2017/415013.
48	Hitachi-GE Nuclear Energy, Ltd., Generic PCSR Chapter 14 : Control and Instrumentation, GA91-9101-0101-14000 (3E-GD-A0063), Revision C, August 2017.
49	Hitachi-GE Nuclear Energy, Ltd., Generic PCSR Chapter 5 : General Design Aspects, GA91-9101-0101-05000 (XE-GD-0645), Revision C, August 2017.
50	Hitachi-GE Nuclear Energy, Ltd., GDA Safety Case Development Manual, GA10-0511-0006-00001 (XD-GD-0036), Revision 3, June 2017
51	ONR, Human factors integration, Revision 3, NS-TAST-GD-058.
52	Hitachi-GE Nuclear Energy, Ltd., Human Factors Issues Register, Revision B, HFE-GD-0061, January 2016.
53	Hitachi-GE Nuclear Energy, Ltd., Printout from the AIRIS database, TRIM: TRIM 2017/285511.
54	ONR, Hitachi-GE Level 4 Human Factors Progress Meeting 22nd to 25th February, ONR-GDA-CR-15-439, Revision 0, February 2016, TRIM 2016/104468.
55	ONR, Step 4 Assessment of Mechanical Engineering for the UK Advanced Boiling Water Reactor, Revision 0, ONR-NR-AR-17-022, December 2017.
56	GRS, Compilation of Boiling Water Reactors (BWR) operational experience (OpEx) to inform ONR's ABWR GDA assessment work during GDA, GRS-ONR188-01, July 2014.
57	Sandia National Laboratories, A compilation of BWR reactor OPEX for the UK's ONR Advanced BWR Reactor GDA, SAND2014-20656, December 2014.
58	Hitachi-GE Nuclear Energy, Ltd., Allocation of Function Report, Revision E, HFE-GD-0063, June 2017.
59	NRC, Methodology for allocating nuclear power plant control functions to human or automatic control, NUREG/CR-3331, Revision 1. Washington DC: US Nuclear Regulatory Commission, 1983.
60	IAEA, The role of automation and humans in nuclear power plants, IAEA-TECDOC-668, Vienna: IAEA. 1992.
61	ONR, HGNE COMMERCIAL - Meeting Materials - HFE-GD-0426 - Rev 0 - GDA Human Factors L4 Progress & Technical Meeting - 10 November 2016, TRIM 2016/439450
62	ONR, HGNE COMMERCIAL - Meeting Materials - HFE-GD-0515 - Rev 1 - L4 GDA - Human Factors Progress Meeting - 23 March 2017, 2017/125604.
63	Reer, B., and Dang, V.H., The Commission Errors Search and Assessment (CESA). PSI Bericht Nr. 07-03, May 2007.
64	Podofillini, L. and Dang, V. H. Progress on Errors of Commission: an Outlook Based on Plant-Specific Results. Proc. PSAM11 and ESREL12, 25–29 June 2012.
65	Hitachi-GE Nuclear Energy, Ltd., Human-Based Safety Claims Report, HFE-GD-0064, Revision E, September 2017.
66	Hitachi-GE Nuclear Energy, Ltd., Human Reliability Analysis Report, Revision E, HFE-GD-0066, July 2017.

67	Hitachi-GE Nuclear Energy, Ltd., Hazards HRA Addendum, GA91-9201-0003-02050 (HFE-GD-0516), Rev. A, May 2017.
68	Hitachi-GE Nuclear Energy, Ltd., Task Performance Analysis for Non-PSA HBSCs, HFE-GD-0517, Revision A, July 2017.
69	ONR, Step 4 Assessment of Probabilistic Safety Analysis for the UK Advanced Boiling Water Reactor, ONR-NR-AR-17-014, Revision 0, December 2017
70	Synergy-CRA, CRA-ONR-POW-J336, Report No. 1, Issue 1, Provision of Technical Support on ONR Assessment of Step 4 Human Claims and Reliabilities for the UK ABWR, July 2017.
71	Hitachi-GE Nuclear Energy, Ltd., Comprehensive list in GDA for requirements and assumptions to be transferred to operating regime, XD-GD-0049, Revision 1, September 2017.
72	Hitachi-GE Nuclear Energy, Ltd., Topic Report on Internal Event at Power Level 1 PSA, GA91-9201-0001-00102 (AE-GD-0257), Revision 4, July 2016.
73	Hitachi-GE Nuclear Energy, Ltd., Generic PCSR Chapter 24 : Design Basis Analysis, GA91-9101-0101-24000 (UE-GD-0208), Revision C, August 2017.
74	Hitachi-GE Nuclear Energy, Ltd., Topic Report on Fault Assessment, Revision 6, UE-GD-0071, July 2017.
75	ONR, Step 4 Assessment Report - Fault Studies, Revision 0, UK ABWR GDA - ONR-NR-AR-17-016, December 2017.
76	Hitachi-GE Nuclear Energy, Ltd., “Class 1 MCC and Backup HMI HF Assessment Report”, GA91-9201-0003-02183 (HFE-GD-0633), Revision A, September 2017.
77	EEMUA, EEMUA Publication 191 Alarm systems - a guide to design, management and procurement, Third Edition.
78	ONR, Step 4 Assessment of Radiological Protection for the UK Advanced Boiling Water Reactor, ONR-NR-AR-17-021 Revision 0, December 2017.
79	ONR, Step 4 Assessment of Structural Integrity for the UK Advanced Boiling Water Reactor, Revision 0, ONR-NR-AR-17-037, December 2017.
80	Hitachi-GE Nuclear Energy, Ltd., GDA ALARP Methodology, GA10-0511-0004-00001 (XD-GD-0037), Revision 1, November 2015.
81	Hitachi-GE Nuclear Energy, Ltd., Basis of Safety Cases on PCV Gas Control Systems, GA91-9201-0002-00074 (SE-GD-0196), Revision 2, June 2017.
82	Hitachi-GE Nuclear Energy, Ltd., Meeting Materials - HFE-GD-0502 - Rev 0 - L4 GDA Human Factors Progress Meeting - 24 February 2017.
83	Hitachi-GE Nuclear Energy, Ltd., HFE-GD-0531 - L4 GDA - Human Factors Meeting - 20 April 2017.
84	Hitachi-GE Nuclear Energy, Ltd., Basis of Safety Cases on Heating Ventilating and Air Conditioning System, GA91-9201-0002-00041 (HPE-GD-H006), Revision 4.
85	ONR, ONR-NR-AR-17-022, Revision 0, Step 4 Assessment of Mechanical Engineering for the UK Advanced Boiling Water Reactor - December 2017.
86	HGNE, UK ABWR, GA91-9201-0002-00109 - 3E-GD-A0166 - Rev.1 - Basis of Safety Cases on Overall Human-machine Interface.
87	HGNE, UK ABWR, GA91-9201-0002-00060 - 3E-GD-A0029 - Rev.2 - Basis of Safety Cases on Main Control Room Human-machine Interface.
88	HGNE, UK ABWR, GA91-9201-0002-00061 - 3E-GD-A0030 - Rev.2 - Basis of Safety Cases on Remote Shutdown System Human-machine Interface.
89	HGNE, UK ABWR, GA91-9201-0002-00062 - 3E-GD-A0031 - Rev.2 - Basis of Safety Cases on Backup Building Human-machine Interface.

Annex 1

Regulatory Observations

RI / RO Ref	RI / RO Title	Description	Date Closed	Report Section Reference
RO-ABWR-0005	Hitachi-GE Nuclear Energy Ltd. Human Factors Specialist Resource and Organisation.	The UK ABWR design makes wide ranging and potentially important safety claims related to human reliability, which require substantiation in a modern standards safety case. ONR expects the development of the HF safety case and nuclear power plant design influenced by modern HF principles to be delivered by an identified HF team under the management of a specialist HF lead. Hitachi-GE's current arrangement is that HF is managed as part of its electrical and control and instrumentation department. ONR considers this organisational arrangement and the current level of HF resource insufficient to deliver the GDA outcomes on HF in the time envisaged. Hitachi-GE therefore needs to increase its HF capability to ensure that it has sufficient suitably qualified and experienced HF specialists and organisation to deliver the volume of HF analyses work required for GDA to meet UK regulatory expectations. Left unresolved, the above matters present a potentially significant project risk for Hitachi-GE delivering a successful GDA safety case within the desired timescale. ONR recognises that the organisational changes sought in the actions to this RO will require some time to develop; the key is continually improving Hitachi- GE's capability throughout the period of GDA Step 2 and into the first part of Step 3 in order to achieve a successful outcome.	Jan 2015	3.2
RO-ABWR-0024	Human Reliability Analysis – Errors of Commission / Misdiagnosis.	The UK ABWR makes potentially important safety claims related to human reliability, which require substantiation in a modern standards safety case. Amongst other human factors matters, ONR expects the safety case to identify and proportionately analyse all reasonably foreseeable human actions and omissions that might impact on safety. During ONR's Step 2 assessment of the UK ABWR, Regulatory Queries (RQ) were raised related to Human Reliability Analysis (HRA) [Ref.1]. Three of these were focussed on the requesting party's approach to the treatment of Errors of Commission (EOC) and their impacts on safety. ONR has assessed the RPs responses to the RQs [Ref. 1] and whilst we welcome the commitment given by Hitachi-GE to identify, understand and qualitatively analyse EOC, and that	July 2016	3.2

RI / RO Ref	RI / RO Title	Description	Date Closed	Report Section Reference
		quantification will be provided 'if appropriate', ONR does not consider the entirety of the responses to be sufficiently justified and fully reflective of HRA relevant good practice and UK regulatory expectations in this area. Hitachi-GE has also stated that 'additional negative impacts that cause new accident sequence are not modelled in the PSA because of the complexity of the impact on the sequence'. This is not consistent with the UK legal requirement to reduce all risks so far as is reasonably practicable. Without appropriate analysis of important EOC an unknown risk gap can exist, resulting in an inadequate safety case, design and the UK ABWR risk estimates being optimistic. Left unresolved, inadequate treatment of EOC is a potentially significant project risk for Hitachi-GE delivering a successful GDA safety case within the desired timescale. The RP should consider the matters identified in this Regulatory Observation (RO), furnish responses to the actions raised, and subsequently provide in the UK ABWR safety case, suitable and sufficient justification and analysis for the treatment of EOC and their impacts within the UK ABWR safety case.		
RO-ABWR-0033	Human Factors Baseline Assessment.	As part of the UK ABWR safety case, Hitachi-GE claims that consideration of human factors (HF) has improved and evolved over the course of the history of the reactor and has been integral to design requirements across all areas of plant. The UK ABWR is therefore already starting from a position of having widespread integrated consideration of HF during the original design. In support of this, the RP conducted a Baseline HF Assessment [Ref. 1] which attempts to capture the nature and outcome of the inclusion of HF activity in the existing ABWR design. The UK ABWR Pre-Construction Safety Report (PCSR) states that the baseline HF assessment and its referenced documents provide the main source of evidence for the Level 1 Human-Based Safety Claims. Hence the baseline HF assessment and its conclusions constitute an integral part of the UK ABWR safety case. ONR is unable to verify the adequacy and validity of the baseline HF claims / conclusions and corresponding aspects of the PCSR based on the information provided by RP. The baseline HF assessment fails to evidence its claims and conclusions, which falls short of modern standards safety case expectations. Given that such evidence is based on the existing ABWR design and operations, this should be readily	October 2015	3.2

RI / RO Ref	RI / RO Title	Description	Date Closed	Report Section Reference
		available and presented in coherent and cogent format as a part of the PCSR supporting documentation. Hitachi-GE needs to assemble (or generate) and compile its baseline HF evidence in a coherent format and submit it as part of the PCSR as detailed in the actions to this RO. This is judged to be necessary in order for both the RP and ONR to be confident that the baseline HF position on which subsequent HFI activities for the UK ABWR are based is as claimed, valid and adequately substantiated.		
RO-ABWR-0069	Human Machine Interface: Strategy, Application and Cognitive Issues	ONR Safety Assessment Principle (SAP) EHF.3 directs an assessment of whether human actions that can affect safety have been identified. In addition, SAP EHF.5 sets out an expectation for the proportionate analysis of tasks contributing positively or negatively to the fulfilment of safety functions. SAPs ESR.1 and EHF.7 direct the assessment of whether such HMIs are 'suitable and sufficient'. Taken together, these SAPs provide principled criteria for ONR inspectors to assess the suitability and sufficiency of user interfaces to support the users' tasks that may be required to support safety. It is a fundamental functional requirement that those personnel in nuclear power plant control rooms, who are responsible for controlling and monitoring that nuclear plant, should have the necessary information to do so available to them through human-machine interfaces (HMIs). Because operators base their understanding and the majority of their decisions on this information, it must be reliably understood if they are to maintain their situation awareness of the plant state and suitably intervene where necessary. In part, this understanding is assured in design by developing user interfaces on HMIs that are clear in the design of their content and match user's' expectations in the methods used for presenting and coding the required information. ONR is generally satisfied that the Hitachi-GE application of human factors (HF) engineering specifications to deliver clear layouts and information coding meets recognised good practice in alignment with the principles of EHF.7. However, such HF engineering specifications do not, by themselves, assure the required understanding and situation awareness. Therefore, ONR is also pleased that Hitachi-GE intend, as a part of verification and validation, to undertake analysis of usability via trials of user interface designs that result from the application of the HF Engineering Specification, in alignment with EHF.5. Nevertheless, the use of such interfaces can be vulnerable to causes of cognitive errors that can compromise the	August 2017	3.2

RI / RO Ref	RI / RO Title	Description	Date Closed	Report Section Reference
		desired levels of understanding and situation awareness that are not easily addressed by the application of engineering specifications. Our concern is focused on the extent to which these other causes are being addressed by the Hitachi-GE design within the HF assessment processes that we know about. From the commencement of GDA Step 4, ONR HF, C&I and PSA inspectors have sought to assess HMI design methods, by means of documentation and discussions with Hitachi-GE. However, Hitachi-GE has not yet delivered sufficient information to date to provide regulatory confidence that Hitachi-GE's design strategies, design analytical processes and acceptance criteria for HMIs, will be sufficient to demonstrate in Step 4 that for all operator interactions with the different user interfaces available in the MCR and elsewhere, the sources for potential cognitive unreliability or avoidable cognitive workload will be controlled by user interface designs, so that risks are as low as reasonably practicable (ALARP). Overall therefore on the evidence seen to date, we consider that Hitachi-GE HF Engineering Guidelines, integrated programme of HF design support and analysis activities, and the currently proposed HF assessment trials during the interface verification and validation phase are unlikely to ensure that the ALARP principle is met. In particular, we would wish to see HF analysis during the HF design input phase to HMI, especially where human-computer interaction (HCI) occurs. This would provide early awareness of any potential workload or cognition issues. Accordingly, ONR considers that the issues described under the headings given below also need to be addressed. However, it should be noted that at the present time ONR has no evidence to suggest that the operational characteristics of the UK ABWR plant are complex relative to other designs of nuclear power plant. Therefore, the scope of this RO is confined strictly to our concerns about the use of HMIs and any potential they might have, when being used, to induce cognitive workload or cognitive error that can be avoided by HMI or HCI design.		