Form10/00

HITACHI

UK ABWR

Document ID	:	GA91-9101-0101-27000
Document Number	:	HFE-GD-0057
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 27 : Human Factors

Hitachi-GE Nuclear Energy, Ltd.

DISCLAIMERS

Proprietary Information

This document contains proprietary information of Hitachi-GE Nuclear Energy, Ltd. (Hitachi-GE), its suppliers and subcontractors. This document and the information it contains shall not, in whole or in part, be used for any purpose other than for the Generic Design Assessment (GDA) of Hitachi-GE's UK ABWR. This notice shall be included on any complete or partial reproduction of this document or the information it contains.

Copyright

No part of this document may be reproduced in any form, without the prior written permission of Hitachi-GE Nuclear Energy, Ltd.
Copyright (C) 2017 Hitachi-GE Nuclear Energy, Ltd. All Rights Reserved.

Table of Contents

Executive Summary

This chapter describes the United Kingdom (UK) Advanced Boiling Water reactor (ABWR) Human Factors (HF) programme for Generic Design Assessment (GDA), including integrated HF support to design activities and HF analysis of human interactions with the plant. It lists all the Human-Based Safety Claims (HBSCs) that support the achievement of Safety Functional Claims (SFCs) and Safety Property Claims (SPCs) that are presented in many of the other Pre-Construction Safety Report (PCSR) chapters. Due to the fact HF cuts across topic areas, this chapter acts as a head document for a whole group of documents that comprise the GDA Human Factors Safety Case for UK ABWR. It also provides consideration of the impact on HF of issues that arise from topic areas covered in other PCSR chapters. In these cases, this chapter describes the most significant links to other chapters.

The scope of this chapter includes a list of all known HBSCs for the whole safety case (as at the end of GDA), describing how the claims link specifically to the SPCs and SFCs or to the Nuclear Safety and Environmental Design Principles (NSEDPs) (for the functional HBSCs or HF property claims, respectively), and describes the underpinning programme of work related to the substantiation of the claims. Many of the operator actions or design requirements to achieve the HBSCs are performed on or relate to the systems' Human-Machine Interfaces (HMIs) that are described in PCSR Chapter 21: Human-Machine Interface. This creates a close link between Chapters 27 and 21. The assumptions made in the HF analyses described in this chapter are consistent with the design information and safety claims for the HMIs that are presented in PCSR Chapter 21 and the operational assumptions described in PCSR Chapter 30: Operation.

Consideration of HF issues is an integral part of the overall process of demonstrating that risks of operating the UK ABWR are As Low as Reasonably Practicable (ALARP), and inherently included in other topic area ALARP assessments and the resulting recommended risk-reduction measures. Such risk-reduction measures that include an inherent consideration of HF are presented within the PCSR chapter for the relevant topic area, for example one of the systems chapter. However, risk-reduction measures that are implemented specifically to address HF aspects of the safety case, or that have HF consideration as the key driver, are presented within this chapter. Examples of the latter include additional automation of some functions important to nuclear safety, and improvements to alarm presentation to optimise alarm processing by operators.

Development of the basic design presented in GDA will be required in several topic areas post-GDA. For example, design activities relating to the development of the new Control and Instrumentation (C&I) platform, the radioactive waste management systems, and the fuel handling equipment specifications, will all require development of detailed HMI designs and design of related operations and evaluation, maintenance, inspection and testing (EMIT) tasks. Hence along with the systems design development, there will be a requirement for further HF work post-GDA. The requirement for further work in all topics post-GDA is addressed through the use of suitable formal handover arrangements to the future licensee.

This chapter demonstrates that the risks associated with human aspects of the design and assumed operation of the UK ABWR are ALARP, as far as is possible for the status of the design within the GDA. It is acknowledged that further work will be required post-GDA to further develop the UK ABWR design and fully incorporate site-specific aspects, particularly the actual operating

organisation structure and operating arrangements. This will require further HF design input and HF analysis, but that will be the responsibility of the future licensee.

27.1 Introduction

This chapter provides an overview of the HF design activities and analysis outcomes that formed an integral part of the UK ABWR GDA. It also provides a high-level description of the overall structure of the HF safety case showing where greater detail on the claims, arguments and evidence is presented. This more-detailed information is contained in a set of topic reports (TRs) and supporting technical reports, and includes the HBSC Report [Ref-1], which is in essence the Basis of Safety Case (BSC) for the HF topic area. The TRs and other supporting documents are shown on a document map (Appendix C to this chapter) which is used to show the links from the various sources of evidence to the claims and arguments, and back to the overall safety case.

27.1.1 Background

Current good practice in the UK requires consideration of HF in nuclear power plant design. This should be undertaken such that HF is addressed throughout the plant's lifecycle, though it is especially important to address HF during the design stage. Timely and adequate consideration of HF in the design of a system is key to achieving the system's fundamental safety functions and ensuring risks from human interactions with the system are managed to ALARP.

Hitachi-GE has a long history of designing, manufacturing and providing support to operations of over 20 nuclear power plants. This started with the original Boiling Water Reactor (BWR) in the 1960s and developed through the evolution of the ABWR [1] over three generations of design. Elements of HF have formed a part of Hitachi-GE's core design and engineering processes for much of that history. This has been achieved through the use of standards and good practice guidance and the incorporation of lessons-learned. The inclusion of HF principles within design requirements has enabled a reduction in human error (in general terms), optimisation of workload and improvements in operability throughout the historical development of the reactor. Thus, the benefits from the formal and informal integration of HF is embedded in the current Japanese J-ABWR design, a design which forms the baseline for the UK ABWR.

To develop the baseline J-ABWR into the UK ABWR design, a formal structured Human Factors Integration (HFI) programme was developed. This comprised suitable design support and analysis activities in accordance with current good practice for the UK nuclear industry.

The scope of the UK ABWR GDA HFI programme covered the entire plant design in all operating and fault modes. The scope was such that the depth of coverage of HF in each area and for each plant mode was proportionate to risk. The HFI programme was focused on identifying and substantiating human actions required to achieve the UK ABWR Fundamental Safety Functions (FSFs) and defining basic HF requirements for the plant design to meet the NSEDPs[2] [Ref-2]. These actions and design properties comprise the HBSCs, i.e. the human action "functional" claims and HF

[1] As with other chapters of this PCSR, "ABWR" refers to the basic reactor type, "J-ABWR" indicates the reference Japanese plant design and "UK ABWR" is the design of the generic UK plant undergoing GDA.

[2] The FSFs and NSEDPs for UK ABWR are presented and described in detail within Chapter 5: General Design Aspects and its supporting documents.

design and organisational "property" claims. This focus ensured the HBSCs were effectively understood and that the design supported their successful achievement.

In line with the Safety Case Development Manual (SCDM) [Ref-3], the HBSCs were identified and categorised as one single group of claims separately from the SFCs and SPCs within the UK ABWR safety case. This single grouping ensured more effective understanding of reliance on the human element of the system for successful and safe UK ABWR plant operation, and good visibility of the HF aspects of the safety case. This also then allows for effective implementation of the required organisational and operational arrangements to support the HBSCs by the future licensee.

The structure and content of this chapter is centred around the HFI programme, its activities and its results. These provide the case for the adequacy of the HF activities undertaken for UK ABWR GDA. This includes explaining how the human actions required to achieve the FSFs were adequately identified and substantiated.

27.1.2 Document Structure

Each chapter of the PCSR stands as the head document for that topic area, providing the links to relevant other chapters within the PCSR and its own network of BSCs and supporting reports. Thus, each chapter consists not only of its own content, but the content of all the linked documents.

Chapter 27 Overview

The remainder of this chapter comprises the following sections:

Section 27.2 Purpose and Scope: Explains the purpose of the chapter and items that are considered within and out of scope of the safety justification for this topic area for GDA.

Section 27.3 UK ABWR Integrated Human Factors Programme: This section provides a description of the programme of integrated HF design support and analysis activities undertaken for GDA. It summarises how appropriate methods were chosen and their outputs documented. It also describes in detail how HF interfaces with other relevant topic areas. Finally it explains how HF issues have been managed and resolved in GDA, such that any risks from HF can be shown to be reduced to ALARP.

Section 27.4 Baseline HF Position: This section summarises the preliminary HF activities. It establishes the level of HF that was included within the baseline, reference plant design. In order to capture the extent that HF requirements were embedded in the existing J-ABWR design, a baseline HF assessment was conducted which is summarised in this section. Where the assessment identified gaps and shortfalls, linkages were provided to the HFI programme to demonstrate how they would be addressed in GDA.

Section 27.5 Human Factors in GDA: Activities and Results: This section summarises the design support, HF analyses and safety case support activities conducted throughout GDA. In summarising the key results it demonstrates the effective implementation of the HFI programme.

Section 27.6 Structure and Substantiation of HBSCs: This section provides a description of the structure of the high-level HBSCs that support the achievability of the SFCs and SPCs made throughout the Generic PCSR. It summarises the processes used to identify the specific claims that support the High Level Safety Functions (HLSFs) and thus ultimately the FSFs. It also provides links to the arguments and evidence which are presented in detail within the HBSC Report [Ref-1].

Section 27.7 Assumptions, Limits and Conditions for Operation: This section provides a high-level overview of the approach to capturing any assumptions made within the HF design and analysis work in GDA. It also summarises the links from the other chapter limits and conditions for operation (LCOs) to the HF topic area.

Section 27.8 Summary of ALARP Justification: This section provides a summary of the ALARP justification that appears within the UK ABWR GDA HF ALARP Report [Ref-4].

Section 27.9 Conclusion: This section provides a summary of the main aspects of this chapter.

Section 27.10 References: This section lists documents referenced within this chapter.

Appendices: These provide: a list of the HBSCs (both functional and property types of HF claims), showing links to SFCs and SPCs; relevant HF Engineering Standards; and the chapter's document map.

Chapter 27 Supporting Documents

Key to meeting the objectives of this chapter is collecting the body of information that forms the arguments and evidence that substantiate the HBSCs. This PCSR chapter consists of an entire suite of documents that make up the chapter as a whole; as shown in the document map within Appendix C. As with the other chapters, this document is the "Level 1" safety case document; it is directly supported by the Level 2 documents shown in the document map. Those Level 2 documents are themselves underpinned by many more Level 3 documents (only shown in an indicative way within the document map) that provide further detail.

This HF chapter is slightly different to both the engineering and the other analysis chapters; in essence the HF topic area is a combination of both engineering and analysis. As such, it does not have a "BSC" labelled as such like the engineering topics do. However, one of the TRs in the document map, the HBSC Report [Ref-1], essentially is the BSC for the HF topic, containing all the human action claims, and the arguments and evidence that substantiate them, for the entire generic PCSR. The other Level 2 documents within the document map are the supporting TRs, with the HF "design" TRs being supported by Level 3 documents that are more design engineering in nature (technical queries, design verification reports, etc.), and the HF "analysis" TRs supported by analysis supporting reports.

The supporting documents capture the information required to demonstrate the achievability of the HBSCs. In doing so they provide justification that the design supports the claimed human actions and ensures the risk from human error is reduced to ALARP. The following is a summary of the purpose of the key Level 2 documents and how they contribute to the substantiation of the HBSCs

and ALARP justification. Further detail is provided in Appendix C for each document shown within the document map. Key documents include:

- The Baseline HF Assessment Report (BAR) [Ref-5], and the HFI Plan (HFIP) [Ref-6] along with the HF Methodology Plan (HFMP) [Ref-7] set out the HF that was already integrated into the ABWR reference design and the further programme of HF support that was integrated into the UK ABWR design. This demonstrates the suitable and sufficient consideration has been given to HF principles within the design and safety analysis in accordance with modern relevant good practice.
- The HF Design and Engineering Report (HF DER) [Ref-8] with its key supporting references, particularly the HF Engineering Specification (HFE Spec) [Ref-9], demonstrate that the intended HF support to the design has been effectively undertaken.
- The HF Assessment Report (HFAR) [Ref-10] and its supporting references (in particular the Human Reliability Analysis Report (HRAR) [Ref-11]), demonstrates that appropriate HF analyses have been undertaken during GDA to underpin the functional HBSCs and inform the design.
- The Requirements Compliance Tracking Matrix (RCTM) [Ref-12] and the HF Issues Register (HFIR) report [Ref-13] are the means for demonstrating that the 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 (HFVP) [Ref-14] and all the resulting verification and validation (V&V) output, as captured in the HF V&V Report (HFVR) [Ref-15] provide the demonstration that the assumptions made within the analysis are valid and the recommendations made for the design have been implemented. To the extent possible within GDA, the V&V activities within the HFI programme are intended to demonstrate the link between the design and analysis.
- The ALARP Report [Ref-4] documents the ALARP justification as it stands at the end of GDA. Where further activities to develop the ALARP justification are necessary, the remaining work will be handed over to take place in the site-specific stage.

The above are the key references that contain the arguments and evidence that substantiate the HBSCs. Taken together, the above documents and their supporting references provide the case that suitable and sufficient consideration has been given to HF within the UK ABWR design and that the claimed human actions are achievable.

Links to Other Chapters

This chapter provides links to other key chapters within the safety case that form part of the case for the HF topic area. In practice, HF considerations are relevant to most chapters of the PCSR to varying extents, so only the main links are specifically identified here. The main links of this chapter with other Generic PCSR chapters are as follows:

- The most significant links for the HF analysis and identification of HBSCs are to the analysis chapters of: Chapter 24: Design Basis Analysis; Chapter 25: Probabilistic Safety Assessment; and Chapter 26: Beyond Design Basis and Severe Accident Analysis.
- As per the SCDM [Ref-3], the SFCs identified in the engineering chapters list any required supporting system SFCs as arguments within their BSCs. Functional HBSCs required to support the achievement of the SFCs for Structures, Systems and Components (SSCs) are identified in this way. The most important links to the engineering chapters are with Chapter 21 Human Machine Interface and Chapter 14: Control and Instrumentation. These are important because the HMIs provide the primary physical means to perform the human actions required to support the SFCs.
- Of the other engineering/systems chapters, the main reactor and non-reactor systems chapters that relate closely to the HF design activities and the identification of functional HBSCs are: Reactor Coolant Systems, Engineered Safety Features, Electrical Systems, Auxiliary Systems, Radioactive Waste Management, Fuel Storage and Handling, and Spent Fuel Interim Storage (Chapters 12, 13, 15, 16, 18, 19 and 32, respectively).
- There are close links to Chapter 5: General Design Aspects. The categorisation of safety functions and safety classification of SSC in this chapter conform with the methodology described in PCSR Chapter 5, Section 5.6. Additionally, the general requirements for Equipment Qualification, Examination Maintenance Inspection and Testing (EMIT) and codes and standards that come from this safety categorisation and classification are also described in Chapter 5, sections 5.7 and 5.9, respectively. Further details can be found in the EMIT section of the corresponding Basis of Safety Case document referred to for the PCSR section. Chapter 5 also addresses compliance with the Hitachi-GE NSEDPs.
- General requirements for decommissioning of the systems, structures and components within this chapter scope are described in PCSR Chapter 31: Decommissioning. Although the specific safety claims for decommissioning are not developed at this stage, HF played an important role in demonstrating that the UK ABWR plant as at GDA could be decommissioned safely and that no significant HF issues have been identified at this stage of the design (noting the strategic nature of the decommissioning case at this time).
- General requirements related to conventional safety aspects are described in PCSR Chapter 4: Safety Management throughout Plant Lifecycle, particularly sections 4.7 through 4.11, which describes the safety arrangements in all phases of the plant. Chapter 4 also includes a detailed description of the Assumptions, Limits and Conditions for Operations for the plant as at GDA (see Section 27.7).
- As described within Section 27.2.2 Scope, HF related to security and environmental protection aspects of the plant design are covered more explicitly outside the PCSR. Chapter 1: Introduction gives further detail of the generic links to the Generic Environmental Permit (GEP) and Conceptual Security Arrangements (CSA) documentation.
- Finally, because HF and the HBSCs also span from the system to the organisational aspects of the plant, this chapter also has strong links to the following “operations” chapters: Safety Management, Radiation Protection, Emergency Preparedness, Commissioning, Operations, and Decommissioning (Chapters 4, 20, 22, 29, 30 and 31, respectively).

27.2 Purpose and Scope

27.2.1 Purpose

The purpose of this GDA PCSR chapter is to demonstrate that the risks associated with the human element of the UK ABWR plant generic design have been managed to be ALARP as at the end of Generic Design stage.

This is achieved by presenting a concise, coherent record of the HF-related activities carried out as part of the GDA HFI programme. The HF activities comprising the HFI programme were selected to provide suitably proportionate and sufficient consideration of good practice HF principles. This effectively covered two workstreams, design and HF analysis. The results of both streams of activities are summarised in this chapter and its supporting documents. In this way, the chapter provides the means to substantiate the HBSCs and enables the ALARP justification to be made.

Specific objectives of the chapter are to:

- Describe the programme of integrated HF design support and safety-related analysis activities that ensure the UK ABWR generic design takes adequate consideration of HF. This covers both the generic antecedent or "pre-set" requirements (i.e. codes and standards for HF) and plant-specific task-based "emergent" requirements.
- Describe the structure of the UK ABWR HBSCs, and explain how these link to the FSFs and High-Level Safety Functions HLSFs.
- Capture and summarise the explicit and implicit claims on human actions made throughout the remainder of the GDA PCSR chapters and their supporting documents.
- Demonstrate that the set of HBSCs identified is as complete as possible at the end of generic design stage.
- Describe, or provide references to where the detailed arguments and evidence can be found in the supporting documentation.
- Using the arguments and evidence, demonstrate so far as is reasonably practicable at GDA, that all of the identified HBSCs are achievable. Thus, demonstrating that the human element of the generic UK ABWR plant can successfully contribute to achieving the FSFs as required.
- Provide links to information that can be used to demonstrate compliance of the UK ABWR generic design with the sections of Hitachi-GE's Nuclear Safety and Environmental Design Principles (NSEDPs) [Ref-2] relevant to HF[3].
- Identify links to relevant content of other GDA PCSR chapters. This ensures consistency across the whole safety case and that the safety case presented is complete.

[3] Compliance with NSEDPs is a key part of demonstrating that the UK ABWR is safe. Relevant principles from the UK ABWR NSEDPs form the starting point for all the SPCs. Although HF itself as a topic area does not have SPCs, there are HBSCs that are intended to act as HF SPCs (see Section 27.6); these are linked to the NSEDPs where applicable.

- Detail the mechanisms and activities that support the effective capture and hand-over of assumptions and outstanding HF issues/activities for further development during the site-specific stage.

27.2.2 Scope

Within the HF topic area, the principles, issues and requirements are broad, and they impact on, and are affected by most of the other technical topic areas within design, operations and safety analysis. Because of this, the scope of the GDA PCSR for the HF topic area covers:

- All relevant HF activities that form part of the GDA HFI programme.
- 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.

The scope of the overall GDA HFI programme is proportionate and risk-based. It covers all areas of plant and related operations that potentially impact:

- Process and personnel nuclear safety.
- The environment.
- Plant and site security.

The scope of this PCSR chapter and its supporting documents is solely those areas of plant and related operations that potentially impact on process and personnel nuclear safety.

Human action claims that form part of the environmental case and underpin the GEP [Ref-16] are identified within the HFI programme of work. A certain level of achievability of those claims is justified through the HF design support given during GDA, since environmental equipment and related plant processes were within scope of the HFI programme. In addition, some of the claimed human actions within the GEP overlap with the Radioactive Waste Management HBSCs; these claims are within scope of this chapter, but the remainder of the GEP claims on human action are not within the scope of this chapter (see item 4 below).

The following are not within scope of this chapter.

(1) System descriptions for, and complete list of associated SFCs and SPCs of HMIs that are used to perform some of the human actions that are claimed as HBSCs. Based on the agreed scope of each topic area within GDA, these items are fully covered by Chapter 21: Human-Machine Interface. Note that, similar to HBSCs, the SFCs for HMIs are identified (in the relevant systems chapters supporting BSCs) as arguments that demonstrate the achievability of SFCs for other SSCs.

(2) Different SSCs have been developed to different levels of design maturity within the GDA stage. As such, for SSCs that are only at basic or early concept design, any part of the HF assessment and V&V that cannot be performed until the detailed design of the SSCs has been completed, will not be available to substantiate the related HBSCs. For example, it is

not planned that the HMI designs will all be fully mature within the timescales of GDA. Detailed design of the HMIs is expected to be undertaken during the site-specific phase. This impacts the amount of HF-related evidence that can be developed within the GDA phase. (The expected design maturity of the HMIs is discussed in more detail in the Scope section of Chapter 21.) Therefore, further work to substantiate the HBSCs will be required post GDA. This will need to be reported in the corresponding site-specific stage PCSR HF chapter and its supporting documents.

(3) The plant and site security systems/arrangements were only developed as a high-level strategy and concept during GDA. This was captured in the CSA document [Ref-17]. Although security has direct links to nuclear process and personnel safety, the scope of security systems and any related claimed human actions that support the security case are outside of the scope of this chapter. These systems and their claims are expected to be developed in the site-specific stage of UK ABWR development.

(4) Environmental aspects of the UK ABWR design, other than GEP claims linked to Radioactive Waste Management claims, as described in the included scope, above. For generic links to GEP documentation, please refer to Generic PCSR Chapter 1.

27.3 UK ABWR Integrated HF Programme

27.3.1 Introduction

The HF topic area sits within the analysis chapters of the PCSR however because of the nature of HF, this chapter does not only address analysis. It covers HF analysis, design-related HF engineering, and summarises functional claims. Both the HF analysis and design support are required to demonstrate that all key HF risks (see Section 27.8.1) are reduced to ALARP.

There are four elements of the HF programme of activities that demonstrate that it was sufficient to meet the relevant HF SPCs and therefore the applicable NSEDPs (see Section 27.6):

(1) A systematic approach was taken to the management and integration of HF activities within GDA.

The HF analyses undertaken for GDA were appropriate, because they addressed:

- The Allocation of Function (AoF) between humans and engineered systems.
- Task analysis.
- Analysis of staffing levels.
- Human Reliability Analysis (HRA).

HF was addressed within the design generally and specifically in relation to:

- Workspaces.
- Human system interfaces.

The safety claims involving humans were identified and substantiated.

Though noted separately above, these four elements did not exist in isolation to one another. Many interactions were required between these elements of the HFI programme to achieve the substantiation of the HBSCs. The first element, the use of a systematic approach, was primarily a function of the HFIP [Ref-6] as described in this section, and its effective implementation is covered by Section 27.5. The second and third elements are discussed in Section 27.5. In relation to the fourth element, the identification and substantiation of the HBSCs is discussed in Section 27.6.

27.3.2 Human Factors in Complex Systems Design

HF is a broad and holistic discipline that impacts and interacts with most traditional engineering disciplines as well as health and safety. The impact and interaction of HF takes place throughout all stages of the system lifecycle. HF is applied contextually, with the specific industry and type of systems dictating its focus. As such, there is no single correct way to apply HF to a complex system design. Therefore, to ensure the effective consideration of HF within a project, it is necessary to ensure it is integrated with the specific project management and design processes.

An HFI process was developed to ensure that the equipment, process and people components of a complex system are considered in a balanced manner during system design and that the resulting

system is able to work effectively and safely. HFI is essentially a sub-set of the project management effort for any large or complex system design project. It is used as a tool to define an effective programme of HF support for the project and ensure the timely and adequate consideration during the design stage of the entire extent of human involvement in the system throughout its intended life.

Using effective HFI principles, the programme of HF supporting activities for any project is designed to be fully integrated with the project schedule, processes and organisation(s). This provides the necessary analysis and support in a timely manner, as early as possible in order to be cost-effective.

For UK ABWR GDA, the HFI programme provided the means to ensure that:

- The "broader holistic assessment across a range of important HF aspects" required by the Office for Nuclear Regulation (ONR) GDA guidance [Ref-18] has been conducted in a well-managed and traceable fashion.
- The Hitachi-GE UK ABWR NSEDPs [Ref-2] related to HF, plus the broad HFI and specific HF requirements for design and analysis identified by the specialists in the Hitachi-GE HF Team have been demonstrably met (as per PCSR Chapter 5: General Design Aspects and the RCTM [Ref-12], respectively).
- The Environmental Agency (EA) Radioactive Substances Regulation (RSR) Environmental Principle (REP) ENDP5 [Ref-19] for HF and any HF-related requirements derived from other REPs have been demonstrably met[4].
- The UK ABWR HBSCs – which include environmental safety – were adequately developed and validated in a systematic fashion and sufficiently substantiated through the course of UK ABWR GDA.

HFI programmes are customised to meet specific project needs, system characteristics, risk levels and stakeholder requirements. Therefore, the HFI programme is always bespoke and is defined and managed through the use of a HFIP [Ref-6]. This section summarises the HFI programme for UK ABWR during GDA. The summary demonstrates that the programme as planned was suitable and sufficient to ensure that the activities were focussed on reducing the key risks related to HF in the UK ABWR to ALARP (see Section 27.8).

27.3.3 HF Integration: Planning and Management

The UK ABWR GDA HFIP [Ref-6] defines how Hitachi-GE managed the integration of HF into the development of the UK ABWR for the GDA in order to meet international HF good practice. The plan outlines the HF activities for the project and details the processes by which the HF analysis and expertise was provided to the relevant GDA design and safety analysis teams.

Specifically the HFIP [Ref-6] details how the programme ensured that HF support was provided:

[4] It is recognised that the EA REPs are intended for use by the Regulators when assessing plant designs; however, the requirements for the UK ABWR GDA HFI programme have been derived in part from the guidance contained within those regulatory documents.

- to the design of the equipment and processes to be used within the plant;
- to help meet safety, operational and end-user requirements;
- in a timely manner; and
- at an appropriate level, commensurate with the project and facility risks.

This last point is essential in demonstrating that the programme was planned to effectively address and resolve key known or expected HF risks and issues. As mentioned, HF is a broad discipline, with relevance to and impact on many different system topic areas. In addition, there are many different ways to approach integrating HF into a complex design project and different methods to use for each activity. No HFI programme can do every possible activity in every different area of system. To do so would involve grossly disproportionate time and effort for the benefit gained. The HFI programme must be designed to be proportionate and risk-based, providing a suitable breadth of coverage across the system design and relevant topic areas, with adequate depth to the activities in key areas where risk, and therefore potential for risk reduction, is greatest.

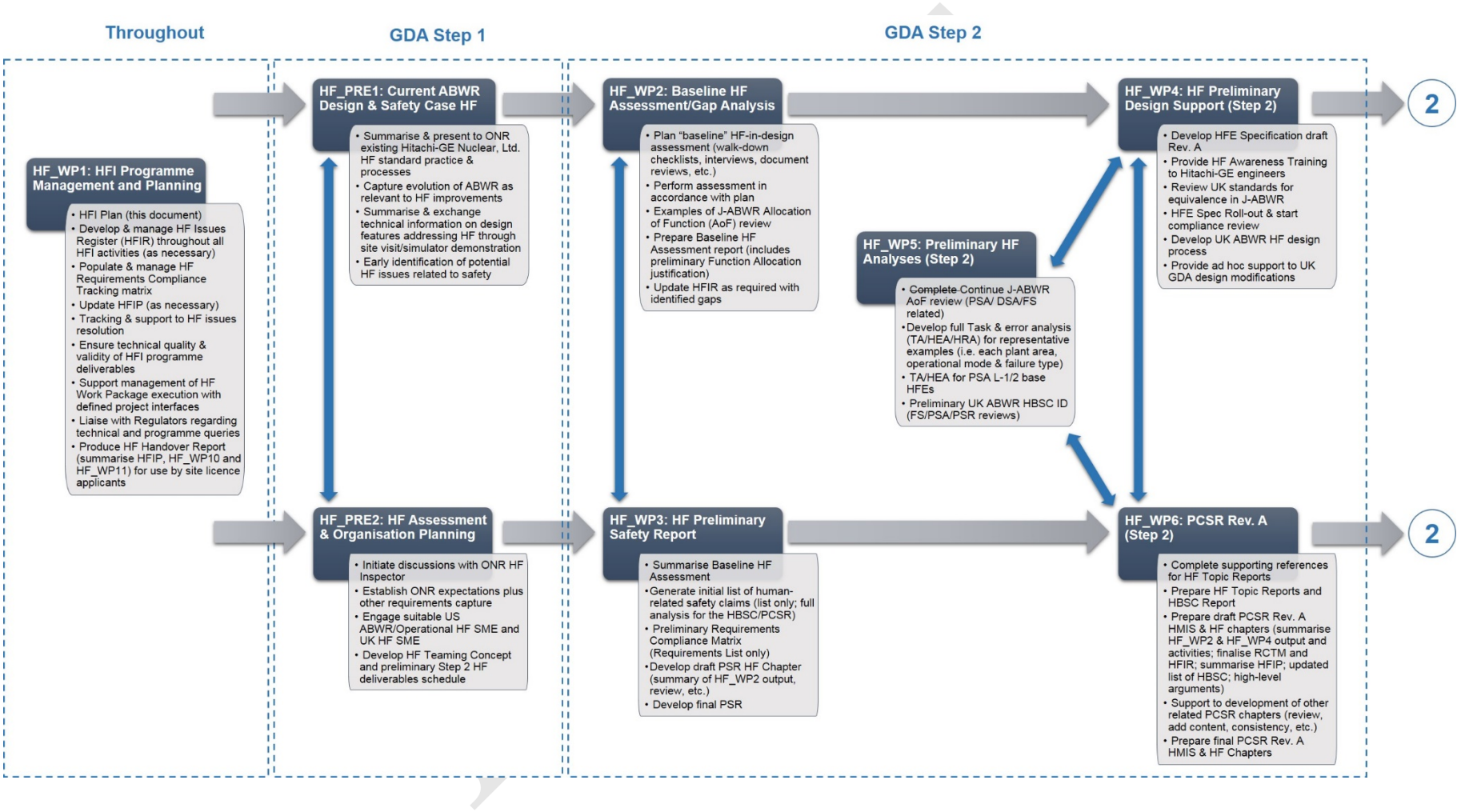
The HFIP details the basis for determining a proportionate set of HF activities for UK ABWR in the GDA stage. It outlines and justifies how the activities were chosen on that basis. This includes the following criteria for the programme as a whole:

- It is based on national and international good practice in the industry for which the system is designed for (i.e. systems used in rail, or oil and gas, or defence, will necessarily have different risks and therefore different HFI programmes required to be effective).
- It takes cognisance of key known or expected risks, identified based on operational experience, current safety analysis, and competent HF expert judgement.
- It recognises the evolving nature of the ABWR plant design by understanding the baseline design HF, identifying not only gaps and shortfalls, but areas where further HF is unlikely to produce much benefit in terms of risk reduction.
- It reflects the overall priorities and scope of the programme, ensuring that the level of effort is commensurate with the intended progression of the design and safety case in any given area.
- It includes a balance of activities that are both “fixed” and responsive in nature, to reflect the iterative nature of, and emerging issues within related design and safety analysis activities.

By using the above criteria, Hitachi-GE HF team ensured that the chosen HF activities, their timing and their scope were suitable and sufficient to enable key HF risks to be identified and reduced to ALARP.

As it is essentially a project management plan, the HFIP was treated as a live document throughout GDA and has been updated regularly as required. The HFIP defines the required HF Activities as “Work Packages”; each Work Package describes: the approach or methodology to be used, inputs, outputs, constraints and dependencies, timescales and project milestone links (as appropriate). The HF and/or project resource required to undertake the activity is also given to ensure that activities are conducted in a competent manner.

The HFIP for GDA outlines two interrelated streams of HF activities supporting both optimal consideration of HF within the development of the UK ABWR design and HF analysis to feed into the design requirements and substantiate the safety case claims. An overview of the HFIP activities is provided in Figure 27.3-1. As with the rest of GDA design and PCSR, these activities have been conducted in an iterative and staged way to align with the state of design and safety analysis at any given time. Section 27.5 gives a summary of the outputs and impact of these activities on the UK ABWR design and safety case for GDA.


Throughout
GDA Step 1
GDA Step 2
HF_WP1: HFI Programme Management and Planning
• HFI Plan (this document)
• Develop & manage HF Issues Register (HFIR) throughout all HFI activities (as necessary)
• Populate & manage HF Requirements Compliance Tracking matrix
• Update HFIP (as necessary)
• Tracking & support to HF issues resolution
• Ensure technical quality & validity of HFI programme deliverables
• Support management of HF Work Package execution with defined project interfaces
• Liaise with Regulators regarding technical and programme queries
• Produce HF Handover Report (summarise HFIP, HF_WP10 and HF_WP11) for use by site licence applicants
HF_PRE1: Current ABWR Design & Safety Case HF
• Summarise & present to ONR existing Hitachi-GE Nuclear, Ltd. HF standard practice & processes
• Capture evolution of ABWR as relevant to HF improvements
• Summarise & exchange technical information on design features addressing HF through site visit/simulator demonstration
• Early identification of potential HF issues related to safety
HF_PRE2: HF Assessment & Organisation Planning
• Initiate discussions with ONR HF Inspector
• Establish ONR expectations plus other requirements capture
• Engage suitable US ABWR/Operational HF SME and UK HF SME
• Develop HF Teaming Concept and preliminary Step 2 HF deliverables schedule
HF_WP2: Baseline HF Assessment/Gap Analysis
• Plan "baseline" HF-in-design assessment (walk-down checklists, interviews, document reviews, etc.)
• Perform assessment in accordance with plan
• Examples of J-ABWR Allocation of Function (AoF) review
• Prepare Baseline HF Assessment report (includes preliminary Function Allocation justification)
• Update HFIR as required with identified gaps
HF_WP3: HF Preliminary Safety Report
• Summarise Baseline HF Assessment
• Generate initial list of human-related safety claims (list only; full analysis for the HBSC/PCSR)
• Preliminary Requirements Compliance Matrix (Requirements List only)
• Develop draft PSR HF Chapter (summary of HF_WP2 output, review, etc.)
• Develop final PSR
HF_WP5: Preliminary HF Analyses (Step 2)
• ~~Complete~~ Continue J-ABWR AoF review (PSA/ DSA/FS related)
• Develop full Task & error analysis (TA/HEA/HRA) for representative examples (i.e. each plant area, operational mode & failure type)
• TA/HEA for PSA L-1/2 base HFEs
• Preliminary UK ABWR HBSC ID (FS/PSA/PSR reviews)
HF_WP4: HF Preliminary Design Support (Step 2)
• Develop HFE Specification draft Rev. A
• Provide HF Awareness Training to Hitachi-GE engineers
• Review UK standards for equivalence in J-ABWR
• HFE Spec Roll-out & start compliance review
• Develop UK ABWR HF design process
• Provide ad hoc support to UK GDA design modifications
HF_WP6: PCSR Rev. A (Step 2)
• Complete supporting references for HF Topic Reports
• Prepare HF Topic Reports and HBSC Report
• Prepare draft PCSR Rev. A HMIS & HF chapters (summarise HF_WP2 & HF_WP4 output and activities; finalise RCTM and HFIR; summarise HFIP; updated list of HBSC; high-level arguments)
• Support to development of other related PCSR chapters (review, add content, consistency, etc.)
• Prepare final PCSR Rev. A HMIS & HF Chapters
2
2

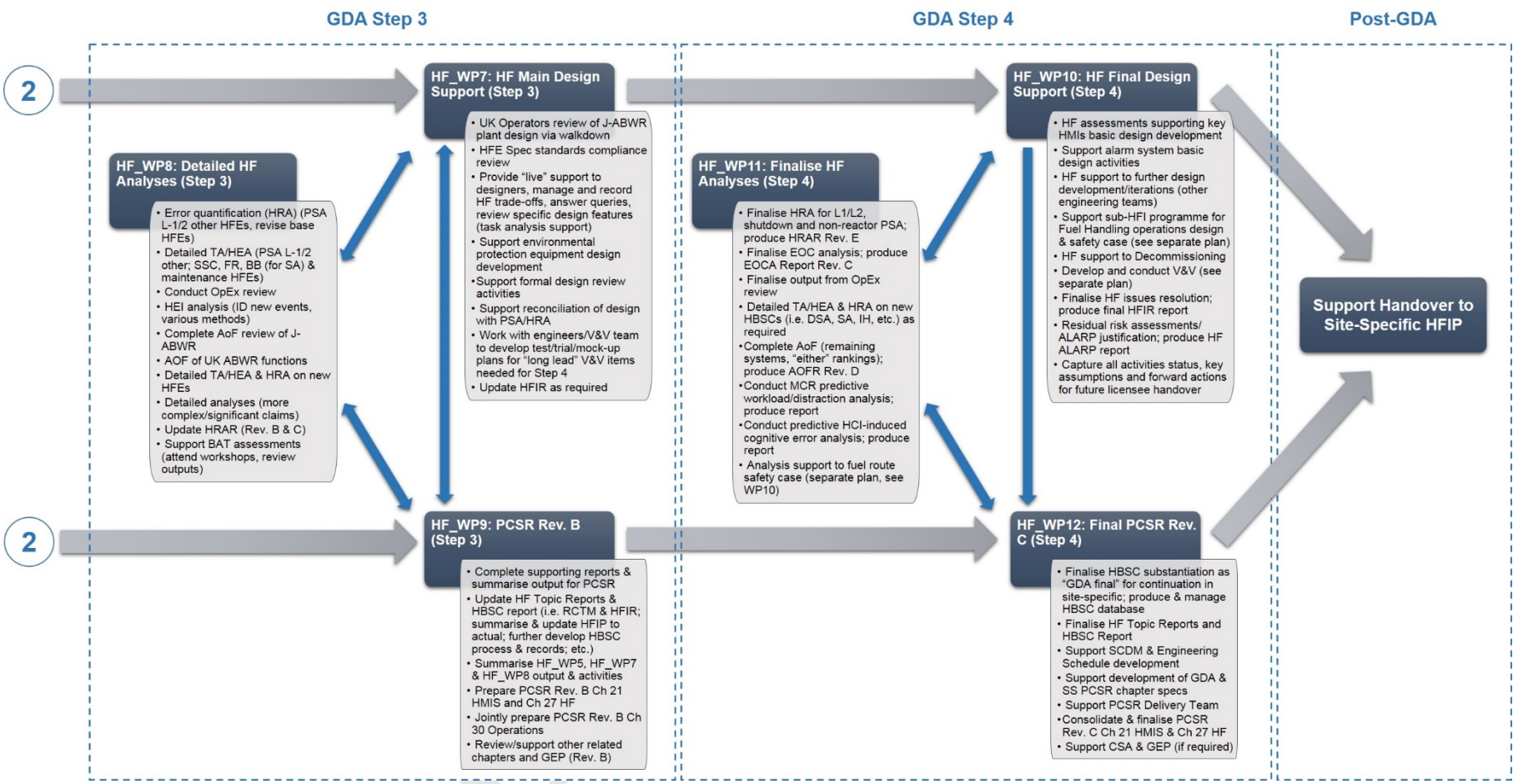


Figure 27.3-1: Overview of Hitachi-GE HFI Programme

27.3.4 HF Processes and Methodologies

Within the HFIP [Ref-6], HF activities are described and planned at a relatively high-level. For some activities, the method to be used is more involved and needs greater description than that given in the HFIP. In addition, for many types of HF analysis, there is a choice of tools and/or techniques within the range of what constitutes HF good practice. In such cases, selection of an appropriate tool or technique is required with appropriate justification regarding its applicability.

To provide greater detail than what was appropriate in the HFIP and to support the descriptions of activities within the HF Work Packages, the HFMP [Ref-7] was developed. The HFMP provides:

- detail regarding the processes, tools and techniques that were used to carry out HF activities within the HFI programme; and
- justification (where appropriate or required) as to the suitability and adequacy of the methods chosen.

The HFMP ensured, and helps demonstrate that the results, conclusions and recommendations from the activities within the HFI programme are valid by being based on good practice up-to-date analysis techniques.

27.3.5 Interfaces with Other Topic Areas

As a broad cross-cutting topic, HF is impacted by and, conversely, has an effect on most other technical topic areas. The HFI programme included HF activities that span the entirety of GDA. This included managing interfaces with any related or affected technical areas within the GDA stage of the UK ABWR design. Managing these interfaces was performed through informal and formal means as described in the HFIP [Ref-6]. This allowed effective management of a complex set of interfaces to ensure cross-cutting HF issues were effectively identified and resolved throughout GDA.

The interface points and level of interaction of HF topic area with, or the impact from HF on the other topic areas are shown in Table 27.3-1. Note that these are areas of technical and design activity for GDA; they are not necessarily all within scope of this PCSR. The complete list is shown to demonstrate the comprehensiveness of the GDA HFI programme.

Table 27.3-1: HF Interfaces in the GDA Project

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.

No.	Topic Area	Potential HF Interface/Impact
3	C&I	Fully integrated topic: Main focus of HF is to support design of the Main Control Room (MCR)/local panel HMIs; an area of continuously integrated working.
4	Probabilistic Safety Analysis (PSA) & Fault Studies	Fully integrated topic: human-related claims (implied and explicit) in safety studies need Suitably Qualified and Experience Person (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.

No.	Topic Area	Potential HF Interface/Impact
16	Radiological Protection	Medium interface: administrative arrangements and plant design for reducing and monitoring dose uptake must include 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	Radwaste	Medium interface: design of fuel handling & radwaste plant and systems must include consideration of HF as per operating plant design.
19	GEP	As above for security & internal hazards, interface to support design/assessment of human-related environmental protection claims.

27.3.6 HF Issues Management

The main goal of the proposed HF activities within the HFI programme is to identify and resolve all HF issues affecting the correct functionality, maintainability, safety operation and through-life management of the UK ABWR. HF issues management is described in detail within the HFIP [Ref-6]. HF issues were defined as shortfalls with regards to usability, operability, maintainability and HF GDA process (e.g. topic area interfaces). These may relate to observed or expected features of the UK ABWR plant design. They may also relate to assumptions underpinning analysis, or proposed operations that require reliable human performance to deliver safety. HF issues were also captured for behaviours and activities within the project that did not meet the stated requirements for HFI.

The task-analysis based and functionally-related HF requirements (i.e. those related to achievement of HBSCs) were the result of analysis activities within GDA. They were therefore “emergent” in nature. This meant they had UK ABWR context-dependent solutions (as opposed to fixed HF requirements set by the HF good practice standards and guidance distilled into the HFE Spec [Ref-9]). In addition, because the UK ABWR is an evolutionary design, many of these recommendations were regarding changes to the existing design. As such, where specific requirements were recommended because the required features were different to, or non-existent in the reference plant design, these were also tracked using the HF issues process. Use of the single register to capture and track recommendations for the design allowed simpler management of those “emergent” HF design requirements. It also enabled cohesive tracking of them to ensure implementation of the HF requirements was balanced against other potentially conflicting design requirements in accordance with ALARP principles.

To ensure effective tracking and resolution of HF issues, the issues were captured in the HFIR [Ref-13] by the HF Team. These were also recorded in the project-wide risk register database.

27.3.6.1 HF Issues and Recommendations Tracking and Resolution

Following the entry of HF issues (including emergent HF design requirements arising from analysis) in the HFIR [Ref-13], the HF Team or relevant design team (as appropriate for each issue) then managed the progress and resolution of the issues through regular design issues resolution meetings. Each HF issue was resolved in accordance with the ALARP principle. This required each HF issue to be assessed in terms of its unmitigated risk level and the cost and technical feasibility of any recommended resolution to the issue (elimination, control or mitigation) to be defined. Note that some issues were assessed as tolerable and ALARP without any recommended resolution. In these cases this was documented within the HFIR [Ref-13].

Where a HF issue necessitated a change, a request was made by the HF Team to the appropriate engineering or analysis team in accordance with the Hitachi-GE design change management system. Cost-proportionate and feasible modifications were identified through consultation with the relevant designers and engineers. Recommended modifications were recorded in the HFIR against each issue. The HFIR was also used to capture: "live" design decision-making; items resolved through design reviews; and items resolved by integrated engineering team members who made changes in situ.

Where HF issues were claimed as "Closed" by the design team, the actual resolution was recorded against the issue. In cases where the implemented resolution differed from that recommended by the HF team, a SQEP HF specialist ensured that the resolution was adequate to address the original issue. Any further assessment through V&V that was needed to assess the adequacy of the issue resolution was also noted. For those items where V&V suitable to ensure issue closure can only be conducted post-GDA, the status of the issue will remain open until that assurance activity was satisfactorily completed.

The above process and the comprehensive nature of the HFIR [Ref-13] means it provides an audit trail that tracks and documents the impact of the HF effort on the UK ABWR design. This demonstrates how risks associated with HF design issues have been managed to ALARP. It also provides a clear understanding of any HF-related residual risks associated with the plant and operations that can be communicated to future licensees. As some issues can only be resolved in detail design or the purchasing stage, the HFIR [Ref-13] is intended to be transferred to future licensee in order to ensure the open issues are effectively managed in the post-GDA phase.

27.4 Baseline HF Position

27.4.1 Introduction

The consideration of HF within Hitachi-GE's domestic plants (BWR, J-ABWR), as explained in Section 27.1.1, has improved and evolved throughout the history of the reactor. The formal and informal integration of HF can therefore be seen reflected in the current J-ABWR design, a design which forms the baseline for the UK ABWR (the "reference" design). As such, the UK ABWR is starting from a position in which HF considerations have been addressed within the reference design. The design that forms the baseline for UK ABWR is described in greater detail in the ABWR General Description document [Ref-20].

27.4.2 Baseline HF Assessment

In order to capture how the existing J-ABWR design addresses HF considerations, a baseline HF assessment was undertaken. This was identified as an essential preliminary HF activity within the UK ABWR GDA programme. The full details of the assessment are reported in the BAR [Ref-5]. This section provides a summary of the scope, approach and findings.

The purpose of the baseline HF assessment was to:

(1) Understand and demonstrate how HF considerations were already addressed within Hitachi-GE's current processes and the J-ABWR design.

Identify any areas of specific focus for the UK ABWR HFI programme. This would determine how the current J-ABWR design and Hitachi-GE's current processes compare to UK expectations, modern HF good practice and requirements of the expected UK user group. This included paying particular attention to ensuring human actions related to safety are supported and achievable.

In line with the above scope, the objectives of the baseline HF assessment were as follows:

(1) The first objective was to be able to provide a preliminary demonstration that the reference design for UK ABWR has already made significant inroads to addressing HF considerations, as an integral part of the plant design.

There was no expectation that the manner in which HF had been addressed in J-ABWR would have been done exactly to in accordance with what is considered in the UK to be modern HF good practice. Neither was formal documented evidence of how HF had been addressed within the design expected to be readily available in English. Therefore, the second objective of the baseline assessment was for Hitachi-GE to determine and document the breadth and depth of HF considerations within J-ABWR and the existing Hitachi-GE design organisation. This baseline HF position would enable the development of a suitably proportionate HFI programme for the remainder of GDA.

The third objective was to build up the initial body of evidence for features of J-ABWR plant design and safety case that could be carried over to UK ABWR. It must be noted that this third objective was not the primary focus for the baseline assessment and it was expected that such evidence would likely only be suitable and sufficient for less significant claims. It might also require further specific validation for UK ABWR.

27.4.2.1 Assessment Approach

The assessment was carried out using a multi-faceted approach to ensure that the level to which HF considerations were addressed within the baseline ABWR design was truly understood and properly documented.

The review consisted of the following activities:

(1) Defining the scope of the J-ABWR "baseline" design to be reviewed.

Identifying previous HF analysis activities and outputs, including use of Operational Experience (OPEX).

Describing current Hitachi-GE HF processes for designing J-ABWR.

Reviewing J-ABWR allocation of function.

Conducting HF Expert Team Review.

The approach used to carry out these activities is described in detail in the BAR [Ref-5]. The key feature of the assessment approach was to ensure that the assessment drew from a full breadth of plant design and analysis information and used multiple methods and multiple disciplines to draw out the require information. In order to carry out such an assessment in a proportionate and timely manner, a sampling approach was taken. This involved representative information and examples from across the breadth of the design and organisation being selected and reviewed. An audit style of review was performed, with the assessment relying on the collective experience and knowledge of a multi-disciplinary team of Hitachi-GE SMEs. This team had competencies in: HF, including existing international nuclear and other high-hazard industry practices and requirements; ABWR design evolution; systems engineering; fault studies; and safety case.

In defining the baseline design, the key elements of the J-ABWR design that act as human-system interfaces and provide representative actions and design features relating to any known preliminary HBSCs were selected for review. The assessment criteria were compiled from a wide range of modern HF standards, guidance, tools and techniques. The assessment techniques combined the use of:

- Interviews with key Hitachi-GE engineering and related teams, experienced ABWR operations and maintenance personnel, and senior experts with knowledge of the design evolution.
- Review of process documents and records.
- Review of drawings and Computer Aided Design (CAD) models, examining overall design and key specific HF-related elements.
- Assessment of performance of a sample of critical operational tasks during simulated fault conditions.
- Review of as-built design in a suitably representative ABWR operating plant through a systematic walkdown.

27.4.2.2 Summary of Findings and Conclusions

The following are the key findings and conclusions from the baseline HF assessment. These are further detailed in the BAR [Ref-5].

HF Integration in the Hitachi-GE Design Organisation and Processes

Many documents and records providing coverage of HF in specific areas of engineering were received. These were examined and assessed in detail against the selected assessment criteria. These criteria considered the inclusion of HF in: the design of plant and equipment; procurement; operations; EMIT task design; assurance; and for safety analysis, modern safety case requirements relating to the potential for human error. With regard to HF processes, the review also considered the nature and effectiveness of the past approach to HF assessment during ABWR development. Specifically, the HF Engineering (HFE) processes applied for previous domestic projects to integrate HF holistically within the design.

An overview of how HF considerations were historically addressed by Hitachi-GE is given in Figure 27.4-1.

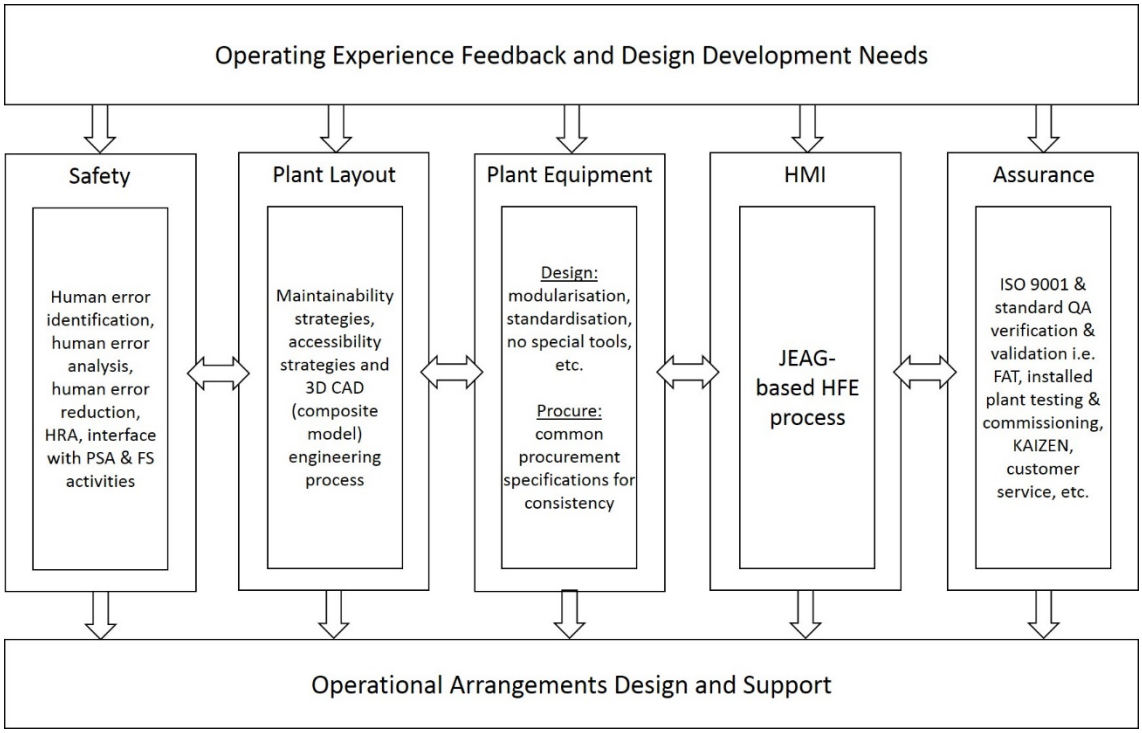


Figure 27.4-1: Overview of Baseline HFI at Hitachi-GE

AoF Review

A key part of reviewing the existing J-ABWR design and an essential requirement for the GDA HFI programme was the review of the baseline Allocation of Function (AoF) within the system. The

review of the existing J-ABWR AoF considered the level and nature of the automated functions of the system and compared them with expectations based on HF good practice.

Note that the possible outcomes from the review for each existing J-ABWR function were:

- Same allocation for UK ABWR (when analysed using the UK criteria), as is currently found within J-ABWR and no change planned for UK ABWR.
- Same allocation for UK ABWR as J-ABWR, but change planned for UK ABWR (discounted at this point as there are no reasons for the HF review to suggest such a change. This could occur later in GDA due to other over-riding design or safety criteria).
- Different allocation result for UK ABWR to current J-ABWR, but no change planned for UK ABWR.
- Different allocation result for UK ABWR to current J-ABWR and change planned for UK ABWR.

A commentary providing justification of the AoF for each function analysed is provided in the detailed tables within Appendix B in the BAR [Ref-5]. The third bullet point above required the most justification. Justification for the decision not to change the allocation, despite the review findings, largely involve other design or operational constraints that would prevent such a change. In some cases the change would not be in accordance with the ALARP principle.

The results of the AoF review were presented in their preliminary form within the BAR. However, due to the extent of information required for the analysis and the scope of systems and functions to be reviewed, the analysis was continued throughout GDA. Further AoF analysis was undertaken for any new functions, where there were design changes, or in response to HF recommendations. Thus the detailed results from the baseline AoF analysis were incorporated into the evolving UK ABWR AoF analysis which is described in Section 27.5.3.1.

HF Expert Team Review: Hitachi-GE Processes & J-ABWR Plant Design

The HF Expert Team reviewed documents, records and the as-built plant. The review determined whether there was evidence that HF considerations had been addressed in a systematic and integrated manner within the design and the safety case, as would be required by modern UK HF good practice.

The review found that HF considerations had been addressed systematically by Hitachi-GE's current processes and within the J-ABWR design. The majority of this HF work had been undertaken and captured formally, in reports, specifications and test/assessment results. This was particularly evident within the C&I engineering discipline in relation to the design of the HMI System (HMIS). Where a less formal approach to HF had been taken, there was still evidence for HF strategies being implemented, embedded HF design criteria and related HF principles (e.g. consistency in purchased parts specifications, minimisation of construction delays through detailed installation sequence planning, etc.). Both the formal and less formal approaches to HF were found to have successfully implemented HF to meet the desired end goals, making for a usable and optimised design. These activities had been underpinned by a rigorous programme of quality assurance (QA), verification and

validation (V&V), continuous improvement through customer feedback, plus management and use of national and international operating experience.

The baseline HF assessment concluded that the current J-ABWR design had been optimised to effectively support successful performance of user tasks. It provided a robust baseline position for the UK ABWR with regards the formal and informal integration of HF considerations. Reference to the long operating history, the carefully managed design development, and the operator feedback that had been implemented provided validation of the baseline design. This evolution had identified and addressed HF issues (where there had been any) with regards baseline plant operations in the domestic plant.

Throughout the baseline assessment, consideration was given to the areas of J-ABWR that may need additional focus during the UK ABWR GDA HFI programme. This included areas where HF considerations were less formally documented. It also considered areas impacted by differences in UK regulatory expectations, modern HF good practice, and differences in the concept of operations (as outlined within the UK ABWR HF Concept of Operations Report (COR) [Ref-21]). These areas of focus, identified through the assessment, fed into the development of the HF programme (see Section 27.3 for greater detail). The consideration of these areas contributed to developing a proportionate and effectively-focussed HFI programme for UK ABWR GDA.

In addition to areas of focus for the GDA HFI programme, the baseline HF assessment identified 26 specific HF issues for resolution in the UK ABWR that were transferred to the HFIR [Ref-13] (issue numbers: HFE-IR-0001-0007, -0013, -0014, -0017, -0027, -0029, -0041, -0042, -0045, -0047, -0051, -0052, -0054, 0081, -0082, -0084, -0089, -0090, -0097, and -0110). The range of issues included: specific design items; checks against UK HF design and engineering standards (as specified in the RCTM [Ref-12]); consideration of differences in safety analysis, such as HRA; and potential issues due to the expected concept of operations (e.g. number of personnel, procedure usage). Where the issues were applicable to GDA stage, the resolution of these was managed through the GDA HF issues management process as described in Section 27.3.5.

27.5 Human Factors in GDA: Activities and Results

27.5.1 Introduction

The HF analyses and design activities undertaken during GDA are key to demonstrating that the risks associated with the human element of the UK ABWR plant generic design have been managed to be ALARP (see Section 27.8), as at the end of Generic Design stage. Section 27.3 has discussed the HFIP and provided justification for its scope. This section demonstrates that the GDA HF activities described in the HFIP were implemented, such that a suitably proportionate and sufficient analysis of the HF risks was undertaken and used to inform the design.

This section addresses the second and third key elements of the GDA HF topic area listed in the introduction to the HFI programme in Section 27.3.1. It summarises the HF activities carried out in support of the design and the HF analyses undertaken. In doing so it also addresses part of the first element. By addressing these three elements the HF activities have also addressed the HF SPCs relevant to GDA (see Appendix B and the HBSC report [Ref-1]).

Demonstration of effective HF support to the design is essential for substantiation of the HF property claims (see Section 27.6) and the purpose of much of the HF analysis was to either support design decisions (and therefore the achievement of HF property claims) or directly substantiate the functional HBSCs (see Section 27.6). In addition, support to other topic areas as part of safety case development ensured that the cross-cutting issues and the content and context of the HBSCs was consistent and able to be substantiated across the case.

This section therefore summarises the content of the two key Level 2 Topic Reports that form part of this PCSR Chapter, the HF DER [Ref-8] and the HFAR [Ref-10] (see Appendix C Document Map).

27.5.2 Design Support HF Activities

This section presents a summary of the HF activities and analysis conducted in support of the evolving UK ABWR design. The activities were defined in the HFIP [Ref-6] and methods for HF support to the design, especially support to the implementation of the HFE Spec [Ref-9] are described in the HFMP [Ref-7]. The design support activities are reported fully within the HF DER [Ref-8] and its supporting references. This report is a key Level 2 document underpinning this chapter (see Appendix C Document Map); it demonstrates that the design-related activities in the HFIP [Ref-6] and the processes described in the HFMP [Ref-7] (see Section 27.2) were implemented as required. It also demonstrates that these activities addressed general aspects of the design, as well as specific key areas where known or expected HF issues arise, such as workspace (for access, reach and clearance, both local to plant and within control rooms) and human system interface design.

27.5.2.1 HF Design-Based Requirements Capture

HF requirements for the UK ABWR project were derived from several sources. The main ones are as follows:

(2) HF standards and HF elements of other design standards (international, Japan and UK).

(2) Hitachi-GE corporate engineering processes.

(3) Hitachi-GE UK ABWR NSEDPs.

(4) Hitachi-GE QA processes for considering operational experience and continuous product improvement in design evolution.

(5) Regulatory (particularly United States Nuclear Regulatory Committee) assessment and design approval findings.

(6) UK ABWR HF SME experience based on international HF good practice.

The requirements were also informed by reference to the UK ONR Safety Assessment Principles (SAPs) [Ref-22] and Technical Assessment Guides (TAGs) related to HF. In referring to these ONR principles and guides, cognisance was taken of the fact they are not prescriptive, nor written as requirements. For UK ABWR GDA, the prescriptive principles are provided by Hitachi-GE's NSEDPs [Ref-2]. Derivation of specific requirements that meet those principles involved consideration of applicable current HF standards and good practice guidance by Hitachi-GE's HF team of specialists. These documents are listed in Appendix B.

The HF requirements for the project were captured and listed in the HF RCTM[5] [Ref-12]. This matrix contains all the known "in-feed" fixed design HF requirements. Other more specific requirements that emerged as a result of HF analyses (largely task and error analyses) and safety case-driven requirements were captured and tracked using the HFIR [Ref-13] (see Section 27.3.5). Both registers were kept "live" throughout the GDA stage of UK ABWR design. Hitachi-GE used them to ensure the HF requirements were comprehensively identified and understood. They also ensured the means of meeting the requirements were documented and communicated to the relevant stakeholders.

27.5.2.2 HF Awareness Training for Engineers

HF is a broad topic that cuts across many systems and engineering areas and the basic HF requirements for design are extensive. A key enabler for effectively integrating HF into the UK ABWR GDA design and analysis activities was to ensure that all relevant design and engineering teams (including analysis teams) had a basic level of HF awareness. In addition, within each team a number of individuals were chosen to be "HF-responsible" engineers for the team. These members formed the key contacts for the HF team with the engineering teams and were responsible for ensuring the HF requirements were duly considered. This section summarises the training given to ensure suitable embedding of HF within the engineering teams.

HF Awareness Training was provided for a large sub-set of Hitachi-GE engineers who were working on GDA, drawn from all the relevant design areas. This training comprised a lecture on HF principles and fundamentals, as well as a summary of the UK HF requirements and some potential issues to be considered in the UK ABWR design. The training also included a Q&A session

[5] Although general requirement to meet international and national standards are listed by standard within the RCTM [Ref-12], the individual requirements within the applicable standards are managed separately through the HFE Specification (see Section 27.5.2.3).

following the lecture to help the GDA engineers to understand the UK standard HF practice and key issues particular to each engineer's area. In addition, technical communications among the HF team and other design teams were stimulated through this training. This encouraged the designers/engineers to seek ad hoc HF support for making design decisions and preparing design documentation (see Section 27.5.2.5).

A second awareness training session was given in support of the implementation of the HFE Spec [Ref-9] (see Section 27.5.2.3). This training was provided for the key HF-responsible engineers from each design team involved in the GDA stage of UK ABWR design. These engineers were responsible for ensuring the application of the HFE Spec within their respective design teams during GDA.

27.5.2.3 HFE Specification Development and Implementation

Nuclear power plants in the UK must be designed to meet modern standards and relevant good practice in HF. A key method for ensuring inclusion of and compliance with UK HF-related design requirements has been through the use of the UK ABWR HFE Spec [Ref-9]. The HFE Spec provides a more concise distillation of the HF-related design criteria relevant to UK ABWR that derive from the standards, codes and guidance identified within the RCTM [Ref-12].

The list below shows the topic areas covered within the HFE Spec. The breadth of topics covered ensured that general aspects of the design were covered, along with particular areas of HF focus for nuclear power plants where HF issues tend to arise and HBSCs tend to be made, particularly those related to the design of workspaces (both local to plant and within control rooms) and human system interfaces. Appendix B of this PCSR chapter gives a summary of the main standards and guidance referenced within each topic.

(1) Access and Egress
(2) Work Postures and Positions
(3) Equipment Layout for Operability and Maintenance
(4) Electrical, Control & Instrumentation (EC&I) Equipment Installation
(5) Main Control Room and Supplementary Control Points
(6) Displays and Controls (Non-Control Room)
(7) Alarms
(8) Digital System Design
(9) Materials Handling
(10) Labelling and Signage
(11) Working Environment

The HFE Spec was developed by HF team specialists and distributed to the HF Team and the appropriate design teams based on the scope of plant indicated in the HFIP [Ref-6]. The usage of the HFE Spec within existing engineering processes, specifications and design tools is as described in Section 27.5.2.4. Further detail is provided in the HF DER [Ref-8].

27.5.2.4 HF Engineering Processes for UK ABWR

A HFE process flow to implement HFE design principles and requirements was developed, as illustrated in Figure 27.5-1. In the HFE process on the left side, the HF Team delivered the HFE Spec [Ref-9] to the design teams and registered the related standards in the RCTM [Ref-12].

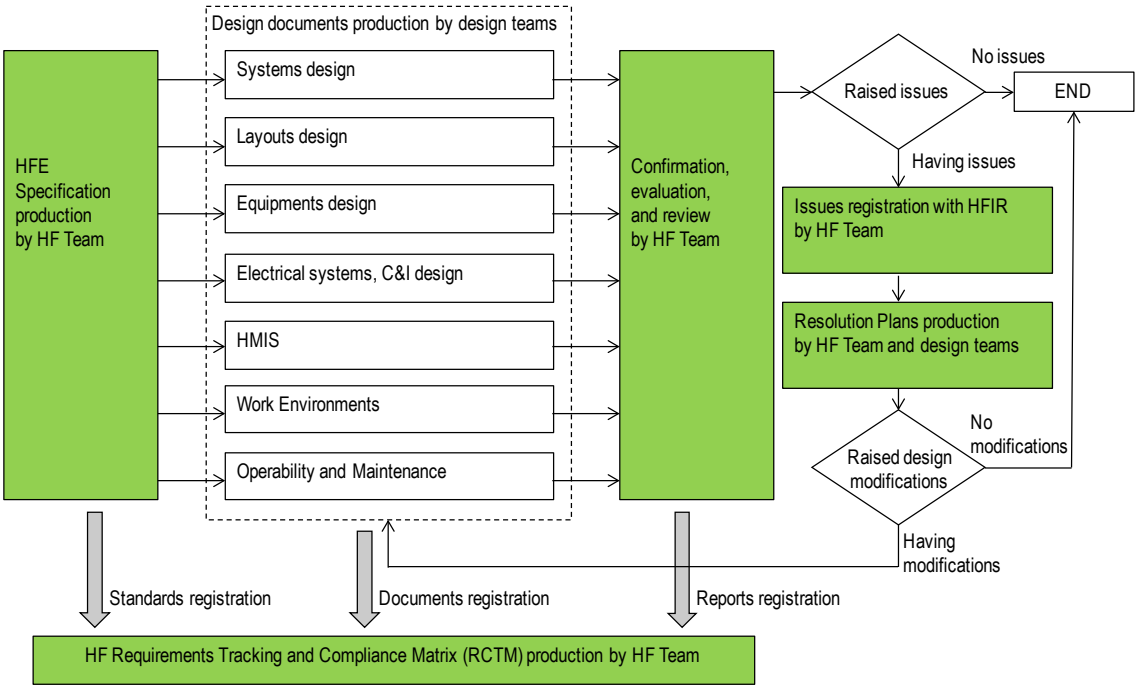


Figure 27.5-1: GDA Design & Engineering Process Flow Diagram

The remainder of this section summarises the HFE Spec gap analysis process which is described in detail in the HFMP [Ref-7].

Following the process shown in Figure 27.5-1, each design team produced its design documents based on incorporating the requirements of the HFE Spec [Ref-9]. These were then registered and evaluated to confirm compliance with the HFE Spec. Compliance with the HFE Spec was then tracked within the RCTM [Ref-12]. This identified any potential gaps in relation to complying with requirements in the HFE Spec (when compared to the ABWR reference design specifications).

The HF specialists then reviewed the potential gaps to confirm these were indeed gaps. This was to ensure misinterpretation or misapplication of the HFE Spec did not get identified as gaps where no actual non-compliance existed. They then conducted further evaluation/reviews of the design outputs to confirm the extent of the non-compliance, or risk resulting from it. The results were reported within HF Technical Query (TQ) forms.

Once issues were confirmed, the HF team entered them in the HFIR [Ref-13]. This meant that non-compliances were captured, tracked and if need be justified, within the HFIR. Then, suitable issue resolutions were recommended by the HF Team. These were discussed with the relevant design team. Where the HF Team and the design team concluded design modifications were needed and feasible,

the design document production process was repeated, implementing the agreed resolution to resolve the issue.

Specific queries about interpretation of requirements, or how best to incorporate them into the design were also captured in the HF TQ form, to which the HF specialists provided a response.

As a result, a total of 52 HF TQs were raised from this design process. The TQ template and management process, including detailed description of design team's process flow for managing non-compliances with the HFE Spec are given in the HFMP [Ref-7]; the TQs themselves are summarised in the HF DER [Ref-8].

27.5.2.5 HF Specialist Design Support

In addition to identification of gaps between the HFE Spec [Ref-9] and reference design specifications, designers actively sought HF specialist support in other areas that were not necessarily driven by the documented HF standards and guidance. The HF team provided "live" ad hoc support to the design teams in ensuring that the SSCs for UK ABWR were designed with consideration of the users in general. In particular, design of new features and facilities within the UK ABWR plant received HF specialist support integral to the design team's activities.

For simple queries, the TQ process described in the HFMP [Ref-7] was used. However in most cases, further detail was required to determine the best design solution to support users, so HF-Design workshops were held to identify preferred design options and to provide advice and support to implementing HF requirements.

The remainder of this section gives a representative, but not exhaustive, list of the ad hoc HF design support given to various design teams in Hitachi-GE. Details of the activities and supporting references are given in the HF DER [Ref-8].

Electrical Engineering

- Support to the design and assessment of lighting and the illumination system, particularly application of task-based factors to lighting requirements for MCR work and high-risk task area emergency lighting.

Control & Instrumentation

- Early in GDA, Hitachi-GE conducted intensive multi-disciplinary discussions about increasing the level of automation across the plant. During these discussions, the HFE team provided advice and support in judging the benefits and disadvantages of employing automation for particular systems, based on AoF analysis (see Section 27.5.3). As the result of these discussions, the eight key functions were selected to become automated.
- Support to the MCR layout optioneering and design by assessing the adequacy of the reference design MCR layout in regard to the movement and visibility of all MCR personnel, maintenance space requirements and frequency, lighting requirements for all activities, etc. and providing recommendations.

- One of the most significant design support activities that the HFE team has undertaken in GDA is support to the modification of existing, and design of new HMIs for UK ABWR. The support during GDA has focussed in general on all new and redesigned HMIs important to safety (including within the MCR, Remote Shutdown System (RSS) and Back-up Building (B/B)). Particular attention was paid to the new diverse Class 1 Safety System Logic and Control (SSLC) HMI on the main control console (MCC), within the MCR. This HF support and assessment is summarised in the HF DER [Ref-8]

Reactor Building Crane and Fuel Handling Operations

- The Hitachi-GE HF team has been involved in design support work related to the fuel route. The work provided recommendations directly to the design team that were incorporated into the UK ABWR design. Where issues and non-compliances were identified, they were recorded in the HFIR. The work has included the following:

Qualitative tabular task analysis and human error analysis (TTA/HEA) in support of fuel handling machine (FHM) automation optioneering during concept development (captured in the HRAR [Ref-11]).

Support to design specification for Reactor Building Crane (RBC) and FHM as compared to the HFE Spec [Ref-9] (through workshops).

Assessment of, and recommendations for AoF for RBC and FHM operations and movement control, especially “zoning” control and interlocks (through workshops, and significant points input to design team reports; see HF DER [Ref-8]).

Detailed task analysis of FHM maintenance tasks to ensure HFE Spec compliance or where non-compliances exist, risk levels are aligned with ALARP principles (as response to TQs; see HF DER [Ref-8]).

Plant Layout

- Continual support to the Plant Layout Engineering team in their staged 3D composite model design process. This involved provision of UK-sized 3D CAD mannequins, review workshops, and high-level task analysis.
- The Plant Layout design team were instructed in a technique for conducting high-level task analysis (TA) to determine the risks and issues (if any) in cases of non-compliance with the HFE Spec [Ref-9]. The design team considered basic task information such as frequency, posture, tools and equipment, laydown areas, etc. and prepared preliminary sentencing of non-compliances for HF review and agreement.
- Support was given to the design and maintenance aspects of planned changes in methodology for removal of safety relief valves (SRVs) and main steam isolation valves (MSIVs).

Conventional and Fire Safety

- Review of fire safety strategy, support to HF issues and considerations for the “defend in place” strategy, evacuation route considerations.

- Support to creation of Construction (Design and Management) (CDM) Red, Amber, Green (RAG) lists to be consistent with HF and support to CDM hazard log identification and review workshop sessions.

Radiation Protection

- The evacuation design guidance (a document outlining design requirements to enable evacuation during radiological emergencies) was reviewed against the HFE Spec [Ref-9] requirements and recommendations were provided to ensure alignment with HF principles.
- Support to evacuation analysis modelling, including suitable consideration of the design aspects (i.e. clear and safe escape routes; consideration of, and accommodating number of people evacuating, etc.) and human capabilities (i.e. walking speed, tolerance to degraded environments, etc.) to support this activity.

External & Internal Hazards

- Support to the Internal Hazards engineers and related system designers regarding claimed human responses during an internal flooding scenario to determine if design change was needed to support the claim; as a result of HF advice of the significant risk (lack of achievability of the task, impact on other HF aspects of the safety case), the claim was withdrawn and no change was necessary.

Civil Engineering & Structural Integrity

- Support to the structural integrity case, particularly ensuring consideration of HFE Spec topics on access and clearance for EMIT to ensure in-service inspection claims for structural integrity could be met.

(See also entries under Plant Layout and Conventional Safety)

Mechanical Engineering

- Support to a comprehensive optioneering study that led to a design change of the RHR Heat Exchangers (Hx). Due to an increase in Hx size without a large increase in the surrounding plant area where they are located, the HF team conducted an HF assessment related to space, access and work environment. This paid particular attention to conducting maintenance and removal/replacement activities. As a result of this assessment, HF specialists reported that there were no significant issues regarding the new design.
- Following a change to automatic initiation of the SLC (see C&I activities above), the strength of the SLC piping was identified as a design issue. The issue would arise if two pumps were initiated simultaneously. The HFE team supported multi-disciplinary discussions. They advised that manually stopping one pump would not meet HF good practice, as this is a critical task step with a small time margin. Following optioneering, Hitachi-GE decided to change the SLC pump start logic to avoid simultaneous initiation of two pumps.

Radioactive Waste (Radwaste) Management Facility

- The Radwaste systems and facility designs are undergoing significant modification to incorporate the new "Chemical Process Philosophy". The HFE team has provided HF requirements to the Radwaste design team such as: establishing a "Concept of Operation for the Radwaste System"; conducting preliminary AoF analysis of Radwaste operations; and checking the compliance with the HFE Spec [Ref-9].
- The HFE team discussed with the mechanical/system design engineers potential human errors in the Off Gas (OG) system Steam Jet Air Ejector (SJAE) operation leading to both SJAEs operating at once. The discussion focussed on potential design changes.
- Support was provided to the Radwaste team regarding claims (including human action) in response to an OG system pipe break. Optioneering was undertaken for automatic versus manual initiation of safety measures (i.e. closure of valves) and interlocks. This included consideration of time constraints, accessibility to the valve and justification of the SSC nuclear category and classification (Cat & Class)[6].

Decommissioning

- Support was provided to the Decommissioning team on a number of topics. These included: application of the HFE Spec requirements when considering decommissioning tasks; and review of the Decommissioning teams Topic Reports to ensure that HF best practice was being considered in the design for Decommissioning.

Spent Fuel Export & Spent Fuel Interim Storage

- Support provided to the concept design of spent fuel handling operations and SSCs including: support to FHM movement and zoning optioneering and ALARP studies; feasibility of installing impact limiters for spent fuel cask drops; Spent Fuel Interim Storage (SFIS) optioneering; and development of the basic specification for the Concrete Cask Storage System process and equipment.

In addition to providing advice and support to the development of the design, the HF specialists supported production of design documentation and topic reports where required. Further detail on areas where design teams received in-depth HF support are described in the HF DER [Ref-8].

27.5.2.6 Support to Design HF Knowledge Transfer to Future Licensee

One important aspect of GDA activity is ensuring any future licensee is fully aware of the basis for the design and safety case. To achieve effective knowledge transfer to the future licensee of how HF considerations were addressed within the design during GDA, the Hitachi-GE HF team developed material for informal and formal communications of the GDA HFE design activities to the future licensee (including their Operations team). In particular, workshops were held with suitable ex-operations representatives, and feedback sought with regards the intended operational concept to ensure that plant design would support tasks as expected by the ultimate "end user" organisation.

[6] SSC Cat & Class are described in detail in Chapter 5: General Design Aspects, Section 5.6.

Formal records of all GDA activities and documents are managed at project level through a suitably formal process. However, early engagement and discussion with suitably representative UK end users and stakeholders was critical to ensure that the generic design would assure operability and maintainability throughout the plant. This facilitates the effective "ownership" and further development of the HFI programme and HF design requirements by the future licensee during the site-specific stage of the PCSR.

27.5.2.7 General HF Design Verification

This was conducted as part of the overall verification programme providing evidence and substantiation of the HBSCs (see Section 27.5.4).

27.5.2.8 Impact of HF Design Support Activities on UK ABWR Design

The HF design activities as summarised above and in the HF DER [Ref-8] were implemented as required by the HFIP [Ref-6] and HFMP [Ref-7]. The HF key activities undertaken were associated with: HF requirements capture; HF awareness training for engineers; the development and implementation of the HFE Specification; and the implementation of HFE Processes for managing HF issues. These activities demonstrate that a systematic approach was taken to the management and integration of HF activities within the design workstream.

The use of the HFE specification, the Concept of Operations and the HFE processes ensured that HF was addressed within the design generally and specifically in relation to workspaces and Human System Interfaces. This was supplemented by the HF Specialist Design Support to the twelve engineering disciplines/design areas. These activities provide evidence for the HF SPCs relevant to GDA having been met (see Appendix B and HBSC report [Ref-1]). The activities have also ensured HF knowledge transfer to the future licensee. Where HF issues have been identified, these have been addressed in accordance with the HFE processes. This has included optioneering and design modifications as required.

The HF DER [Ref-8], as summarised in the above sections, provides the details of how the design-support HF activities for GDA contributed to both design improvements and ALARP decisions on system design changes. The design improvements related to HF requirements are suitably comprehensive, and incorporated by systems engineers in every area throughout the plant. In addition, specific issues raised through UK ABWR systems design and analysis activities were resolved with due consideration of HF. These improvements provide demonstration of the effectiveness of the planned set of HF design activities. The design improvements ensure that the three key HF risks (see Section 27.8.1) have been managed to ALARP within GDA.

27.5.3 HF Analyses

Key activities that support the implementation of HF requirements in design and substantiation of the functional HBSCs are the HF analyses that were carried out as part of the HFI programme. These analyses have included: AoF between humans and engineered systems; task analysis; Human Reliability Analysis (HRA); and analysis that informs staffing levels. The various analysis activities were completed in an integrated manner with input from the relevant design and safety analysis

teams. Where issues and recommendations arose these were captured and managed through the HFIR (see Section 27.3.5).

The integration of the HF analyses with the broader design and safety analyses meant that the HF analyses were performed in an iterative, progressive and often responsive way to the rest of the project activities. The analysis activities and results have been summarised within a single document, the HFAR [Ref-10]. This demonstrate the comprehensiveness of the HF support provided via the analysis workstream in the HFIP [Ref-6]. The analyses workstream reported in the HFAR complement the support provided to implementing general HF design requirements described in Section 27.5.2. The HFAR is also one of the key Level 2 Topic Reports that underpins this PCSR chapter (see Appendix C Document Map).

This section provides a summary of the HF analysis activities that are reported in greater detail within the HFAR and its supporting references.

27.5.3.1 Allocation of Function Analysis

As discussed in Section 27.4.2 describing the baseline HF assessment, AoF is a key element of consideration of HF in design. It sets the overall level of automation of the plant, defining the role and tasks of the humans within the systems.

The AoF was undertaken in accordance with the HFIP [Ref-6] and the method defined in the HFMP [Ref-7]. The methodology for this AoF was based on the method presented in NUREG/CR-3331 [Ref-23], and the criteria were selected in line with current HF good practice, particularly related to effective and safe post-fault operations.

Of particular importance to the safety case and the achievement of the functional HBSCs is the consideration of capabilities and limits of the operations and maintenance personnel. This is especially relevant where these relate to fault and accident conditions. For this reason, the analysis focussed on functions related to safety. The criteria chosen for the analysis focussed on the consequences and risks associated with an incorrect allocation in these conditions.

The AoF was the product of a multi-disciplinary approach that took account of the concept of operations and the description of the user group's capabilities [Ref-21]. In particular consideration was given to: personnel capability; crew complement; basic assumed competence; expected roles and responsibilities; plus operating experience feedback from the fleet of J-ABWR. The AoF was also informed by more detailed task and error analysis undertaken for the HRAR [Ref-11] and the Hazards HRA Addendum [Ref-24]. These analyses ensured that the AoF was informed by a risk based consideration of the HBSC identified in the PSA. This included reviews of operator actions required in potentially hazardous/hostile environments, the required level of reliability, the timescales and the impact of other Performance Influencing Factors (PIFs). The AoF has also been informed by the results of the Task Performance Analysis for Non-PSA HBSC [Ref-25] (see Section 27.5.3.3) and Cognitive Workload Analysis [Ref-26] (see Section 27.5.3.4).

The results from the AoF analysis are presented in the AoF Report (AOFR) [Ref-27]. The key results are summarised here. The total number of functions selected for the AoF evaluation was 264. 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, 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. Table 3-2 within the AOFR [Ref-27] shows the fifteen new or changed functions that were identified by the hypothetical allocation for UK ABWR. Where it is noted that J-ABWR has the same design (in the "New Design?" column), this signifies that a change in the function allocation has been recommended 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 system technology. The human 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.

The more detailed HF analyses for GDA (HRAR, workload analysis, etc.) and assumptions for operations (i.e. procedure structures, command and control concept, etc.) provide assurance that situation awareness is maintained despite this level of automation during fault conditions. Much later in fault sequences (i.e. after excessive damage to the plant, including core damage, and/or with multiple failures of automated safety systems), greater flexibility is needed in implementing system responses. This arises due to the highly-variable state of plant degradation and availability. Therefore, in these scenarios greater allocation is given to the human operator, in line with the expected roles and responsibilities of the Emergency Controller and MCR personnel at that time.

In summary, the AOFR [Ref-27] provides substantiation of the AoF for the UK ABWR at GDA. Where changes to the AoF were recommended, these were recorded and tracked through the HFIR [Ref-13]. Resolution of the issues was discussed with the relevant system engineer. Where the recommended automation of any function was deemed not feasible, a suitable alternative resolution was found and any residual risk or ALARP justification provided in the HFIR record, in line with the issues managements process outlined in the HFIP [Ref-6]. Activity to further support design assurance and ensure the implementation of any recommended changes in allocation are reported in the HF DER [Ref-8].

27.5.3.2 Identification of HBSCs Throughout the Safety Case

Key to the UK ABWR safety case is the systematic and thorough identification and understanding of all human actions that are important to achieving safety and resilience in response to abnormal events. These are known as the functional HBSCs (see Section 27.6.3). The design of the system is

inextricably linked to, and invariably a key factor in the achievement of the required reliability for the successful performance of these claimed human actions. That system design is underpinned by further HBSCs, the HF property claims (see Section 27.6.3).

In order to identify the UK ABWR HBSCs, the HF team conducted a variety of HBSC and "human error" identification activities. These looked for potential actions important to safety for tasks performed throughout the plant, in all operating modes. A review of outputs from other topic areas within the UK ABWR was also used to identify specific claims.

The methods chosen for the purposes of identifying all the HBSCs for UK ABWR depended on the availability of information (e.g. maturity of design), other design and safety case activities taking place, objectives, and timescale of each method.

The functional HBSCs are not all equally important to safety and the reduction of risk in the plant. A proportionate approach was taken based on the associated risk. This shaped the focus of the HBSC identification work, the level of substantiation, and amount of detail provided in each record (which varies based on the level of HF importance). In order to define "proportionate effort" for HBSC substantiation work, and to provide a similar means of determining the importance of HBSCs to the risk levels of the plant, a HBSC ranking system was implemented.

These methods and the work to capture HBSCs are described in detail in the HFMP [Ref-7] and the HBSC Report [Ref-1]. More detail on the structure and nature of the HBSCs identified within GDA, the ranking of them and summary of their substantiation is given in Section 27.6.

27.5.3.3 Task and Human Reliability Analyses

As described within the HFMP [Ref-7], as part of the HF activities within the HFI programme, the HF team and HF-responsible members of other design and engineering teams have used various types of tabular task analysis (TTA) for the following purposes:

(1) To support new or modified plant layout and equipment design for UK, particularly to advise on HMI designs (in MCR, local control HMIs such as the RBC, plant equipment control and indicators, etc.) for optimum usability/maintainability and to reduce error traps.

To underpin further HF-led design analysis such as workload assessment, identification of communications and team design needs, working environment assessment, and V&V activities.

As the core of the HEA and HRA[7] techniques. TTA has been used for both error identification and for detailed qualitative error analysis in support of the various deterministic safety analyses (DSAs) (i.e. design-basis analysis, beyond-design basis analysis, severe accident analysis), as well as the basis for quantification of human error probabilities (HEPs) using HRA in support of the PSA.

[7] It is recognised that many guidance documents consider HRA to mean all aspects of human error analysis, both qualitative and quantitative. However, often HRA has a specific limited meaning, particularly in the context of PSA and when used by safety analysis specialists. For the purposes of clarity and consistency with Hitachi-GE current practice, within the HFMP [Ref-7], HRA is used to mean the solely the error quantification portion of the analysis; HEA is used to mean all the other elements qualitative human error analysis that make up a HRA, except for quantification.

The use of TTA and HEA in support of design activities is described in Section 27.5.2, and in more detail within the HF DER [Ref-8]. However, within the HFI programme of analysis activities, the most important purpose of the TTA/HEA and HRA is the third point above, which provides key evidence to substantiate the functional HBSCs as achievable.

During GDA, TTA and qualitative HEA was conducted on all the functional HBSCs. The level of detail of the analysis was proportionate, in accordance with the HBSC importance (see Section 27.5.3.2). These analysis activities were integrated with the evolving safety analyses in order to provide HF input in a timely manner.

For human failure events identified within the PSA model, in addition to developing more detailed TTAs, quantification of human reliability was performed using appropriate HRA techniques. A key purpose of the HRA was to provide probabilistic data (i.e. HEPs) to the PSA. However, from the perspective of HF and substantiation of HBSCs, an even more important output of the HEA and HRA was:

- Assurance that tasks are achievable or determination that they are not. This allows the HF team to challenge unachievable HBSCs and have them removed from the safety case (e.g. by introduction of engineered safety measures).
- Identification of key aspects of the design (i.e. HMI elements, functionality of SSCs, location of SSCs, etc.) that needed further assessment and/or improvement to ensure they support expected human task performance.
- Identification of recommendations for future operational arrangements (e.g. supervisory checks, additional personnel, highlighting of critical task steps in future procedures, etc.) to ensure that risks of human error in these tasks are reduced to ALARP post GDA.

The TTA template used in GDA facilitated identification of the design features on which the tasks depend. The design features were reviewed to determine whether they were adequate to support the tasks. The TTA sheets include a column for identifying specific operational arrangements, HF issues and capturing recommendations (to resolve the issue or to improve performance even when no issue exists). They also include a place for assigning those entries a HFIR number. This allows transfer of the issues and/or recommendations to the HFIR for effective tracking to resolution (see Section 27.3.5), or passing them to the future licensee.

The HRA was conducted in an iterative manner to match the PSA development. The scope was progressive and the final HRA covered all types of potential human failure events relating to:

- Pre-initiator errors (e.g. latent EMIT errors such as miscalibrating a transmitter).
- Errors that cause initiating events (e.g. failing to connect a lifting attachment to the RBC correctly causing a dropped load when lifting).
- Failure to perform required post-fault actions (e.g. failure to provide manual back up to loss of the duty Fuel Pond Cooling (FPC) pump in station black-out conditions).

For PSA-related HBSCs the results of the TTA/HEA and HRA activities are summarised in the HFAR [Ref-10] and detailed in the HRAR [Ref-11] and Hazards HRA Addendum [Ref-24]. For all

other HBSC the results of the TTA/HEA are captured in the Task Performance Analysis for Non-PSA HBSCs Report [Ref-25].

Evaluation of Errors of Commission

A study was conducted to analyse potentially significant Errors of Commission (EOCs). This was in order to demonstrate that should an EOC occur (e.g. due to an error of cognition or a simple execution slip), the design has robust mechanisms in place to prevent or recover from the situation. It was also used to identify opportunities to improve the design to minimise such errors. A multi-faceted approach to the analysis was used. This applied various methods as defined in the HFMP. These included the use of inputs from PSA, formal operating experience (OPEX) records, and workshops with subject-matter experts (SMEs). These investigated both the potential for EOCs and potential improvements for the UK ABWR design.

Results showed that where potential EOCs were identified, design-focused measures were already in place that would prevent them (i.e. through interlocks), or mitigate their effects (i.e. by warning of the EOC through an alarm). In a small number of instances where there are no dedicated alarms, the EOC will still be clearly indicated to operators by associated alarms and indications. In addition, in certain instances while an early operator response would be preferable, an engineered safety system is present should error recognition and manual recovery fail.

Despite the sufficient level of existing design measures in place, the analysts identified opportunities for design improvements. This was done with the assistance of appropriate system design engineers and maintenance and operations SMEs. Furthermore, this activity also captured potential operational and administrative measures that could assist in minimising the occurrence and impact of EOCs during operation of the UK ABWR. These recommendations have been extracted and fed into the HFIR and/or the assumptions tracking process (as appropriate) to be managed within GDA or passed to future licensees as necessary.

The conclusions from the EOC analysis reflect the fact that UK ABWR is a modern power plant design which features design interlocks and high levels of automation. It is also assumed to be operated using well-written procedures that support optimum task performance. This effectively eliminates error potential where possible and where it cannot be eliminated managing the risks to ensure that they are ALARP.

The method and results of the EOC analysis are summarised in the HFAR [Ref-10] and presented in greater detail in the EOC Analysis Report [Ref-28].

HCI-Induced Cognitive Error Analysis

Although the HRA included a certain level of consideration of cognitive error, specific concerns were identified regarding the potential for the "modern" digital Human-Computer Interface (HCI) to induce an additional cognitive burden. This potentially results from the cognitive effort required to interpret or navigate the on-screen digital system. It therefore introduces cognitive errors specifically related to use of the HCI. In response a separate HCI-Induced Cognitive Error Analysis was undertaken in order to provide assurance that the computerised HMIs in the MCR do not themselves

significantly increase cognitive burden and impact on the HEPs derived in the HRA. The method and results are summarised in the HFAR [Ref-10] and presented in greater detail in the HCI-Induced Cognitive Error Analysis Report [Ref-29].

A multi-faceted approach using a variety of accepted methods was taken to the analysis, as described in the HFMP [Ref-7]. The analysis identified the potential Internal Error Mechanisms (IEMs) and the PIFs likely to affect performance and cognitive error within the MCR. The IEMs were fairly consistent across the tasks chosen. They gave insight at the 'generic design feature' level as to what elements were likely to be important for optimising task performance. The output of the analysis was then used to inform the design, with recommendations tracked in the HFIR [Ref-13].

27.5.3.4 Staffing and Workload Analysis

A workload analysis was undertaken in order to provide assurance that assumptions on staff complement made in the COR [Ref-21] were generally acceptable and the tasks important to safety generally achievable with that assumed complement. A risk based approach was taken that focussed on MCR operations. This included related EMIT tasks performed from within the MCR. The analysis considered cognitive burdens from both distraction and workload. The details of the method and results are described in the HFAR [Ref-10] and its supporting references, the HFMP [Ref-7] and the Cognitive Workload Analysis Report [Ref-26].

The HFMP [Ref-7] required use of the Pro-Subjective Work Load Assessment Technique (Pro-SWAT). This method provides a simple means of rating cognitive workload along three dimensions: Time, Mental Effort and Psychological Stress. No available method was identified as "good practice" for assessing distraction, so a series of questions were developed to help explore distraction within the MCR. Japanese and UK nuclear power plant operators rated a series of tasks during a two-day workshop using the Pro-SWAT rating scale. Justification was provided for the workload rating and these ratings were reviewed during and after the workshops.

The overall findings from the analysis provided the Hitachi-GE HF team with useful insights about the impact of distraction and workload, and although this work was carried out independently of the HRA work, the findings align with the findings from that analysis [Ref-11]. Two types of distraction were explored by the analysis; general distractions and specific distractions. The general distractions were further subdivided into Generic Deviant Distractions and Non-operational Distractions. The specific distractions related to secondary testing tasks, such as online testing and plant functional testing. Issues with distraction were noted to be particularly problematic when several distractors occurred simultaneously. In relation to cognitive workload, one scenario was rated as having a low level of cognitive workload. For three of the scenarios, there were distinct transitions into periods of high workload and into periods were there was a medium level of workload. For one scenario the workload was predominantly at a medium level, with three brief high workload spikes associated with specific subtasks. Interventions identified to address high workload were largely in the form of organisational controls. In response to this, an important recommendation was made to ensure the design of the control room, equipment and HMIs did not preclude later organisational interventions that might be required to reduce potential distractions and high workload.

In addition to the workload analysis, timeline analysis was applied to human failure events identified as important in the PSA (as described in the HRAR [Ref-11]). It was applied 'pessimistically' as a first pass, that is, it was assumed that any recovery steps would require a full repetition of the actions taken prior to the final 'confirm success' step in the sequence. Where a clear time margin remained after this assumed recovery, the time available was deemed to be adequate. Where the time margin was short – time remaining approached zero – the timings were examined closely to identify opportunities for reducing the time taken step by step or to reduce pessimisms in the estimate of time available to complete a task. A total of twenty human failure events were examined, the majority of which were found to have adequate time margins. Where time margins were questionable, these led to design recommendations and HF issues being raised.

27.5.3.5 Impact of HF Analysis on UK ABWR Safety Case and Design

The HFAR [Ref-10] has summarised the HF analyses that have been undertaken during GDA for the UK ABWR. This key Level 2 document shows how those analysis activities have been undertaken using a systematic and comprehensive approach, and that these activities were conducted in line with international good practice guidance and methods. Undertaking these analyses has addressed the HF SPCs relevant to GDA (see Appendix B and the HBSC report [Ref-1]).

In relation to AoF, the analysis provided substantiation of the adequacy of the AoF for the UK ABWR at GDA. Where changes to the AoF were recommended, these were recorded and tracked through the HFIR [Ref-12]. Most were implemented within GDA and can be shown to improve the achievability of the claims made on human action within the case.

HF issues and design modifications were identified from the HRA, non-PSA HBSC task performance analysis, qualitative human error analyses (e.g. EOC study), and the preliminary workload analysis. These issues and design changes have been resolved through the HF issues management process. The HF analysis activities have demonstrably contributed to reducing the key HF risks (see Section 27.8.1) to ALARP. This was particularly true for the risks related to human errors during operations and EMIT that contribute to the initiation of faults or lead to the failure of the required safety measure. The HF analysis activities, were integrated with the safety analyses. This enabled the HF analyses to inform and modify those safety analyses in addition to the relevant design. This was particularly the case with the GDA PSA and fault assessment. HF issues within the safety analyses were identified in the HRAR [Ref-11] and the HBSC Report [Ref-1]. Where appropriate and agreed, changes to the safety analyses were made to better reflect HF good practice and take account of user capabilities and limitations. This ensured that the UK ABWR safety analysis and ultimately the overall PCSR is based on sound, justifiable expectations of the expected future plant user group.

27.5.4 HF Verification and Validation

An important set of activities that forms part of the demonstration that HF has been adequately considered during design development (i.e. effective implementation of the HFI programme and substantiation that the HF property claims are met), and that functional HBSCs are achievable as analysed is V&V. This section gives a summary of the HF V&V programme, as described in the HFVP [Ref-14] and the results.

27.5.4.1 V&V Programme Overview

The V&V activities for HF in GDA form a set of independent and diverse checks. They provide proportionate, appropriately designed tests and trials intended to demonstrate that the design conforms to HF design principles. They consider the key tasks and whether they can be performed safely, to meet UK ABWR operational safety goals.

The HFVP [Ref-14] defines the scope and activities of HF V&V undertaken during the GDA stage. The HFVP outlines the basic strategy and general process of GDA HF V&V and provides a high-level indication of the nature and timing of activities to be undertaken, with a suitable level of justification for each activity as required.

A proportionate approach has been taken when selecting the V&V activities. These activities used a representative sample of plant conditions, tasks, and situational factors affecting human task performance (and the associated HMIs). The HFVP outlines the decision-making process that underpinned this proportionate approach. This includes focussing on risk-important and new plant design features or functions.

The output from the V&V provides the assurance that HF generic requirements and plant-specific task-based requirements have been satisfied by the design. The V&V activities also provide an initial demonstration that the functional HBSCs are achievable. The level of fidelity available for the V&V tests was suitable for the design maturity at GDA stage.

In summary, the breadth of V&V activities covered the entire plant and matched the scope of the HFI programme. For those areas identified as having key risk significance, particularly to nuclear safety, or as being novel, or potentially complex, the related HF V&V activities were conducted as “deep dives” to provide a more thorough and robust demonstration. Figure 27.5-2 illustrates this breadth and depth of the V&V scope as applied to the three key areas of Control Room, Plant Layout and Plant Equipment design. The overall process flow for V&V is as shown in Figure 27.5-3.

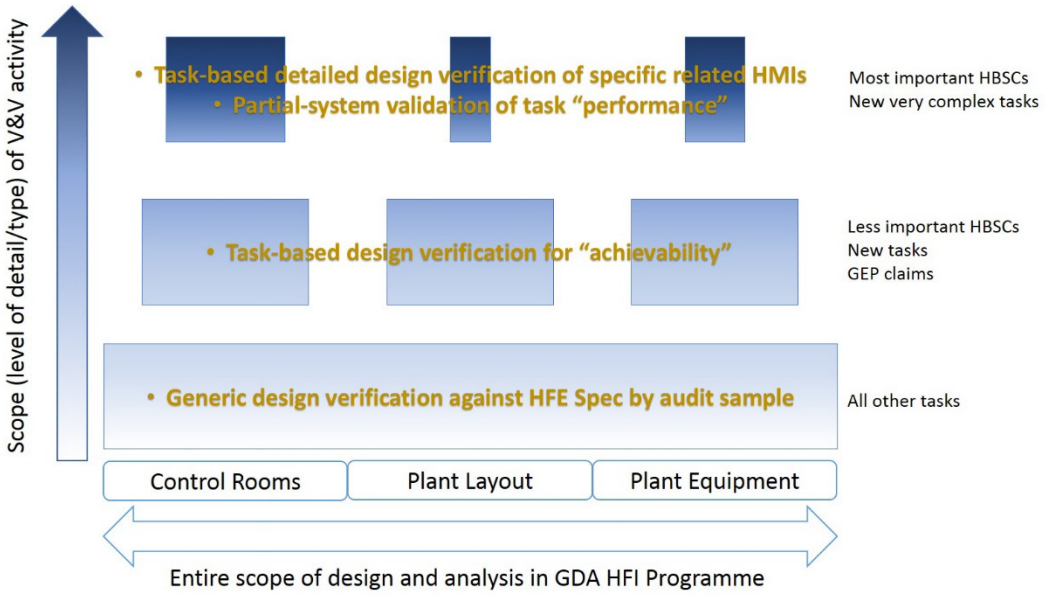


Figure 27.5-2: Scope of V&V (breadth and depth) across V&V areas

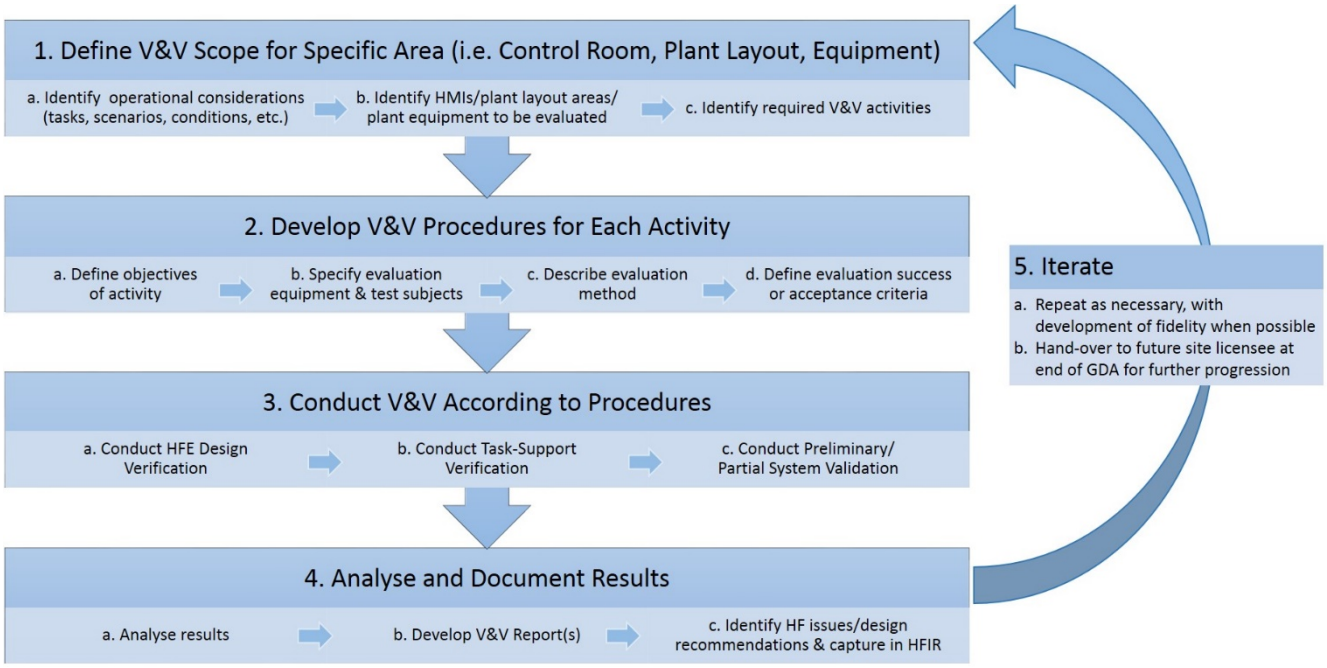


Figure 27.5-3: GDA HF V&V process

27.5.4.2 V&V Results

The HFVP [Ref-14] and HFVR [Ref-15] provide details on the rationale and methodology for the V&V activities covering the three areas: Control Room, Plant Layout and Equipment Design.

For the Control Room aspects, experienced NPP operators (Japanese and UK) conducted a series of 'trials' in which they performed proceduralised tasks in a static mock-up of the MCR. The mock-up

was constructed to accurately 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.

The Plant Layout and Equipment V&V was begun early in GDA with the development and application of the HFE Spec [Ref-9], and the development of the RCTM [Ref-12] to capture and track of the compliance with requirements and good practices for design (see Section 27.5.2). and. The Technical Queries process and the ability to raise HF issues, and register them for resolution also formed part of the V&V for Plant Layout and Equipment. A summary of the HF V&V results is described in the remainder of this section.

MCR V&V

The breadth and depth of the V&V trials for MCR operations are described below.

Trials by J-ABWR Experienced Operators:

- MCC modified configuration options testing:

  Although not actually "V&V", this optioneering test was conducted using the V&V facility and equipment. It allowed the design team to choose between two possible design options based on operator feedback. The tested MCC layouts were chosen by a multi-disciplinary team, including HF specialists, as the two preferred options out of five potential re-configurations; the re-design is necessary in order to accommodate the new Safety Auxiliary Control System (SACS) portion within the HMI arrangement on MCC, introduced for UK ABWR. The same configuration as the J-ABWR layout of controls and displays on the same "horseshoe" arrangement, with an additional "wing" containing the SACS panel, was selected as the preferred layout. The selection was based on interviews and surveys of the test participants who tested both arrangements using a series of simulated tasks, and on statistical analysis of operator rating scale scores. The selected layout was used for the V&V trials and put forward as the official design option for GDA.

- Early verification on the main MCR HMIs (WDP, MCC):

  The purpose of these trials was to test the main HMI (WDP, MCC) and communication/coordination between Control Room Operators (CROs) and the MCR Supervisor (MCRS) by the task performance-based testing. A set of simulated activities was carried out: start-up, shutdown, surveillance tests and post-fault operations. At the end of each activity, the operators were interviewed to gain feedback, using a standard set of questions and then followed by open discussion. This indicated that the increased width of the MCC/SACS did not present any hindrance to movement or communication.

- Early verification on the backup MCR HMIs (SAuxP and HWBPs):

  These trial were run to test the functionality and operability of the backup HMI. They were conducted in two parts: a design 'talk-through' in which SQEP HF and C&I specialists critically reviewed and commented on backup panel design, taking into consideration key or complex tasks; and a 'walkthrough' using scenarios to test these HMI. The talk-through and walkthrough findings were collated and will feed into the design post-GDA.

Following the above trials, the mock-up was modified to reflect the results. Then, to test the usability of the backup HMI and communication/coordination between CROs and MCRS task performance-based testing was conducted. A set of simulated activities were carried out that involved post-fault operations where operators were required to move to the backup HMI. At the end of each activity, the operators were interviewed to gain feedback, using a standard set of questions and then followed by open discussion. This indicated that the backup HMI design did not present any significant hindrance to information, operators' movement or communication.

- Early validation by testing the UK ABWR HBSCs:

  To validate preliminarily the MCR layout and HMI by performance-based testing on the twenty HBSC-related tasks ranked as 'Category A' (see Section 27.6) that required use of the main HMIs and the twelve 'Category B' HBSCs where task steps required the use of all MCR HMIs (including the backup HMIs). At the end of each activity, the operators were interviewed to gain feedback, using a standard set of questions and then followed by open discussion. This indicated that there were not any fundamental issues to achieving the HBSCs in terms of the MCR layout and the design of the HMIs.

Trials Using UK-Experienced Operators:

- Early feedback based on UK ex-operator practice:

  This trial was to allow UK-experienced operators to carry out a number of tasks according to typical UK conduct of operations and to determine from this if any changes to the design might be required. The UK MCR crew successfully performed the three selected post-fault operations. At the end of each activity, the operators were interviewed to gain feedback, using a standard set of questions and then followed by open discussion. This indicated that there were not any fundamental issues with the MCR layout and HMI designs from the viewpoint of a set of representative UK operators.

In summary of all the V&V trials, the Japanese and UK operator representatives found no difficulties in carrying out the trial tasks. They considered the layout of the MCR and the HMI as simulated in the mock-up to be fit for purpose. In their roles as CROs and MCRS, the operators experienced no problems in communicating with each other throughout the scenarios. They were able to move around the facility easily and unhindered to access each panel. The crew provided some feedback considering changes to be 'desirable' rather than essential. These are captured in the HFVR: some have also been registered as formal HF issues and all will be passed to the licensee for attention and resolution [Ref-13].

Plant Layout and Equipment

The V&V of plant layout and equipment design has been achieved, to the extent possible within GDA, primarily by the application of the HFE Spec by HF SQEP and design teams. HF specialists, have participated in numerous design optioneering studies and reviews concerned with, for example, the FHM and RBC, EP equipment, RVI and backup building HMI and supported the design process extensively, as described in Section 27.5.2.

27.6 Structure and Substantiation of HBSCs

27.6.1 Introduction

This section provides a summary of the process for identification and substantiation of all the HBSCs within the UK ABWR Generic PCSR. It presents the structure of the claims and the relationship of the HBSCs to the SFCs and SPCs in the other chapter BSCs. In this way, it demonstrates how they support the achievement of the HLSFs and FSFs as well as the NSEDPs [Ref-2] (compliance with the NSEDPs is discussed in PCSR Chapter 5: General Design Aspects).

The HBSCs (both functional and property claims) are listed within the Appendices of this chapter. However, the CAE themselves are presented in detail in the HBSC Report [Ref-1] rather than at the PCSR chapter level. The HBSC report is the HF topic area equivalent to the BSCs that are the key Level 2 documents in the system topic areas This allows consistent treatment of the CAE related to this chapter as that in the systems chapters.

27.6.2 Identifying HBSCs Throughout the Safety Case

Within the safety case, HBSCs have been defined as "an action or set of actions that, if not performed to the required end result with the required reliability, would leave the plant vulnerable to unacceptable increased levels of nuclear or environmental safety risk". To identify HBSCs the HF Team has conducted a variety of claim and "human error" identification activities, looking for potential actions important to safety. These encompass tasks performed throughout the plant in all operating modes. They have included review of outputs from other topic areas within the UK ABWR GDA safety case that have also identified specific claims.

27.6.3 Structure and Relationship of HBSCs

The claims presented in Section 27.6.7 and detailed in the HBSC Report [Ref-1] are organised, grouped and ranked into a structure that supports and aligns with the general use of claims within the safety case while also facilitating proportionate analysis and substantiation of them.

The UK ABWR GDA HFI programme was focused on ensuring that human actions within the plant support and enhance the FSFs. As noted within PCSR Chapter 5: General Design Aspects there are five FSFs for UK ABWR as listed below:

FSF1 – Control of reactivity

FSF2 – Fuel cooling

FSF3 – Long term heat removal

FSF4 – Confinement/Containment of radioactive materials

FSF5 – Others

These FSFs are decomposed further into a set of HLSFs. The HLSFs are the more specific means to ensure that individual systems are designed such that they contribute to the achievement of the overarching FSFs.

Within the overall safety case, at the SSC level, two types of claims support achievement of the nuclear safety functions. These are SFCs and SPCs. In brief, SFCs are actions performed by an SSC to directly implement the safety function, for example insert control rods. SPCs are those claims that provide the safety justification that the UK ABWR design is compliant with Hitachi-GE's NSEDPs [Ref-2] and cover matters such as the integrity, reliability and environmental qualification for the claimed SSC in the corresponding topic areas.

HBSCs are identified and categorised separately from SFCs and SPCs. The separate presentation of HBSCs allows more effective understanding and demonstration of the reliance on the human element of the UK ABWR "system" for maintaining or returning the plant to a safe state. It makes for much greater visibility of the HF-related aspects of the safety case which then allows for more effective implementation of the required organisational and operational arrangements by the future licensee to support the HBSCs.

Although presented as a single group, separately from SFCs and SPCs, it is clear that the HBSCs comprise both specific human actions that are "functional" claims and more generic HF design and organisational "property" claims. To map onto the related systems chapters more easily and to allow greater integration of the HF topic area into topic areas to which SFCs and SPCs do apply, the HF Team organised the HBSCs into the same two generic types of claims: functional HBSCs and HF property claims.

Figure 27.6-1 shows the relationship of these two types of HBSCs with the overall safety case claims structure; further explanation of each type is provided in Section 27.6.7.

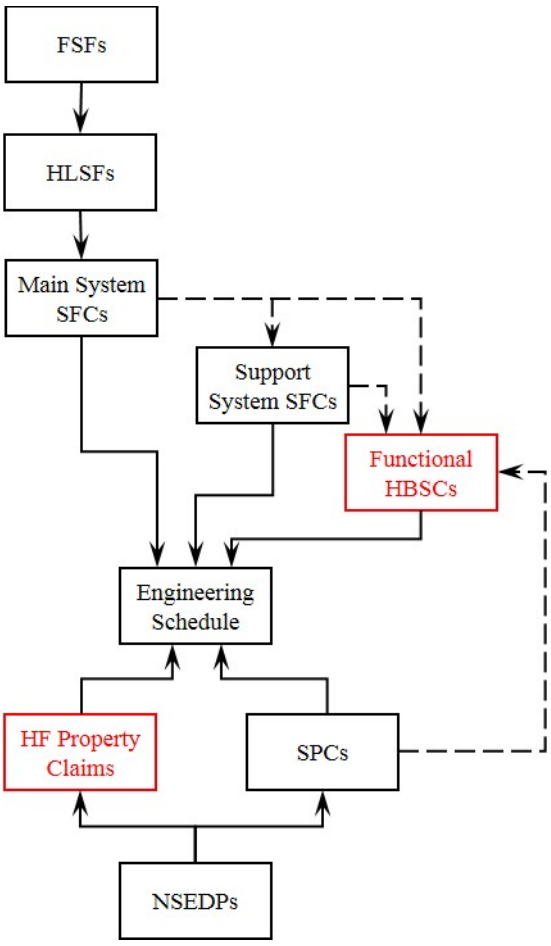


Figure 27.6-1: UK ABWR safety claim structure

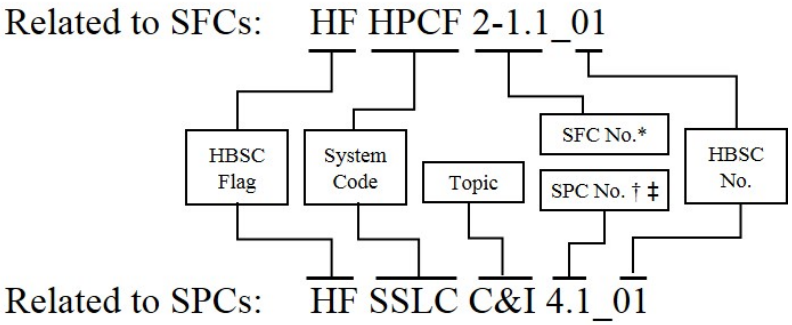
27.6.4 HBSC Identification Coding

For traceability and accountability each HBSC is provided with a unique identifier. The purpose of the identification code is to:

- Clearly identify the claim as related to the HF topic area as being "human-based".
- Clearly identify the HBSC as either a HF property claim or a functional HBSC.
- Integrate HF claims into the overall claim structures for the safety case and show clear traceability between each functional HBSC and its related SFC or SPC and, through this, back to the HLSF and FSF or NSEDP (in the case of SPCs) that the claim supports.

Rules have been developed for these unique identifiers as shown in Table 27.6-1 below. Because the HF property claims are not linked directly to SFCs or SPCs, but are themselves basic system (or future organisation) property claims, they are all given identifiers starting with "HFSPC", to indicate they are a "HF Safety Property Claim", followed by a sequential number. Further details of the application of the coding system and its nuances is provided within the HBSC Report [Ref-1].

Table 27.6-1: Identification coding scheme for HBSCs

Functional HBSCs

HF Property Claims
HFSPC (claim number) e.g. HFSPC 1, HFSPC 9, etc.

27.6.5 Grouping of HBSC

Wherever possible, the HBSCs have been grouped for substantiation purposes. The grouping of HBSC was done where multiple similar functional HBSCs are grouped together. This is based on different criteria dependent on the source of the claim. Grouping similar claims allows for more efficient analysis, giving a structured and concise approach to presenting the necessary arguments and evidence for similar HBSCs one time rather than them being repeated. It also allows for the "worst case" claims to be substantiated as the bounding claim, with all other less onerous claims in the group then considered bounded by that substantiation. Any claims that cannot be grouped have been recorded as individual HBSCs.

The following gives a brief explanation of the grouping criteria used:

- Claims identified from the PSA are grouped based on similarity in the claimed actions and TTAs. Relative risk importance of the grouped HBSCs is considered when defining the bounding scenario. The grouping and bounding process is described in greater detail within the HRAR [Ref-11].
- Claims identified from the DSA have been grouped based on the function and location of the human action. This is because the location of the action is often driven by the initiating event, with similar actions being claimed in the same location. In addition, this approach achieves an appropriate level of granularity in assessing the actions to be able to provide input to the design of HMIs, alarms, procedures, training, etc., during GDA and beyond.
- Claims identified from other sources (e.g. BSCs, TRs, etc.,) have been grouped based on similarity of function and task. For example, EMIT tasks for civil structures are broadly similar if not identical and as such it is appropriate to group them into a single functional HBSC related to the EMIT of civil structures.

27.6.6 Analysis and Substantiation of HBSC

For the claims on human action and HF properties to be considered valid within the UK ABWR safety case, each HBSC has been substantiated. The substantiation process captured the arguments and evidence that each claimed action is achievable. The following section summarises the substantiation process for the identified HBSCs and then, ultimately, how the claims and their substantiation are recorded and managed. A more detailed description of the techniques used, as well as the results is given in the HBSC Report [Ref-1].

27.6.6.1 Ranking of HBSCs

HBSCs are not all equally important to safety and the reduction of risk in the plant. The HBSC analysis and substantiation within GDA has therefore been undertaken in a manner proportionate to the assessed risk and importance of the claim. To define "proportionate effort" in HBSC substantiation work, and to provide a similar means of determining the importance of HBSCs to the risk levels of the plant, a HBSC ranking system has been implemented.

The ranking of HBSCs is done using a 3-part code based on the impact of the human action (as opposed to the related SSC) to plant risk levels and the HF complexity of it. Together these features represent the overall HF-related risk level attributed the claim.

Although the rules of SSC Cat & Class ranking (as per Chapter 5: General Design Aspects) do not apply to HBSCs, it was decided that a similar system would be used for indicating the importance of the human action to plant risk. The first two entries of the 3-part ranking code are therefore based on using the equivalent Cat & Class rules but applied to the function of the human action and its priority as a claimed measure (i.e. primary measure, secondary measure, ALARP action, etc.). This gives "category" and "class" indicators for the HBSC.

Added to the category and class indicators is a HF-importance indicator of High, Medium or Low, signifying the HF risk level assessed for the specific actions of the claim. The HF importance indicator was determined using HF specialist judgement guided by criteria related to: task novelty (both in terms of unique within the GDA analysis and to the operator when doing the task); frequency of task performance; complexity; requirement for the task to be performed in extreme working environments; etc.

Thus the resulting ranking code was structured as: (Category)(Class)-(HF Importance), e.g. A1-M, B2-L or C3-H. For ranking PSA-related HBSCs or actions claimed that are not a response to fault conditions (which drive the class indicator), slight variations to the above rules were used.

27.6.6.2 Substantiation of HBSCs

Once the HBSC was ranked, the level of substantiation required was determined based on a decision matrix. The matrix was based on the concept of other two-axis risk matrices, whereby the "equivalence" of different combinations of plant risk versus HF importance are accounted for. The matrix then dictates the substantiation level for that HBSC. The amount of detail for substantiation for each of the three levels given by the matrix were described in general terms for use as a guide by

the HF specialists doing the substantiation. Note that exceptions and variations to the general rules shown were possible, with appropriate justification for the exceptions.

The arguments for substantiating each claim follow a standard format and syntax. They are a similar set for similar types of claims, with some arguments that are specific to the context of the claim, and generic arguments that are almost universal for all HBSCs. These "generic arguments" essentially equated to the HF property claims. As such, the relevant HFSPCs for each functional HBSC were listed within the arguments section of each record. This is consistent with the system topic areas and the explanation of the role of SPCs as generic arguments for SFCs given in the SCDM [Ref-3].

Arguments and evidence that substantiate each HFSPC are given in a separate HBSC record for each HFSPC.

27.6.6.3 Recording and presentation of HBSCs

Following the identification, ranking and substantiation of each HBSC, they are recorded in the UK ABWR HBSC database. The database contains the following fields:

HBSC ID: The unique identifier that links the HBSC to the HLSF through the associated SSC(s) SFC/SPC.

HBSC Generic Type: The general nature of the claim being made, i.e. property or functional claim.

HBSC Specific Type: The specific type claim regarding what kind of protection or contribution to nuclear safety it gives.

Claim: A short description of the claim being made.

Context: A more detailed description of the scenario or conditions in which the claim is made.

Location of Operation: Where the claimed action is conducted from.

Related Human Failure Event Type: Identifies if the Claim is a Type A, B or C human failure events (PSA-related HBSCs only).

Ranking: Code indicating the HBSC risk-importance ranking.

Reason for Ranking: An explanation of how the ranking code was derived.

HBSC Substantiation (Argument): A list of the specific arguments being made to substantiate the HBSC. Each record identifies any related HFSPCs which act as generic arguments for all HF functional claims.

HBSC Substantiation (Evidence): A list of the evidence locations (reference documents) for each Argument being made, including an indication where further evidence will be provided by the future licensee. Whilst the HFSPCs act as generic arguments for the HF functional claims and are identified

in each record, the evidence to substantiate those generic arguments is only be contained in the HBSC records for the HFSPCs themselves.

Related HBSC(s): Reference to any other HBSCs within a group bounded by a single substantiation record.

ALARP Discussion (if necessary): Captures any recommendations and resolution decisions that provide justification that the claim or design supporting it contribute to risk level being ALARP.

Remark: Captures any relevant notes and commentary on the HBSC, including any key HF issues, assumptions, and recommendations on which the claim is based.

Source: A list of reference documents for Evidence as well as DSA & PSA Event IDs, Procedural Sequence IDs (for future use) and HMI Claim IDs that the HBSC is related to.

27.6.7 HBSCs

As a result of the above identification, grouping, ranking and substantiation activity throughout GDA, a comprehensive database of HBSCs has been developed. Because the information related to each HBSC record and required to provide adequate demonstration of the achievability of each claim is extensive, the HBSC coding, the source links and the evidence references provide the "golden thread" of substantiation for each claim. This allows each claim to be traced from the FSF it supports achievement of, through to each piece of detailed analysis or verification that shows it is a valid claim.

The use of a database allows for the more comprehensive linking of related aspects of the case. It ensures efficient management of the large amounts of related information, found in a variety of different documents both within and outside of the HF topic area, that are linked to each claim. However, Hitachi-GE also ensured that the database records still enable the reader to understand the effective demonstration of each claim and its links. The HBSC Report [Ref-1] describes, with examples, the standard structure and syntax of each of the key fields of each database record and how they are intended to be used to follow the substantiation "trail" for each HBSC.

27.6.7.1 Functional HBSCs

As shown in Figure 27.6-1, functional HBSCs are the specific claims on human actions required to achieve the FSFs and ALARP risk levels throughout the plant. They relate to both operational and EMIT actions that support achievement of both the SFCs and SPCs (respectively for each action type). In other words, functional HBSCs do not only support achievement of SFCs. Specific human actions are also claimed as required for some of the SPCs to be achieved.

Functional HBSCs that support achievement of SFCs are required to be explicitly identified within each relevant system or PCSR topic area, and within the safety analyses. As per the SCDM [Ref-3], where the SFCs in one system rely on functions of other supporting systems (e.g. electrical power, Heating Ventilation and Air Conditioning (HVAC), etc.) to achieve their HLSFs, those supporting system functions are listed as arguments for the main system SFC. They are also identified and substantiated as SFCs in the supporting system claim tree. The functional HBSCs that support SFCs

are specified as arguments in system BSCs in the same way as the other supporting system functions. Note that as per Figure 27.6-1, there are also HBSCs that support the "supporting SSCs" achieve their supporting functions.

Functional HBSCs that support achievement of SPCs (for example, plant being left in the correct alignment following maintenance to ensure that the related SSCs meet their SPC on availability) tend to be more implicit in nature and are not explicitly identified in the system topic BSCs or chapters within the PCSR. Within GDA these claims are limited to specific EMIT tasks whose correct performance is important to the availability of SSCs in risk-significant sequences within the PSA model. Generic claims on the correct and timely performance of required EMIT tasks across the plant are included as a single HF property claim (see Section 27.6.7.1) instead of individual functional HBSCs.

The comprehensive set of functional HBSCs, which represent the human actions important to the safety of UK ABWR identified within GDA, are presented in detail in the HBSC Report [Ref-1]. The report explains in detail the context and conditions related to each claim. In line with the structure of the other systems chapters, the claims are presented in summary within the claims lists shown in Appendix A of this chapter.

27.6.7.2 HF Property Claims

HF property claims relate to the broad holistic programme of HF activities supporting the UK ABWR design, and the generic HF principles that underpin a system and organisation design and operating practices that are optimised for human performance. The HF property claims were identified based on UK regulatory expectation for incorporating HFI in complex system design, as well as modern good HF practice and standards. The claims relate to the specific HF areas that comprise an effective HFI programme and ensure the adequate consideration of HF in the design and (in future) the organisation.

In addition to the properties of the HF activities undertaken that helped to optimise the design, generic broad "action" claims were needed to cover the variety of human actions done in the plant that are not specific functional HBSC. Notwithstanding specific more detailed substantiation of individual actions important to safety, the overall conduct of activities of operators and maintenance personnel on site must be done with care and attention such that the operational limits of the plant are adhered to and safety systems are not unduly called on to perform their role. As such, three generic claims related to the "organisational" properties of the UK ABWR were also made.

The HF property claims are presented in Appendix B Section B.1. The HF property claims act as SPCs for the HF topic area and as such they link to the requirements of the NSEDPs [Ref-2] that relate to HF. The identification of the relevant NSEDPs and the links to the HF property claims is presented in the HBSC Report [Ref-1]. Compliance with the NSEDPs is discussed in PCSR Chapter 5.

Note that there are HF property claims which are largely assumptive during GDA. These are identified within GDA for completeness (because they will need to be claimed for the future licensee

to be able to meet the ONR's Licence Conditions), but can only be partly substantiated within scope of this PCSR so they are "greyed out" in the tables in Appendix B.

Appendix B also lists the key HF engineering standards that have been applied through the HF design support activities, particularly the HFE Spec [Ref-9] (see Section 27.5.2). These form part of the argument for the HF property claims being met.

27.6.8 Arguments and Evidence

In line with the SCDM [Ref-3], the arguments and evidence to justify the claims are not presented at the PCSR chapter level, since the level of detail is much greater than belongs in a safety case "head" document. The full substantiation of each HBSC is presented in detail and managed through the HBSC database, as presented within the HBSC Report [Ref-1].

It should be noted that some of the HF property claims have only limited application within the GDA (those "greyed out" in the table in Appendix B.1) since they relate to areas that will only be developed in the site-specific stage of the UK ABWR. They are provided in GDA as "assumptive" claims to be taken up by the future licensee. As such they have limited substantiation with only basic development of arguments and evidence within scope of GDA. They are likely to change in nature in the site-specific stage.

27.7 Assumptions, Limits and Conditions for Operation

27.7.1 Purpose

One purpose of the generic PCSR is to identify constraints that must be applied by the future licensee of a UK ABWR plant to ensure safety during normal operation, fault and accident conditions. Some of these constraints are maximum or minimum limits on the values of system parameters, such as pressure or temperature. Others constraints are conditional, such as prohibiting certain operating modes (or certain conditions within modes), or requiring a minimum level of availability of required SSC. They are collectively described in other chapters of the GDA PCSR as Limits and Conditions for Operation (LCOs).

The generic PCSR must also clearly identify the working assumptions that are made in order to demonstrate that the SSCs will achieve all safety claims and that nuclear safety issues have been adequately considered in the GDA process. During commissioning and all phases of operation, the assumptions and LCOs made in the safety case are to be utilised to ensure that the plant is operated and maintained within safe operating conditions.

The applicability of LCOs, and the assumptions relevant to the HF topic area are described further in the remainder of this section. Assumptions and LCOs are described generically for the PCSR in Chapter 4: Safety Management throughout Plant Lifecycle, Section 4.12.

27.7.2 Limits and Conditions

LCOs are not derived from the HF topic area. As such this section differs to the equivalent sections for the systems and other chapters with SSCs. This section explains the relevance of LCOs to the HF topic area.

During normal operation, the plant is required to be maintained within a safe operating envelope. This prevents situations arising that could lead to anticipated operational occurrences, or accident conditions. This helps to minimise the consequences of such events if they do occur. If an unexpected deviation from an LCO actually occurs during normal operation, then the plant must be returned to a safe condition. The event should also be investigated and any appropriate corrective actions implemented.

As part of GDA, Hitachi-GE has developed the Generic Technical Specifications (GTS) [Ref-30] to capture all the LCOs and their related requirements for safe operations into one document. The GTS for GDA define the operational limits on plant parameters and corresponding actions required to ensure that plant operations remain inside the limits and conditions of the GDA Safety Case. They also provide a preserved level of margin (i.e. the operating envelope must always sit inside the safety case envelope). As described in Chapter 30: Operations, it is assumed that the future licensee will develop appropriate Operating Technical Specifications based on the GTS [Ref-30] and appropriate operating instructions and procedures. It is also assumed the future licensee will ensure that the plant

is operated in accordance with the Operating Technical Specifications. This ensures that the plant remains within the operating envelope defined by LCOs within the safety case.

It is expected that part of the HFI programme in the site-specific stage will be to ensure that any of the actions required to maintain the plant within, or return it to its operating envelope are achievable and clearly supported by operational arrangements that the future licensee will put in place.

27.7.3 Assumptions

The list of assumptions in this section are specific to the HF topic area, as presented within this chapter of the PCSR. They underpin the HFI programme of activities and are key to the validity of the HF analysis results. Note that there are many more detailed assumptions made in various activities and analysis within the GDA HF activities that apply specifically to those activities and analyses. Those assumptions are not listed here, but have been identified, categorised and captured in line with the assumptions and issues management processes described in the HFIP [Ref-6]. All assumptions will be transferred to the future licensee in the formal handover arrangements that will be in place for the UK ABWR at project level. The key assumptions are:

(1) The HFI programme, particularly its application of proportionality in the focus and scope of and within its activities, is suitable and sufficient to ensure that key risks to nuclear safety within the HF topic area have been identified.

(2) The HF methods chosen and/or adapted to be applied to the HF activities within the HFI programme are aligned with current accepted practice and the most applicable for the type of system design project and high-hazard industry that they are being applied to.

(3) The HF awareness training given to design engineers and engineering analysts, and the investiture of some HF responsibility in engineers who are not fully SQEP in order to perform basic HF support within design teams improves the effective integration of HF across the project without incurring any significant risk of invalid or missed important or required HF activities or results.

(4) In implementing the HFE Spec across the relevant engineering teams in a formal and systematic manner, and in recording non-compliances and performing audit sampling checks through V&V (rather than performing 100% positive checking of compliance to every requirement for every design document), no significant HF “fixed” design requirements were missed out of the compliance checks by the design teams and no significant non-compliances were missed upon doing the checks.

(5) Focussing the functional HBSC identification activities on the DSA and PSA, with graduated and screened consideration of other sources of claims, has identified the human actions of most importance to safety in the GDA safety case.

(6) The HF property claims, developed by HF SMEs taking due consideration of areas of HF good practice, are suitable and sufficient to demonstrate compliance with any applicable NSEDPs [Ref-2] relevant to HF to the extent possible in GDA.

(7) The UK ABWR concept of operations as described in the COR [Ref-21] and all its underpinning assumptions have been effectively incorporated into the design and analysis as require and will be broadly implemented in practice by the future licensee, or the impact of any significant deviations will be factored into the HF safety case in site-specific stage or beyond.

(8) The level of OPEX sought and used within the project has captured all significant learning points relevant to the HF programme for the UK ABWR to ensure that risks are reduced to ALARP in the GDA Safety Case.

(9) Where uncertainty in or lack of UK ABWR information exists, either reference plant design or operations information or suitably conservative estimations are used instead and these provide an analysis that is valid for the purposes of GDA and will be built upon or revised based on more accurate UK ABWR information in the site-specific stage.

(10) For any plant systems or equipment that are the same design as the reference plant (except where such items of plant relate to HBSCs), J-ABWR experience is assumed to have provided suitable validation of the basic design for general usability (see the BAR [Ref-5]) so no further analysis or V&V within GDA is necessary. Further, it is assumed that the need for and a suitable programme of V&V of these aspects of the design will be determined and conducted by the future licensee.

27.8 Summary of ALARP Justification

This section presents a high-level overview of how the ALARP principle has been applied for the HF topic area and how this contributes to the overall ALARP argument for the UK ABWR.

Generic PCSR Chapter 28: ALARP Evaluation presents the high-level approach taken for demonstrating ALARP across all aspects of the design and operation of the UK ABWR. It presents an overview of how the UK ABWR design has evolved, the further options that have been considered across all technical areas that have resulted in a number of design changes and how these contribute to the overall ALARP case. The approach to undertaking ALARP Assessment during GDA is described in the GDA ALARP Methodology [Ref-31] and SCDM [Ref-3].

Details of the ALARP position and the justification, including consideration of proportionality within the HFI programme of activities, plus summary of the residual risks and known assumptions that are passed onto the site-specific stage are given in the HF ALARP Report [Ref-4]. The material provided in this section is therefore a summary of that.

27.8.1 Risks Related to HF

In the HF topic area, the risks which must be identified, understood and managed relate to:

- Human failures during operations and / or EMIT which either contribute to the initiation of faults or events, or lead to the failure of the required safety measure (either through SSC unavailability or failed human action) required to mitigate a fault or event. This leads to increased risk of loss of the FSFs.
- Human failures which lead to increased personnel dose uptake either through normal operations or EMIT tasks being incorrectly conducted, increasing planned dose, or as a consequence of a fault or event.
- Human interactions with the plant and plant equipment being ineffective or unsafe, leading to risk of personnel conventional health and safety incidents, including death.

Note that this last risk is not explicitly part of the nuclear safety case and therefore is outside the scope of this ALARP justification; however, it is mentioned for completeness and also because the design options chosen to reduce the first two risks will almost certainly reduce the last (for SSCs within scope of the PCSR). This is due to the fact that conventional health and safety risks related to HF-related activities in GDA, and resolution of any related issues, were within the scope of the GDA HFI programme, as detailed within the HFIP [Ref-6]. As such, support was given to the related activities within GDA that reviewed conventional safety in relation to Construction Design and Management (CDM) regulations. This work is summarised in PCSR Chapter 4: Safety Management.

While the various and numerous elements of the HF work undertaken as part of the UK ABWR GDA safety case have sought to address the sets of risks defined above, it must be noted that achieving a totally ALARP position for HF within GDA is not feasible. The scope of GDA precludes significant consideration of organisational factors. Many such factors pertain directly to the HF safety case and therefore can only be captured as assumptions and recommendations for future licensees both to facilitate meaningful analysis during GDA and to ensure that such matters

are recognised and addressed post-GDA. This situation serves to highlight the importance of the HFI programme and approach in capturing and managing such risks and therefore providing a pillar for the overall ALARP justification for HF.

27.8.2 HF Relevant Good Practice

HF Relevant Good Practice (RGP) is extensive when it comes to design (see Appendix B for a list of RGP), but the most essential aspect of current standard HF practice for complex design projects is to have a suitably scoped programme of HF activities. These should be fully integrated with the design process, i.e. a HFI programme, as described in Section 27.3. The HFI programme for the UK ABWR during GDA has been fundamental to ensuring the implementation of other HF RGP within the design.

In both HF design and analysis activities, RGP has been applied in a managed and risk informed manner. Within the area of design this has been achieved through the development and implementation of the HFE Spec [Ref-9] that has disseminated and defined the relevant design related HF RGP. Consideration of HF within design and engineering is covered within many standards and good practice guides. The HFE Spec was used [Ref-9] for UK ABWR, to ensure the key relevant requirements from these RGP documents were effectively understood and applied by all the UK ABWR GDA design teams.

Regarding analytical process and methodologies; the need for the application of RGP has also been captured and addressed within the HFI programme. Embodied within the project HFMP [Ref-7] is the definition and justification for the suite of analytical methods and processes that have been applied during the UK ABWR GDA to support both design decisions and safety analyses such as PSA and DSA.

As noted in Section 27.4 the baseline design has already addressed HF considerations within the domestic context. Therefore, the UK ABWR design started from a position that had been informed by HF good practice.

27.8.3 HF Analysis

A key tenet of the HFI programme has been the extensive HF analysis activities that have been undertaken. These have been wide ranging in both scope and depth as reported in Section 27.5.3 of this chapter. This work has sought to understand the human contribution to risk in operation of the UK ABWR and to consider and substantiate how that risk is managed and controlled. Such work has also contributed to the design process through the identification of potential HF related issues and through the consideration of design options.

The overall scope of HF analyses was appropriate in considering the full extent of operator involvement with the plant in various plant states during the plant's lifecycle and in presenting a comprehensive set of HF related analyses. The analyses addressed:

- The allocation of functions between humans and engineered systems.
- Identification and substantiation of HBSC.

- Task analysis (including qualitative error identification and analysis).
- Analysis of staffing levels (through consideration of cognitive workload).
- HRA.

The use of the HFIP and HFMP to guide the analyses ensured that a systematic and justifiably ALARP approach has been taken to the management and integration of the HF analysis activities within GDA. Any issues arising from these analyses have been captured through the HFIR.

27.8.4 HF-Related Design Options Considered Within GDA

HF has been a key contributor to the design of the UK ABWR. Such input has increased as the design has progressed through the various steps of GDA. HF input to the design has been applied on a basis that; is proportionate to the apparent risk, is informed by the results of safety analyses and specific HF analyses and crucially is timely.

Because of the extensive nature of the HFI programme, there have been numerous design options chosen that improve the ability of the design to support required user interactions. The options and improvements have varied in scale and cannot all be listed here. Some important areas where design options to support improved task performance have been chosen include:

- Improvements to the AoF: examples include implementing automation for functions where human capability was challenged such as, SLC initiation, RHR S/P cooling mode switching, FHM operation (full automation option), as well as automation support (i.e. sequential automation) of manually-initiated functions such as certain RHR modes, etc.
- Improvements to the alarm presentation within the MCR, particularly the suppression of certain alarms in certain plant modes or states in order to ensure effective alarm processing.
- Improvements throughout the plant to plant layout, plant equipment and HMIs 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, presentation of information for cognitive processes, etc.).

In a more general way, HF specialist integration with all of the design teams throughout the GDA means that support has been provided to optioneering and ALARP work for every topic area. HF expertise has been provided to multi-disciplinary workshops and reviewing design materials when considering individual design options and decisions related to ALARP justification to ensure that those design decisions have balanced HF constraints along with technical ones.

Further detail on design support activities related to optioneering and issues resolution considering the ALARP principle are provided in the HF DER [Ref-8] and its supporting documents.

As with the design options that were chosen that support HF principles and optimise user interaction (Section 27.8.3), there have been numerous instances where conflicting constraints and the overall consideration of ALARP (i.e. not just the HF aspects) have meant that HF-recommended options were not chosen. Again, these cannot all be listed here; most of them have residual risk but in all cases that risk has been justified as ALARP (as documented within the HFIR [Ref-13]). As with any

complex design, it is to be expected that not all options that would make the design ALARP for HF-risk reasons, will make it ALARP for other risk reasons.

Specific more-significant examples include:

- Not automating the RHR system fully (i.e. all modes);
- Not automating FPC cooling pump start after a station black-out;
- No design solution for boron dilution EOC; and
- One of the reactor vessel instrument (RVI) calibration Type A common-cause failure (CCF) human failure events cannot have any designed safety measures to prevent or correct the error (relies on design solutions for alerting operators to the incorrect configuration, and then manual recognition of the error and suitable correction).

With regards the implementation of HF RGP through the HFE Spec [Ref-9], most non-compliant design options within the plant layout occur in the Reinforced Concrete Containment Vessel (RCCV). The RCCV size is considered fixed due to the complex and lengthy calculations required to ensure its critical structural integrity, and the risks of modifying it which removes the operating experience that is gained from having used the design in existing plants. The same is true of some of the clearances for access around the RBC and FHM due to the R/B size. Essentially the cost and disruption to the design of redesigning the R/B and the RCCV to improve compliance with the HF standards for accessibility and clearance are grossly disproportionate to the risks. Non-compliances have been assessed, particularly in areas where tasks are conducted (versus just access for travel), and local modifications introduced where possible to improve working conditions.

27.8.5 Summary of HF ALARP Position and Justification

In summary, Hitachi-GE have planned and successfully implemented a sufficient and suitable HFI programme within the GDA stage of the UK ABWR design. This has facilitated and enabled the HF topic area to undertake work on the project in a thorough and risk informed manner.

As a result of: the appropriately scoped analyses and integrated design support activities; the HF recommendations implemented; the HF issues registered and closed; the residual risks documented; and the substantiation of the HBSCs; it can be demonstrated that:

- Interactions between the human user and the system are fully understood.
- Any human actions related to nuclear safety (process and personnel) are identified.
- Those human actions that might impact on safety are adequately supported by the design.

As such, the risk of human error within the UK ABWR design has been demonstrated to be ALARP to the extent possible within GDA. Further detailed justification is provided within the HF ALARP Report [Ref-4].

27.9 Conclusions

In GDA, Hitachi-GE has implemented a suitably comprehensive and integrated programme of HF to support the development of the design and safety case for UK ABWR. The HFI programme started by assessing the baseline HF position in the reference ABWR plant. The baseline ABWR design was assessed in the context of UK and modern standard requirements. It was found to have incorporated a certain amount of formal and informal HF principles and analysis within its design and engineering. This was judged by Hitachi-GE HF SMEs to be have been relatively extensive and effective in its implementation. Gaps were identified that were then fed into the UK ABWR HFI programme to be resolved in GDA and subsequent design phases, as outlined in the BAR [Ref-5] and HFIP [Ref-6].

There were four elements of the integrated HF programme of activities that demonstrate that it was sufficient. Firstly, as described in Section 27.3, a systematic approach was taken to the management and integration of HF activities within GDA. Secondly the HF analyses undertaken for GDA were appropriate, because they addressed: AoF, utilised task analysis, addressed staffing levels and completed HRA (see Section 27.5.3 for details of these analyses). Thirdly, HF was addressed within the design generally and specifically in relation to workspaces and human system interfaces (see Section 27.5.2 for details of design input) Fourthly the safety claims involving humans were identified and substantiated (Section 27.6).

Critically, the functional HBSCs relating to human actions required to support the achievement of the FSFs have been systematically identified in all areas of the plant and throughout all relevant topic areas of this PCSR. They have been linked clearly to the overall FSFs and HLSFs for the plant. The HF property claims have also been systematically identified and linked to NSEDPs [Ref-2]. These are presented within the HBSC Report [Ref-1], and summarised in the functional claims list (Appendix A) and the property claims list (Appendix B) within this chapter. Compliance with the NSEDPs is discussed further in PCSR Chapter 5.

The chapter also presents the document map for this topic area (Appendix C) and descriptions within the body of the chapter to provide clear links to the supporting documents that provide the arguments and evidence needed to substantiate the HBSCs. These links, plus the list of key assumptions that underpin this chapter and the summary of the ALARP justification, have provided a comprehensive and complete safety case for the HF topic area as at the end of GDA.

27.10 References

[Ref-1] Hitachi-GE Nuclear Energy, Ltd., "Human-Based Safety Claims Report", GA91-9201-0001-00043 (HFE-GD-0064), Revision D, July 2017.

[Ref-2] Hitachi-GE Nuclear Energy, Ltd., "UK ABWR Nuclear Safety and Environmental Design Principles (NSEDPs)", GA10-0511-0011-00001 (XD-GD-0046), Rev.1, July 2017.

[Ref-3] Hitachi-GE Nuclear Energy, Ltd., "GDA Safety Case Development Manual", GA10-0511-0006-00001 (XD-GD-0036), Revision 3, June 2017.

[Ref-4] Hitachi-GE Nuclear Energy, Ltd., "Human Factors ALARP Report", GA91-9201-0003-02210 (HFE-GD-0524), Revision A, July 2017.

[Ref-5] Hitachi-GE Nuclear Energy, Ltd., "Baseline Human Factors Assessment Report", GA91-9201-0001-00032 (HFE-GD-0068), Revision B, August 2015.

[Ref-6] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Integration Plan", GA32-1501-0007-00001 (HFE-GD-0058), Revision D, August 2017.

[Ref-7] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Methodology Plan", GA91-9201-0001-00033 (HFE-GD-0059), Revision E, January 2017.

[Ref-8] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Design and Engineering Report", GA91-9201-0001-00039 (HFE-GD-0065), Revision C, August 2017.

[Ref-9] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Engineering Specification", GA91-9201-0001-00037 (HFD-GD-0001), Revision D, January 2017

[Ref-10] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Assessment Report", GA91-9201-0001-00042 (HFE-GD-0067), Revision D, August 2017

[Ref-11] Hitachi-GE Nuclear Energy, Ltd., "Human Reliability Analysis Report", GA91-9201-0001-00041 (HFE-GD-0066), Revision F, July 2017.

[Ref-12] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Requirements Compliance Tracking Matrix", GA91-9201-0001-00038 (HFE-GD-0062), Revision C, August 2017.

[Ref-13] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Issues Register", GA91-9201-0001-00036 (HFE-GD-0061), Revision C, August 2017.

[Ref-14] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Verification and Validation Plan", GA91-9201-0003-01353 (HFE-GD-0232), Revision A, October 2016.

[Ref-15] Hitachi-GE Nuclear Energy, Ltd., "Human Factors V&V Report", GA91-9201-0003-02209 (HFE-GD-0525), Revision A, August 2017.

[Ref-16] Hitachi-GE Nuclear Energy, Ltd., "Summary of the Generic Environmental Permit Applications", GA91-9901-0019-00001 (XE-GD-0094), Revision G, July 2016.

[Ref-17] Hitachi-GE Nuclear Energy, Ltd., "Conceptual Security Arrangements", GA91-9101-0301-00001 (XE-GD-0239), Revision C, September 2016.

[Ref-18] UK Office for Nuclear Regulation, "New nuclear reactors: Generic Design Assessment Guidance to Requesting Parties", ONR-GDA-GD-001, Revision 3, ONR, September

2016.

[Ref-19] Radioactive Substances Regulation – Environmental Principles, version 2, Environment Agency, April 2010.

[Ref-20] Hitachi-GE Nuclear Energy, Ltd., "ABWR General Description", GA91-9901-0032-00001 (XE-GD-0126), Revision 2, January 2017.

[Ref-21] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Concept of Operations Report", GA91-9201-0001-00034 (HFE-GD-0060), Revision E, April 2017.

[Ref-22] UK Office for Nuclear Regulation, "Safety Assessment Principles for Nuclear Facilities", 2014 Edition, Revision 0.

[Ref-23] US Nuclear Regulatory Commission, "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.

[Ref-24] Hitachi-GE Nuclear Energy, Ltd., "Hazards HRA Addendum", GA91-9201-0003-02050 (HFE-GD-0516), Rev. A, May 2017.

[Ref-25] Hitachi-GE Nuclear Energy, Ltd., "Task Performance Analysis for Non-PSA HBSCs", GA91-9201-0003-02051 (HFE-GD-0517), Revision A, July 2017.

[Ref-26] Hitachi-GE Nuclear Energy, Ltd., "Cognitive Workload Analysis Report", GA91-9201-0003-01727 (HFE-GD-0415), Revision A, February 2017.

[Ref-27] Hitachi-GE Nuclear Energy, Ltd., "Allocation of Function Report", GA91-9201-0001-00040 (HFE-GD-0063), Revision E, June 2017.

[Ref-28] Hitachi-GE Nuclear Energy, Ltd., "Error of Commission Analysis Report", GA91-9201-0003-00815 (HFE-GD-0157), Revision D, March 2017.

[Ref-29] Hitachi-GE Nuclear Energy, Ltd., "HCI-Induced Cognitive Error Analysis Report", GA91-9201-0003-01726 (HFE-GD-0416), Revision B, June 2017.

[Ref-30] Hitachi-GE Nuclear Energy, Ltd., "Generic Technical Specifications", GA80-1502-0002-00001 (SE-GD-0378), Revision 3, August 2017.

[Ref-31] Hitachi-GE Nuclear Energy, Ltd., "GDA ALARP Methodology", GA10-0511-0004-00001 (XD-GD-0037), Revision 1, November 2015.

[Ref-32] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Fault Assessment", GA91-9201-0001-00022 (UE-GD-0071), Revision 6, July 2017.

Appendix A: List of Functional HBSCs

The following two tables list the full set of functional HBSCs identified within GDA timeframe.

Table A-1 lists the functional HBSCs that support the achievement of other SSC SFCs, and therefore link directly to the HLSFs and FSFs, as shown in the table. HBSCs marked with "*" use a SFC which the HF specialists consider to be correct but does not necessarily exist yet within the related BSC. These items will be confirmed or altered through the live engineering schedule management process. In line with the required structure of the table, the plant conditions are noted and the related fault assessment fault sequences are to be listed. However, because most of the HBSCs listed are claimed in multiple and often numerous fault sequences, the table becomes unreadable due to size if all of the sequences are listed in this summary. Instead, the fault "group" is given (see reference in the table heading). The full list of fault sequences, and other safety analysis (i.e. PSA, etc.) instances where the action is claimed is recorded in the detailed HBSC database record, as shown in the HBSC Report [Ref-1].

Table A-2 lists the functional HBSCs that support the achievement of SPCs, as described in Section 27.6.7. Although not directly linked to the achievement of SFCs, as explained in the SCDM [Ref-3], the SPCs support the achievement of all SFCs for the system they are claimed.

Table A-1: Functional HBSCs Supporting Fundamental Safety Functions

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
1	Control of Reactivity	1-1	Functions to prevent excessive reactivity insertion	-	-	-	-	-
		1-2	Functions to maintain core geometry	-	-	-	-	-
		1-3	Emergency shutdown of the reactor	FS-1	RPS SCRAM (A1)	Fault Conditions	HF CRD 1-3.1_1	Operator recognises specific plant conditions where shutdown is required and manually SCRAMs the reactor using normal SCRAM hardswitches on the MCC.
		1-4	Functions to maintain sub-criticality	-	-	-	-	-
		1-5	Function of alternative reactivity control	FS-5	ARI (A2)	Fault Conditions	HF CRD 1-5.1_01	CRO manually initiates ARI from the HWBP as back-up to both the automated and manual RPS SCRAM (A1) functions, and the automated ARI (A2) function.
				FS-2	SLC (A2)	Fault Conditions	HF SLC 1-5.1_01	CRO manually initiates SLC from the HWBP as back-up to the automated and manual RPS SCRAM (A1) and ARI (A2) functions, and the automated SLC (A2) function.
					RC&IS	Fault Conditions	HF CRD 1-5.4_01	CRO drives the control rods into the reactor using the normal controls (RC&IS) on the MCC, as back-up to the automated and manual RPS SCRAM (A1) and ARI (A2) functions.
		1-6	Functions to circulate reactor coolant (functions to control reactivity of the core in normal operational states)	-	-	-	-	-
		1-7	Functions to plant instrument and control (except for safety protection function) (functions to control reactivity of the core in normal operational states)	-	-	-	-	-
		1-8	Functions to suppress reactor power increase with other system	-	-	-	-	-
		1-9	Functions to maintain sub-criticality of spent fuel outside the reactor coolant system	-	-	-	-	-

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
1	Control of Reactivity (continued)	1-10	Functions to maintain sub-criticality of spent fuel during processes of spent fuel removal from SFP to storage area and during interim storage period	-	-	Normal Conditions	HF SFIS 1-10.1_01	Suitable inspection and monitoring will be carried out on building conditions and spent fuel concrete storage casks when in storage.
				-	-	Normal Conditions	HF SFIS 1-10.1_02	The SFIS Operator(s) and maintenance technicians will take appropriate corrective action on spent fuel concrete storage casks or the SFIS building or any other SSCs to remediate and/or prevent any further damage or degradation to the casks or building SSCs.
2	Fuel Cooling	2-1	Functions to cool reactor core	FS7	HPCF (A1)	Fault Conditions	HF HPCF 2-1.1_01	CRO manually aligns and initiates HPCF(C) using the SAuxP.
				FS7	HPCF (A1)	Fault Conditions	HF HPCF 2-1.1_02	CRO manually switches the HPCF(C) water source from the Condensate Storage Tank (CST) to the Suppression Pool (S/P) using the SAuxP.
				FS-6	RCIC (A1)	Fault Conditions	HF SSLC 2-1.1.1_01	CRO manually initiates the automatic alignment and start sequence for RCIC using the MCC.
				FS-7	HPCF (A1)	Fault Conditions	HF SSLC 2-1.1.2_01	CRO manually initiates the automatic alignment and start sequence for HPCF(B) or HPCF(C) using the MCC.
				FS-9	ADS (A1)	Fault Conditions	HF SSLC 2-1.1.4_01	CRO manually initiates reactor depressurisation to support fuel cooling function using the Automatic Depressurisation System (ADS) initiation switches on the MCC.
				FS-13	SRV (A1)	Fault Conditions	HF NB 2-1.3_01	CRO manually depressurises the reactor to support fuel cooling function using the SRV hardwired switches on the WDP.
				FS-9	ADS (A1)	Fault Conditions	HF NB 2-1.3_02	CRO manually depressurises the reactor to support fuel cooling function using the Automatic Depressurisation System (ADS) SRV hardwired switches on the SAuxP.
		2-2	Function of alternative fuel cooling	-	FLSR (B3)	Fault Conditions	HF FLSR 2-2.2_01*	FO manually aligns and connects the FLSR mobile pump unit to the port for RPV injection outside the R/B as a defence in depth back-up to normal and other back-up fuel cooling systems (DBFs).
				-	FLSR (B3)	BDB Fault Conditions	HF FLSR 2-2.1_01	FO manually aligns and connects the FLSR mobile pump unit to the port for RPV injection outside the R/B as a defence in depth back-up to normal and other back-up fuel cooling systems (BDBFs).
				-	FLSS (B2)	Fault Conditions	HF FLSS 2-2.1_01	CRO manually initiates FLSS for RPV injection from the HWBP as fuel cooling function (DBFs).
				-	RDCF (B3)	Fault Conditions	HF RDCF 2-2.1_01	CRO manually depressurises the reactor to support fuel cooling function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the HWBP (in DBFs).
				-	RHR (B3)	Severe Accident Conditions	HF RHR 2-2.1_01* (with HF RHR 4-9.1_01*)	CRO manually aligns and initiates RHR(C) in low-pressure flooder (LPFL) mode using the SAuxP during severe accidents. (Before RPV failure).
				-	RHR (B3)	Severe Accident Conditions	HF SSLC 2-2.1.1_01* (with HF SSLC 4-9.1.1_01*)	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in low-pressure flooder (LPFL) mode using the MCC during severe accidents. (Before RPV failure).

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
2	Fuel Cooling (continued)	2-2	Function of alternative fuel cooling (continued)	-	FLSS (B2)	BDB Fault Conditions	HF FLSS 2-2.2_01	CRO manually initiates FLSS for RPV injection from the HWBP as fuel cooling function (BDBFs).
				-	FLSS (B2)	BDB Fault Severe Accident Conditions	HF FLSS 2-2.2_02	CRO manually initiates FLSS for RPV injection from the BBCP as fuel cooling function (BDBFs, SAs).
				-	RDCF (B3)	BDB Fault Conditions	HF RDCF 2-2.2_01	CRO manually depressurises the reactor to support fuel cooling function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the HWBP (in BDBFs).
				-	RDCF (B3)	BDB Fault Severe Accident Conditions	HF RDCF 2-2.2_02	CRO manually depressurises the reactor to support fuel cooling function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the BBCP (in BDBFs, SAs).
				-	SRV (C3)	BDB Fault Severe Accident Conditions	HF RDCF 2-2.3_01	FO manually connects dedicated back-up nitrogen gas cylinders to the supply lines of four SRV switching valves to actuate the SRVs and depressurise the reactor locally within the R/B (BDBFs, SAs).
		2-3	Function to make up reactor coolant with other system	-	FLSR (B3)	DB, BDB Fault Conditions	HF FLSR 2-3.1_01*	FO manually aligns and connects the FLSR mobile pump unit to the port for RPV injection outside the R/B to replenish reactor coolant level in support of decay heat removal function (DBFs, BDBFs).
				FS-12	FLSS (A2)	DB, BDB Fault Conditions	HF FLSS 2-3.1_01*	CRO manually initiates FLSS for RPV injection from the HWBP to replenish reactor coolant level in support of decay heat removal function (DBFs, BDBFs).
				FS-12	FLSS (A2)	Fault Conditions	HF FLSS 2-3.1_02*	CRO manually initiates FLSS for RPV injection from the BBCP to replenish reactor coolant level in support of decay heat removal function (DBFs).
				FS-7	HPCF (A1)	Fault Conditions	HF HPCF 2-3.1_01*	CRO manually aligns and initiates HPCF(C) from the SAuxP to replenish reactor water level in support of decay heat removal function (during shutdown faults).
				FS-7	HPCF (A1)	Fault Conditions	HF HPCF 2-3.1_02*	CRO manually aligns and initiates HPCF(B) from the Division II RSP to replenish reactor water level in support of decay heat removal function (during shutdown faults).
				-	MUWC (C3)	Fault Conditions	HF MUWC 2-3.1_01*	CRO manually aligns and initiates the MUWC system to make up water to the RPV via the RHR return line using the MCC (to replenish reactor coolant).
				FS-13	SRV (A1)	Fault Conditions	HF NB 2-3.1_01*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the SRV hardwired switches on the WDP.
				FS-9	ADS (A1)	Fault Conditions	HF NB 2-3.1_02*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Automatic Depressurisation System (ADS) SRV hardwired switches on the SAuxP.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
2	Fuel Cooling (continued)	2-3	Function to make up reactor coolant with other system (continued)	FS-9	ADS (A1)	Fault Conditions	HF NB 2-3.1_03*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Automatic Depressurisation System (ADS) SRV hardwired switches on the RSP.
				-	RDCF (B3)	DB, BDB Fault Conditions	HF RDCF 2-3.1_01*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the HWBP (in DBFs, BDBFs).
				-	RDCF (B3)	Fault Conditions	HF RDCF 2-3.1_02*	CRO manually depressurises the reactor to support replenishment of reactor coolant level in decay heat removal function using the Reactor Depressurisation Control Facility (RDCF) SRV hardwired switches on the BBCP (in DBFs).
				FS-8	LPFL (A1)	Fault Conditions	HF RHR 2-3.1_01*	CRO manually aligns and initiates RHR(C) in low-pressure flooder (LPFL) mode from the SAuxP to replenish reactor water level in support of decay heat removal function (during shutdown faults).
				FS-7	HPCF (A1)	Fault Conditions	HF SSLC 2-3.1.1_01*	CRO manually initiates the automatic alignment and start sequence for HPCF(B) or HPCF(C) from the MCC to replenish reactor water level in support of decay heat removal function (during shutdown faults).
				FS-8	LPFL (A1)	Fault Conditions	HF SSLC 2-3.1.2_01*	CRO manually initiates the automatic alignment and start sequence of RHR in LPFL mode from the MCC to replenish reactor water level in support of decay heat removal function (during shutdown faults).
				FS-9	ADS (A1)	Fault Conditions	HF SSLC 2-3.1.3_01*	CRO manually initiates reactor depressurisation to support replenishment of reactor coolant level in decay heat removal function using the Automatic Depressurisation System (ADS) initiation switches on the MCC.
				-	FLSS (B2)	Fault Conditions	HF FLSS 2-3.2_01*	CRO manually initiates FLSS for SFP spray from the HWBP to replenish reactor coolant level via the SFP in support of decay heat removal function (DBFs).
				-	FLSS (B2)	Fault Conditions	HF FLSS 2-3.3_01*	CRO manually initiates FLSS for reactor well injection from the HWBP to replenish reactor coolant level in support of decay heat removal function (DBFs).
		2-4	Function to cool spent fuel outside the reactor coolant system	-	FPC (A1)	Fault Conditions	HF FPC 2-4.1_01	CRO manually restarts duty pump FPC Pump(D) (FPC(B)) from the MCC.
				-	FPC (A1)	Fault Conditions	HF FPC 2-4.1_02	CRO manually restarts normal duty pump FPC Pump(D) (FPC(B) train) from the SAuxP.
				-	FPC (A1)	Fault Conditions	HF FPC 2-4.1_03	CRO manually aligns and starts standby pump FPC Pump(A) (FPC(A) train) from the MCC.
				-	FPC (A1)	Fault Conditions	HF FPC 2-4.1_04	CRO manually aligns and starts standby pump FPC Pump(A) (FPC(A) train) from the SAuxP.
				-	RCW (A1)	Fault Conditions	HF RCW 2-4.1_01	CRO manually restarts RCW(B) pumps (B&D) from the MCC (for spent fuel cooling function).

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
2	Fuel Cooling (continued)	2-4	Function to cool spent fuel outside the reactor coolant system (continued)	-	RCW (A1)	Fault Conditions	HF RCW 2-4.1_02	CRO manually aligns and initiates RCW(C) from the SAuxP (to support spent fuel cooling function).
				-	RCW (A1)	Fault Conditions	HF RCW 2-4.1_03	CRO manually restarts RCW(A) pumps (A&C) from the MCC (for spent fuel cooling function).
				-	RCW (A1)	Fault Conditions	HF RCW 2-4.1_04	CRO manually restarts RCW(A) pumps (A&C) from the SAuxP (for spent fuel cooling function).
				-	RHR (A1)	Fault Conditions	HF RHR 2-4.1_01	CRO manually aligns and initiates RHR(A) or RHR(B) in SFP cooling mode from the MCC.
				-	-	Fault Conditions	HF SFS 2-4.1_01	CRO manually isolates a SFP liner leak by closing the SFP liner drain valve using the MCC.
		2-5	Functions to make up water for spent fuel pool	-	SPCU (C3)	Fault Conditions	HF FPC 2-5.1_01	CRO manually aligns and initiates the SPCU system to make up water from the suppression pool (S/P) or condensate storage tank (CST) to the SFP using the MCC.
				-	MUWC (C3)	Fault Conditions	HF FPC 2-5.1_02	CRO (with FO) manually aligns and initiates the MUWC system to make up water to the SFP via the RHR-FPC injection line from local-to-plant (RHR-FPC injection isolation valve) then using the MCC.
				-	MUWC (C3)	Fault Conditions	HF FPC 2-5.1_03	CRO (with FO) manually aligns and initiates the MUWC system to make up water to the SFP via MUWC injection to the skimmer surge tanks, from local-to-plant (skimmer surge tank make-up water stop valve and circuit breaker) and then using the MCC.
				-	FP (C3)	Fault Conditions	HF FPC 2-5.1_04	CRO (with FO) manually aligns and initiates the FP system to make up water to the SFP via the RHR-FPC injection line from local-to-plant (RHR-FPC injection isolation valve) then using the MCC.
				-	FP (C3)	Fault Conditions	HF FPC 2-5.1_05	CRO (with FO) manually aligns and initiates the fire protection (FP) system to make up water to the SFP via the MUWC injection to the skimmer surge tanks, from local-to-plant (skimmer surge tank make-up water stop valve and circuit breaker) and then using the MCC.
				-	FLSS (B2)	Fault Conditions	HF FLSS 2-5.1_01	CRO manually initiates FLSS for SFP spray from the HWBP to make up SFP water level during SFP design-basis faults.
				-	RHR (A1)	Fault Conditions	HF RHR 2-5.1_01*	CRO manually aligns and initiates RHR(A) or RHR(B) in SFP cooling mode from the MCC to provide SFP make-up water.
				-	FLSS (B2)	BDB Fault Conditions	HF FLSS 2-5.2_01	CRO manually initiates FLSS for SFP spray from the HWBP to make up SFP water level during SFP beyond design-basis faults.
				-	FLSS (B2)	Severe Accident Conditions	HF FLSS 2-5.2_02	CRO manually initiates FLSS for SFP spray from the BBCP to cool fuel and mitigate damage and release from fuel uncovery, during severe accidents involving the SFP.
				-	FLSR (B3)	Fault Conditions	HF FLSR 2-5.2_01*	FO manually aligns and connects the FLSR mobile pump unit to the port for SFP spray to make up SFP water level during SFP design-basis faults.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
2	Fuel Cooling (continued)	2-5	Functions to make up water for spent fuel pool (continued)	-	FLSR (B3)	BDB Fault Conditions	HF FLSR 2-5.1_01	FO manually aligns and connects the FLSR mobile pump unit to the port for SFP spray to make up SFP water level during SFP beyond design-basis faults and severe accidents.
		2-6	Functions to maintain spent fuel temperature limit during processes of spent fuel removal from SFP to storage area and during interim storage period	-	-	Fault Conditions	HF SFE 2-6.1_01	FRO will manually shutdown the spent fuel canister drying system as a back-up to the automatic over-temperature protection system (OTPS).
				-	-	Fault Conditions	HF SFE 2-6.1_02	FRO(s) will manually set up and operate the Backup Canister Cooling System (BCCS) when the automatic Canister Cooling System (CCS) is unavailable.
				-	-	Fault Conditions	HF SFE 2-6.1_03	In the event that a spent fuel transfer cask gas leak occurs during canister drying, the FRO is required to recognise and isolate the leak then monitor for canister cooling system (CCS) initiation.
				-	-	Normal Conditions	HF SFE 2-6.1_04	RBC Operator will manually lower the transfer cask with filled fuel canister down from the cask stand into the bottom of the cask pit in the spent fuel pool (SFP) and FRO will ensure cask pit is refilled with water.
				-	-	Normal Conditions	HF SFIS 2-6.1_01	Suitable inspection and monitoring will be carried out on building conditions and spent fuel concrete storage casks when in storage.
				-	-	Normal Conditions	HF SFIS 2-6.1_02	The SFIS Operator(s) and maintenance technicians will take appropriate corrective action on spent fuel concrete storage casks or the SFIS building or any other SSCs to remediate and/or prevent any further damage or degradation to the casks or building SSCs.
3	Long term heat removal	3-1	Functions to remove residual heat after shutdown	FS-13	SRV (A1)	Fault Conditions	HF NB 3-1.1_01	CRO manually depressurises the reactor to support long-term heat removal using the SRV hardwired switches on the WDP.
				FS-13	SRV (A1)	Fault Conditions	HF NB 3-1.1_02	CRO manually depressurises the reactor to support long-term heat removal using the Automatic Depressurisation System (ADS) SRV hardwired switches on the SAuxP.
				FS-13	SRV (A1)	Fault Conditions	HF NB 3-1.1_03	CRO manually depressurises the reactor to support long-term heat removal using the Automatic Depressurisation System (ADS) SRV hardwired switches on the RSP.
				FS-14	RHR (A1)	Fault Conditions	HF SSLC 3-1.1.1_01	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in shutdown cooling (SDC) mode using the MCC.
				FS-9	ADS (A1)	Fault Conditions	HF SSLC 3-1.1.2_01	CRO manually initiates reactor depressurisation to support long-term heat removal using the Automatic Depressurisation System (ADS) initiation switches on the MCC.
				FS-14	RHR (A1)	Fault Conditions	HF SSLC 3-1.1.3_01	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in suppression pool (S/P) cooling mode using the MCC.
				FS-14	RHR (A1)	Fault Conditions	HF RHR 3-1.2_01	CRO manually aligns and initiates RHR(C) in shutdown cooling (SDC) mode using the SAuxP.
				FS-14	RHR (A1)	Fault Conditions	HF RHR 3-1.2_02	CRO manually aligns and initiates RHR(A) or RHR(B) in shutdown cooling (SDC) mode from the RSPs.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
3	Long term heat removal (continued)	3-1	Functions to remove residual heat after shutdown (continued)	FS-14	RCW (A1)	Fault Conditions	HF RCW 3-1.2_01	CRO manually aligns and initiates RCW(C) from the SAuxP (to support RHR long-term and containment heat removal functions).
				FS-14	RCW (A1)	Fault Conditions	HF RCW 3-1.2_02	CRO manually aligns and initiates RCW(A) or RCW(B) from the RSPs (to support RHR long-term and containment heat removal functions).
				FS-14	RHR (A1)	Fault Conditions	HF RHR 3-1.3_01	CRO manually aligns and initiates RHR(C) in low-pressure flooder (LPFL) mode using the SAuxP.
				FS-14	RHR (A1)	Fault Conditions	HF RHR 3-1.4_01	CRO manually aligns and initiates RHR(C) in suppression pool (S/P) cooling mode using the SAuxP.
				FS-14	RHR (A1)	Fault Conditions	HF RHR 3-1.4_02	CRO manually aligns and initiates RHR(A) or RHR(B) in suppression pool (S/P) cooling mode using the RSPs.
		3-2	Function of alternative containment cooling and decay heat removal	FS-17	AC (A2)	Fault Conditions	HF AC 3-2.1_01	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs, using the Atmospheric Control (AC) System controls on the MCC.
				FS-17	AC (A2)	Fault Conditions	HF AC 3-2.1_02 (with HF FCVS 3-2.1_01)	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs, using switches on the HWBP to align and open the valves of the Atmospheric Control (AC) System.
				FS-17	AC (A2)	BDB Fault Conditions	HF AC 3-2.1_03 (with HF FCVS 3-2.2_01)	CRO manually initiates containment venting, prior to core damage and containment failure in BDBFs, using switches on the HWBP to align and open the valves of the Atmospheric Control (AC) System.
				-	FCVS (A2)	Fault Conditions	HF FCVS 3-2.1_01 (with HF AC 3-2.1_02)	CRO manually initiates containment venting, prior to core damage and containment failure in DBFs, using switches on the HWBP to align and open the valves of the Filtered Containment Vent System (FCVS).
				FS-7	HPCF (A1)	Fault Conditions	HF HPCF 3-2.1_01*	During HPCF injection when the S/P temperature increases to a certain temperature, CRO switches the water source back to Condensate Storage Tank (CST) from the Suppression Pool (S/P) using the SAuxP.
				FS14	RHR (A1)	Fault Conditions	HF RHR 3-2.1_01*	CRO manually aligns and initiates RHR(C) in PCV spray cooling mode using the SAuxP.
				FS14	RHR (A1)	Fault Conditions	HF SSLC 3-2.1.1_01*	CRO manually initiates the automatic alignment and start sequence of RHR(B) or RHR(C) in PCV spray cooling mode using the MCC.
				-	FCVS (A2)	BDB Fault Conditions	HF FCVS 3-2.2_01 (with HF AC 3-2.1_03)	CRO manually initiates containment venting, prior to core damage and containment failure in BDBFs, using switches on the HWBP to align and open the valves of the Filtered Containment Vent System (FCVS).
				-	FCVS (A2)	BDB Fault Conditions	HF FCVS 3-2.2_02	CRO manually initiates containment venting, in BDBFs and severe accidents, using switches on the BBCP to align and open the valves of the Filtered Containment Vent System (FCVS).
4	Confinement/Containment of radioactive materials	4-1	Functions to form reactor coolant pressure boundary	FS-17	HPCF (A1)	Fault Conditions	HF HPCF 4-1.1_01	CRO manually stops HPCF injection at reactor water level L8 from the SAuxP.
				-	-	Normal Conditions	HF SI 4-1.1_01	Accessibility to SSCs for In-Service Inspection (ISI) is maintained in accordance with the classification of its components.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
4	Confinement/Containment of radioactive materials (continued)	4-1	Functions to form reactor coolant pressure boundary	-	-	Normal Conditions	HF SI 4-1.5_01	In-Service Inspection (ISI) is conducted in accordance with the requirements for SSC classification to ensure structural integrity is validated.
		4-2	Functions to prevent overpressure within the reactor coolant pressure boundary	-	-	-	-	-
		4-3	Functions to contain reactor coolant	-	-	-	-	-
		4-4	Functions to retain reactor coolant (other than No.4-1 and 4-3)	-	-	-	-	-
		4-5	Functions to reseat safety valves and relief valves	-	-	-	-	-
		4-6	Functions to mitigate reactor pressure increase with other system (other than No.4-2)	-	-	-	-	-
		4-7	Functions to confine radioactive materials, shield radiation, and reduce radioactive release	-	-	Fault Conditions	HF CUW 4-7.1_01 (with HF LDS 4-7.1_02)	CRO manually isolates the CUW inlet line using the MCC.
				-	-	Fault Conditions	HF LDS 4-7.1_01 (with HF RHR 4-7.1_01)	CRO manually isolates the RHR inlet line using the MCC.
				-	-	Fault Conditions	HF LDS 4-7.1_02 (with HF CUW 4-7.1_01)	CRO manually isolates the CUW inlet line using the MCC.
				-	-	Fault Conditions	HF LDS 4-7.1_03	CRO manually isolates the drain line using the MCC.
				-	-	Fault Conditions	HF RHR 4-7.1_01 (with HF LDS 4-7.1_01)	CRO manually isolates the RHR inlet line using the MCC.
				-	-	Fault Conditions	HF SSLC 4-7.1.1_01	CRO initiates the automated closure of the containment valves using the Primary Containment Isolation System (PCIS) initiation switch.
				-	-	Fault Conditions	HF HVAC 4-7.2_01	CRO closes the Reactor Area (R/A) HVAC isolation damper from the MCC.
				-	-	Fault Conditions	HF HVAC 4-7.2_02 (with HF HVAC 5-18.2_02)	CRO or FO opens the connecting valves between operating deck to main stack to release heat but mitigate against radiological release.
				-	-	Fault Conditions	HF NB 4-7.2_01	CRO closes the MSIVs to isolate the RPV using the MCC.
				-	-	Fault Conditions	HF SGTS 4-7.2_01	CRO manually initiates SGTS from the SACS section of the MCC.
		4-8	Functions to minimise the release of radioactive gases	-	-	Fault Conditions	HF OG 4-8.1_01	CRO will manually isolate the Off Gas (OG) system in the event of OG system containment failure, as a back-up to automatic isolation.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
4	Confinement/Containment of radioactive materials (continued)	4-8	Functions to minimise the release of radioactive gases (continued)	-	-	Fault Conditions	HF OG 4-8.1_02	CRO will manually isolate the Off Gas (OG) system in the event of a charcoal adsorber fire, to suffocate the fire.
				-	-	Fault Conditions	HF OG 4-8.1_03	CRO will perform normal shut down of the reactor in the event of OG system fault conditions that cause performance degradation of the OG Charcoal Adsorbers.
				-	-	Fault Conditions	HF STACK 4-8.1_01	CRO will take appropriate action to respond to the MCR alarm if radiation levels in the discharge from the main stack increase.
		4-9	Functions to contain radioactive materials in the event of a severe accident	-	FLSR (B3)	Severe Accident Conditions	HF FLSR 4-9.1_01	FO manually aligns and connects the FLSR mobile pump unit to the port for PCV spray (upper drywell (D/W) injection) after RPV breach in order to provide D/W cooling and prevent PCV failure (SAs).
				-	FLSS (B2)	Severe Accident Conditions	HF FLSS 4-9.1_01	CRO manually initiates FLSS for PCV spray (upper drywell (D/W) injection) from the BBCP after RPV breach in order to provide D/W cooling and prevent PCV failure (SAs).
				-	RHR (C3)	Severe Accident Conditions	HF RHR 4-9.1_01* (with HF RHR 2-2.1_01*)	CRO manually aligns and initiates RHR(C) in low-pressure flooder (LPFL) mode using the SAuxP during severe accidents. (After RPV failure).
				-	RHR (C3)	Severe Accident Conditions	HF SSLC 4-9.1.1_01* (with HF SSLC 2-2.1.1_01*)	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in low-pressure flooder (LPFL) mode using the MCC during severe accidents. (After RPV Failure).
				-	RHR (C3)	Severe Accident Conditions	HF SSLC 4-9.1.2_01*	CRO manually initiates the automatic alignment and start sequence of RHR(B) or RHR(C) in PCV spray cooling mode using the MCC during severe accidents.
				-	RHR (C3)	Severe Accident Conditions	HF SSLC 4-9.1.3_01*	CRO manually initiates the automatic alignment and start sequence of RHR(A), RHR(B) or RHR(C) in suppression pool (S/P) cooling mode using the MCC during severe accidents.
				-	FLSR (B3)	Severe Accident Conditions	HF FLSR 4-9.2_01	FO manually aligns and connects the FLSR mobile pump unit to the port for lower drywell (D/W) injection after RPV breach in order to provide D/W cooling and prevent PCV failure (SAs).
				-	FLSS (B2)	BDB Fault Severe Accident Conditions	HF FLSS 4-9.2_01	CRO manually initiates FLSS for lower D/W injection from the HWBP before RPV breach in order to provide lower D/W cooling and prevent RPV and PCV failure (BDBFs, SAs)
				-	FLSS (B2)	Severe Accident Conditions	HF FLSS 4-9.2_02	CRO manually initiates FLSS for lower drywell (D/W) injection from the BBCP after RPV breach in order to provide molten core cooling and prevent PCV failure (SAs).
				-	RHR (C3)	Severe Accident Conditions	HF RHR 4-9.2_01*	CRO manually aligns and initiates RHR(C) in PCV spray cooling mode using the SAuxP during severe accidents.
				-	RHR (C3)	Severe Accident Conditions	HF RHR 4-9.3_01*	CRO manually aligns and initiates RHR(C) in suppression pool (S/P) cooling mode using the SAuxP during severe accidents.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
4	Confinement/Containment of radioactive materials (continued)	4-10	Functions to prevent the dispersion of fission products into reactor coolant, spent fuel pool and canister	-	-	-	-	-
		4-11	Functions to store the radioactive materials as gaseous waste	-	OG (A1)	Fault Conditions	HF OG 4-11.3_01	CRO will either manually switch to the standby OG Recombiner or manually isolate the Off Gas (OG) system (if hydrogen continues to build), as a back-up to automatic isolation on failure or degradation of the OG Recombiner and build-up of hydrogen in the OG system.
		4-12	Functions to store the radioactive materials as liquid wastes	-	-	Normal Conditions	HF LWMS 4-12.1_01	Manual actions required to ensure that radioactivity of liquid wastes is minimised will be conducted safely and effectively.
				-	-	Normal Conditions	HF LWMS 4-12.2_01	Manual actions required to ensure that volumes of liquid wastes are minimised will be conducted safely and effectively.
				-	-	Normal Conditions	HF LWMS 4-12.3_01	The required operator actions will be conducted effectively to reduce dose to personnel and public during normal operations.
				-	-	Normal Conditions	HF LWMS 4-12.5_01	Appropriate levels of monitoring, measuring and sampling will be conducted effectively to ensure waste meets the relevant Waste Acceptance Criteria.
				-	-	DB, BDB Fault Conditions	HF LWMS 4-12.6_01	The required operator actions will be conducted effectively to ensure doses to personnel and the public in fault conditions are within limits and targets for DBFs and BDBFs.
		4-13	Functions to store the radioactive materials as solid wastes	-	-	Normal Conditions	HF SWMS 4-13.1_01	Manual actions required to ensure that volumes of solid wastes are minimised will be conducted safely and effectively.
				-	-	Normal Conditions	HF SWMS 4-13.2_01	The required operator actions will be conducted effectively to reduce dose to personnel and public during normal operations.
				-	-	Normal Conditions	HF SWMS 4-13.4_01	Appropriate levels of monitoring, measuring and sampling will be conducted effectively to ensure waste meets the relevant Waste Acceptance Criteria.
				-	-	DB, BDB Fault Conditions	HF SWMS 4-13.5_01	The required operator actions will be conducted effectively to ensure doses to personnel and the public in fault conditions are within limits and targets for DBFs and BDBFs.
				-	-	Normal Conditions	HF SWMS 4-13.6_01	Manual actions required to process solid wastes into packages will be done such that they ensure suitability for off-site transport to the appropriate nominated facility for incineration, recycling or direct disposal.
				-	-	Normal Conditions	HF SWMS 4-13.7_01	Actions to receive waste in the ILW Store will be conducted effectively and safely .
				-	-	Normal Conditions	HF SWMS 4-13.7_02	Suitable inspection and monitoring will be carried out on ILW building conditions and waste packages when in storage.
				-	-	Normal Conditions	HF SWMS 4-13.7_03	ILW Store operators will take appropriate corrective action on waste packages, the ILW Store building or any other related SSCs to remediate and/or prevent any further damage or degradation to the waste packages or building SSCs.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	**Description**	**Fault Group**	**Front System**	**State**	**Claim ID**	**Claim Contents**
4	Confinement/Containment of radioactive materials (continued)	4-13	Functions to store the radioactive materials as solid wastes (continued)	-	-	Normal Conditions	HF SWMS 4-13.7_04	ILW Store records will be managed appropriately to ensure waste packages can be tracked and monitored effectively.
		4-14	Functions to provide containment barrier during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	Normal Conditions	HF SFIS 4-14.1_01	Suitable inspection and monitoring will be carried out on building conditions and spent fuel concrete storage casks when in storage.
				-	-	Normal Conditions	HF SFIS 4-14.1_02	SFIS Operator(s) and maintenance technicians will take appropriate corrective action on spent fuel concrete storage casks or the SFIS building or any other SSCs to remediate and/or prevent any further damage or degradation to the casks or building SSCs.
		4-15	Function to mitigate impact of radioactive release	-	-	-	-	-
		4-16	Functions to provide radiation shield during processes of spent fuel removal from Cask Pit to storage area and during interim storage period	-	-	Normal Conditions	HF SFIS 4-16.1_01	Suitable inspection and monitoring will be carried out on building conditions and spent fuel concrete storage casks when in storage.
				-	-	Normal Conditions	HF SFIS 4-16.1_02	SFIS Operator(s) and maintenance technicians will take appropriate corrective action on spent fuel concrete storage casks or the SFIS building or any other SSCs to remediate and/or prevent any further damage or degradation to the casks or building SSCs.
5	Others	5-1	Functions to generate actuation signals for the engineered safety features and reactor shutdown system	-	-	-	-	-
		5-2	Supporting functions especially important to safety	-	-	Fault Conditions	HF EPS 5-2.1_01 (with HF EPS 5-3.1_01 and HF EPS 5-3.3_03)	FO switches over the power source of the Class 3 lighting system (which includes MCR lighting) to the available back-up source (EDG).
				-	-	Fault Conditions	HF EPS 5-2.1_02 (with HF EPS 5-3.1_03 and HF EPS 5-3.3_04)	FO refills Light Oil Tank (LOT) before tank is emptied after 7 days of use (EDG).
		5-3	Function of alternative supporting system	-	-	Fault Conditions	HF EPS 5-3.1_01 (with HF EPS 5-2.1_01 and HF EPS 5-3.3_03)	FO switches over the power source of Class 3 lighting system (which includes MCR lighting) to the available back-up source during SBO (BBG).
				-	-	Severe Accident Conditions	HF EPS 5-3.1_02	FO (with CRO) connects the small power truck (SPT) to the diverse safety Class 1 P/C bus connecting ports on the outside wall of the R/B.
				-	-	Severe Accident Conditions	HF EPS 5-3.1_03 (with HF EPS 5-2.1_02 and HF EPS 5-3.3_04)	FO refills the Light Oil Tank (LOT) before tank is emptied after 7 days of use (BBG).
				-	-	Fault Conditions	HF EPS 5-3.3_01	CRO starts the Diverse Additional Generator (DAG) and connects the correct bus from the MCC during SBO.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
5	Others (continued)	5-3	Function of alternative supporting system (continued)	-	-	Severe Accident Conditions	HF EPS 5-3.3_02	FO (with CRO) connects the large power truck (LPT) to the diverse safety Class 1 power bus connecting ports on the outside wall of the R/B.
				-	-	Fault Conditions	HF EPS 5-3.3_03 (with HF EPS 5-2.1_01 and HF EPS 5-3.1_01)	FO switches over the power source of Class 3 lighting system (which includes MCR lighting) to the available back-up source during (DAG).
				-	-	Severe Accident Conditions	HF EPS 5-3.3_04 (with HF EPS 5-2.1_02 and HF EPS 5-3.1_03)	FO refills Light Oil Tank (LOT) before tank is emptied after 7 days of DAG use.
		5-4	Functions to monitor plant conditions in case of an accident	-	-	-	-	-
		5-5	Functions to shut down safely from outside the control room	-	-	-	-	-
		5-6	Functions to handle fuel and heavy equipment safely	-	-	Normal Conditions	HF FHM 5-6.4_01*	Fuel route engineers (FREs) and FHM operators (FROs) will plan fuel movements and move fuel assemblies with sufficient attention and accuracy such that the likelihood of a fuel misload event is minimised.
				-	-	Normal Conditions	HF FHM 5-6.1_01 (with HF NSC 5-6.1_02)	FROs will operate the FHM with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load or collision are minimised.
				-	-	Normal Conditions	HF FHM 5-6.1_02	FOs/FROs will assemble, check and attach lifting attachments correctly so as to ensure that load paths are maintained.
				-	-	Normal Conditions	HF FPM 5-6.1_01 (with HF NSC 5-6.1_03)	FROs will operate the Fuel Preparation Machine (FPM) with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load or collision are minimised.
				-	-	Normal Conditions	HF NFIS 5-6.1_01	FROs will operate the New Fuel Inspection Stand (NFIS) with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load are minimised.
				-	-	Normal Conditions	HF NSC 5-6.1_01 (with HF RBC 5-6.1_01)	RBC Operator will operate the RBC with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load or collision are minimised.
				-	-	Normal Conditions	HF NSC 5-6.1_02 (with HF FHM 5-6.1_01)	FROs will operate the FHM with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load or collision are minimised.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	Description	Fault Group	Front System	State	Claim ID	Claim Contents
5	Others (continued)	5-6	Functions to handle fuel and heavy equipment safely (continued)	-	-	Normal Conditions	HF NSC 5-6.1_03 (with HF FPM 5-6.1_01)	FROs will operate the Fuel Preparation Machine (FPM) with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load or collision are minimised.
				-	-	Normal Conditions	HF RBC 5-6.1_01 (with HF NSC 5-6.1_01)	RBC Operator will operate the RBC with due care and attention such that incorrect load movements that might compromise load path integrity and/or lead directly or indirectly to a dropped load or collision are minimised.
				-	-	Normal Conditions	HF RBC 5-6.1_02	FOs/FROs will assemble, check and attach lifting attachments correctly so as to ensure that load paths are maintained.
				-	-	Normal Conditions	HF FHM 5-6.2_01	FROs will operate the FHM in accordance with designed safeguards and interlocks such that irradiated loads remain suitably submerged so that adequate radiation shielding is provided.
				-	-	Normal Conditions	HF FPM 5-6.2_01	FROs will operate the Fuel Preparation Machine (FPM) in accordance with designed safeguards and interlocks such that irradiated loads remain suitably submerged so that adequate radiation shielding is provided.
				-	-	Normal Conditions	HF RBC 5-6.2_01	RBC Operator will operate the RBC in accordance with designed safeguards and interlocks such that irradiated loads remain suitably submerged so that adequate radiation shielding is provided.
		5-7	Functions to limit the effect of hazard	-	-	-	-	-
		5-8	Functions to clean up reactor coolant	-	-	-	-	-
		5-9	Functions to clean up water except for reactor coolant	-	-	Normal Conditions	HF LWMS 5-9.1_01	Manual actions required to ensure that the LCW and HCW systems treated effluent meet the re-use criteria specified in the Water Quality Specification will be conducted safely and effectively.
		5-10	Functions to supply electric power (except for emergency supply)	-	-	-	HF MSASTBP 5-10.1_01	CRO performs necessary actions from the MCC to enable the power conversion system (PCS) to provide core cooling and heat removal.
				-	-	-	HF MSASTBP 5-10.1_02	CRO re-opens the MSIVs from the MCC to enable the power conversion system (PCS) to provide decay heat removal.
				-	-	-	HF MSASTBP 5-10.1_03	CRO (with FO) using local control and from the MCC restart power conversion system (PCS) Safety Class 3 SSCs and then reopen MSIVs to enable the PCS to provide decay heat removal.
		5-11	Supporting functions to supply power (except for emergency supply)	-	-	-	-	-
		5-12	Functions for plant instrumentation and control (except for safety protection function)	-	-	-	-	-
		5-13	Auxiliary functions for plant operation	-	-	-	HF IA 5-13.1_01 HF IA 5-13.2_01 HF IA 5-13.3_01	CRO recognises loss of instrument air (IA) and CRO/FO recover the IA function or (if at power) CRO manually shuts down the reactor before reactor automatic SCRAM on HCU low pressure.

Fundamental Safety Function (FSF) (from PCSR Chapter 5, Table 5.6-1)		High Level Safety Function (HLSF) (from PCSR Chapter 5, Table 5.6-1)		Fault Schedule (Bounding Fault) (from Table 4-2.1 and its Attachment 1, in Topic Report on Fault Assessment [Ref-32])		Human-Based Safety Claims (Functional Claims)		
		No	**Description**	**Fault Group**	**Front System**	**State**	**Claim ID**	**Claim Contents**
5	Others (continued)	5-14	Functions important to emergency measures and monitoring of abnormal conditions	-	-	-	HF FPS 5-14.4_01*	MCR personnel will extinguish a fire in the MCR.
		5-15	Functions to control hydrogen concentration in accident conditions	-	-	-	-	-
		5-16	Functions to provide radiation shield, canister handling method, fuel retrievability and protection of canister during interim storage period	-	-	-	-	-
				-	-	-	-	-
		5-17	Functions to provide structural support to SSCs	-	-	-	-	-
		5-18	Functions to maintain internal building environment appropriate for SSC	-	-	Fault Conditions	HF HVAC 5-18.2_01	FO opens the door of key electrical panel rooms when the C/B HVAC is lost and the room temperature increases.
				-	-	Fault Conditions	HF HVAC 5-18.2_02 (with HF HVAC 4-7.2_02)	CRO or FO opens the connecting valves between operating deck to main stack to release heat but mitigate against radiological release
				-	-	Fault Conditions	HF HVAC 5-18.4_01	CRO will purge smoke when required during a fire event either in the incipient stage or after the fire is extinguished
		5-19	Functions important to confirmation of abnormal conditions	-	-	-	-	-
		5-20	Function to release heat to the environment	-	-	-	-	-
		5-21	Function to retain water for provision of radiation shield during the refuelling process	-	-	-	-	-
		5-22	Function to limit deceleration loading to canister containment boundary during credible cask drop faults	-	-	-	-	-

Table A-2: Functional HBSCs Supporting Achievement of SSC SPCs

Safety Property Claim (SPC)		Functional HBSCs Supporting Achievement of SPC		
No	**Description**	**State**	**Claim ID**	**Claim Contents**
ME 8	Mechanical SSCs are designed with the capability for being tested, maintained and monitored during power operation and/or refuelling outages in order to ensure the capability to deliver the safety functions claimed without compromising their availability throughout their operational life.	Normal Conditions	HF ATWS ME 8_01	After maintenance activities are completed circuit breakers related to the Anticipated Transient Without SCRAM (ATWS) system will be restored to their correct position to ensure system availability
		Normal Conditions	HF EDG ME 8_01	After maintenance activities are completed, manual valves related to the Emergency Diesel Generator (EDG) system will be restored to their correct alignment
		Normal Conditions	HF FLSS ME 8_01	After maintenance activities are completed, manual valves related to the Flooding System of Specific Safety (FLSS) system will be restored to their correct alignment
		Normal Conditions	HF FPC ME 8_01	Maintenance personnel will correctly calibrate pressure level transmitters related to the Fuel Pool Cooling and Cleanup (FPC) system.
		Normal Conditions	HF FPC ME 8_02	Maintenance personnel will correctly calibrate water level transmitters related to the Fuel Pool Cooling and Cleanup (FPC) system.
		Normal Conditions	HF FPC ME 8_03	Maintenance personnel will correctly calibrate flow transmitters related to the Fuel Pool Cooling and Cleanup (FPC) system.
		Normal Conditions	HF FPC ME 8_04	After maintenance activities are completed, manual valves related to the Fuel Pool Cooling and Cleanup (FPC) system will be restored to their correct alignment.
		Normal Conditions	HF FPS ME 8_01	After maintenance activities are completed, manual valves related to the Fire Protection System (FPS) will be restored to their correct alignment.
		Normal Conditions	HF HECW ME 8_01	Maintenance personnel will correctly calibrate differential pressure transmitters related to the HVAC Emergency Cooling Water (HECW) system.
		Normal Conditions	HF HECW ME 8_02	Maintenance personnel will correctly calibrate temperature transmitters related to the HVAC Emergency Cooling Water (HECW) system.
		Normal Conditions	HF HECW ME 8_03	After maintenance activities are completed, manual valves related to the HVAC Emergency Cooling Water (HECW) system will be restored to their correct alignment.
		Normal Conditions	HF HPCF ME 8_01	After maintenance activities are completed, manual valves related to the High Pressure Core Flooder (HPCF) system will be restored to their correct alignment.
		Normal Conditions	HF MS ME 8_01	Maintenance personnel will correctly calibrate pressure transmitters related to the Turbine Main Steam (MS) system.
		Normal Conditions	HF MUWC ME 8_01	After maintenance activities are completed, manual valves related to the Makeup Water Condensate (MUWC) system will be restored to their correct alignment
		Normal Conditions	HF NB ME 8_01	Maintenance personnel will correctly calibrate reactor water level transmitters related to the Nuclear Boiler (NB) system.
		Normal Conditions	HF NB ME 8_02	Maintenance personnel will correctly calibrate pressure level transmitters related to the Nuclear Boiler (NB) system.
		Normal Conditions	HF RCW ME 8_01	After maintenance activities are completed, manual valves related to the Reactor Building Cooling Water (RCW) system will be restored to their correct alignment.
		Normal Conditions	HF RHR ME 8_01	After maintenance activities are completed, manual valves related to the Residual Heat Removal (RHR) system will be restored to their correct alignment.
		Normal Conditions	HF RHR ME 8_02	Motor Operated Valve F005A will be correctly reassembled and de-isolated to ensure Residual Heat Removal (RHR) system availability.

Safety Property Claim (SPC)		Functional HBSCs Supporting Achievement of SPC		
No	**Description**	**State**	**Claim ID**	**Claim Contents**
ME 8 (continued)	Mechanical SSCs are designed with the capability for being tested, maintained and monitored during power operation and/or refuelling outages in order to ensure the capability to deliver the safety functions claimed without compromising their availability throughout their operational life. (continued)	Normal Conditions	HF RHR ME 8_03	After maintenance activities are completed, the circuit breaker and switchgear related to motor-operated valve F005A in the Residual Heat Removal (RHR) system will be correctly reassembled and restored to their correct positions to ensure system availability.
		Normal Conditions	HF RSW ME 8_01	After maintenance activities are completed, manual valves related to the Reactor Building Service Water (RSW) system will be restored to their correct alignment.
		Normal Conditions	HF SLC ME 8_01	After maintenance activities are completed manual valves related to the Standby Liquid Control (SLC) system will be restored to their correct alignment to ensure system availability.
		Normal Conditions	HF SPCU ME 8_01	After maintenance activities are completed, manual valves related to the Suppression Pool Cleanup (SPCU) system will be restored to their correct alignment.
SSLC C&I 4.1	The SSLC has adequate redundancy which meets Safety Class 1 good practice.	Normal Conditions	HF SSLC C&I 4.1_01	Maintenance technician replaces a failed SSLC CPU in the SSLC controller room in the MCR.

Appendix B: HF Property Claims and Engineering Reference Documents

B.1: HF Property Claims

The following table gives a summary of the HF property claims identified within GDA. The full detailed HBSC database record in the HBSC Report [Ref-1] captures the arguments and evidence for each HF property claim, demonstrating their links to the NSEDPs [Ref-2]. Note that there are HF property claims which are largely assumption during GDA. These are identified within GDA for completeness (because they will need to be claimed in order for the future licensee to be able to meet the ONR's Licence Conditions), but are only partly substantiated within scope of this PCSR. Where this is the case it is noted in the table below and "greyed out". Compliance with the NSEDPs is discussed in Chapter 5.

Table B-1: List of HF Property Claims

HBSC ID	Claim
HFSPC 1	The UK ABWR plant is designed throughout in accordance with modern standards and good practice in HF to be usable and maintainable such that it supports optimal human performance of tasks and minimises human error traps, particularly for equipment and interfaces relating to tasks important to nuclear safety.
HFSPC 2	The allocation of UK ABWR plant functions between engineered system and human is optimised such that risk from human error is reduced through appropriate levels of automation, with clear indication of plant status at all times and facilitation of manual intervention when required. In addition, operator workload is optimised for each operational mode, including during fault scenarios and accident conditions.
HFSPC 3	The working environment for the UK ABWR plant is designed and maintained, wherever possible, to be optimal for supporting expected human performance of tasks. Where of necessity (due to either system constraints or as a result of fault conditions) the environment is less than optimal for human performance, the system design accommodates both protective equipment requirements and a potential decrease in human performance of related tasks in such degraded areas.
HFSPC 4	Personnel job roles, including supervisory roles, are well-designed to provide a balanced workload of clearly-defined tasks including, and particularly highlighting responsibilities that relate to maintaining nuclear safety.
HFSPC 5	Operations staff complement is adequate, based on the defined job roles, for all essential plant operations and EMIT tasks, in all operating modes.
HFSPC 6	Procedures, manuals, plant operating instructions and job aids are clearly written in accordance with good HF practice, and particularly highlight and support those actions required for nuclear safety.

HBSC ID	Claim
HFSPC 7	Personnel basic competence and job-roles specific training requirements are systematically identified, and training material developed such that it ensures optimal knowledge and skills development.
HFSPC 8	Suitable and sufficient EMIT will be conducted on all nuclear-safety related SSCs, in accordance with the maintenance schedule and level of safety classification, such that the risk of SSC unavailability or failure due to incorrect EMIT or degradation or fault in such SSCs is minimised.
HFSPC 9	Operational tasks in Operating Conditions I and II, in all Operations Modes[8], will be conducted with suitable and sufficient attention and accuracy such that risk of actions that might lead to a latent error which has a potential nuclear safety consequence or contribute to an initiating event that leads to Operating Condition III or IV, is minimised.
HFSPC 10	Monitoring of all plant operations, conditions and processes, both automated and manual, relevant to nuclear safety will be conducted with suitable attention and understanding such that situation awareness of the status of any activity or equipment likely to impact nuclear safety is effectively maintained at all times.

B.2: Key HF Engineering Reference Documents

Topics	References
1. Access and Egress	UK Regulations for buildings (The Building Regulations 2010)
	Workplace Design for Health and Safety (The Workplace (Health, Safety and Welfare) Regulations 1992
	BS EN 614-1:2006+A1:2009 Safety of Machinery – Ergonomic Design Principles – Terminology and Principles
	BS EN 547-1:1996+A1:2008 Safety of Machinery – Human Body Measurements – Principles for Determining the Dimensions Required for Openings for Whole Body Access into Machinery
	BS EN 547-2:1996+A1:2008 Safety of Machinery – Human Body Measurements – Principles for Determining the Dimensions Required for Access Openings
	BS 5395-1 to -3 Stairs - Code of practice for the design of stairs
	BS 4592-0:2006 +A1:2012 Flooring, stair treads and handrails for industrial use. Common design requirements and recommendations for installation
	BS EN ISO 14122-1 to -3 Safety of machinery - Permanent means of access

[8] See PCSR Chapter 5, Section 5.4 for description of Operating Conditions and Operating Modes.

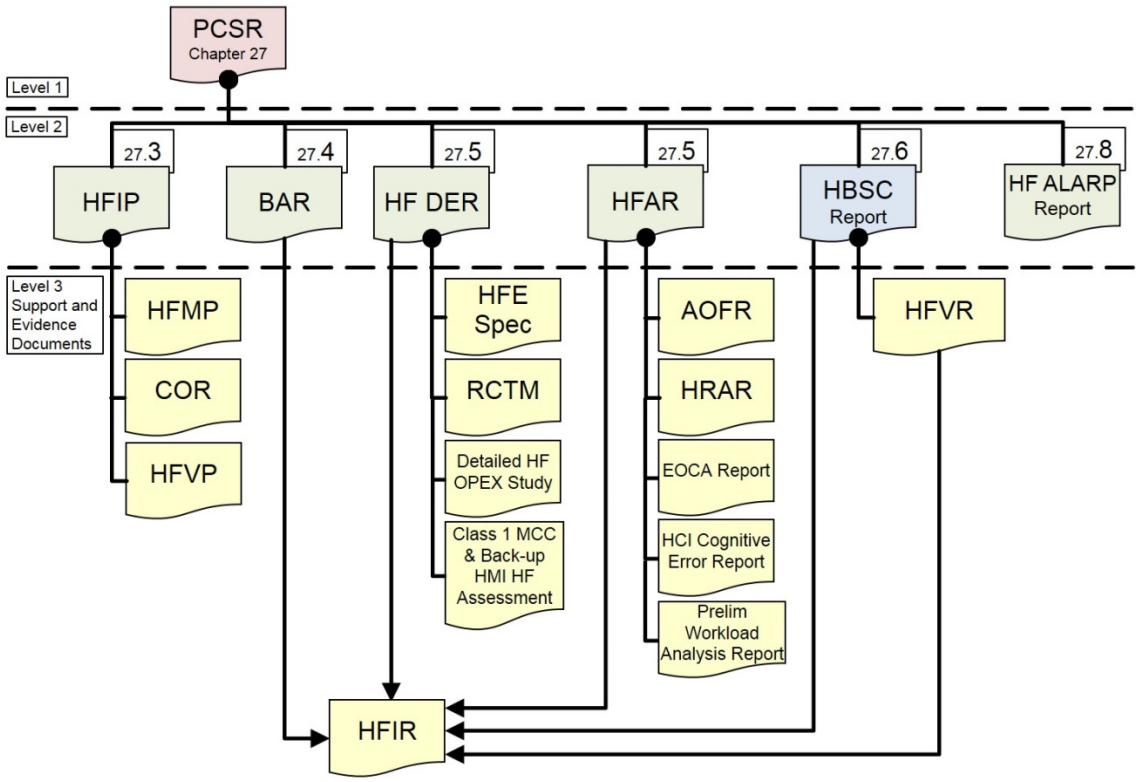
Topics	References
	to machinery
	HSE Work at Height Regulations 2005
	BS EN 349:1993+A1:2008 Safety of Machinery – Minimum Gaps to Avoid Crushing of Parts of the Human Body
2. Work Postures and Positions	NUREG-0700, Revision 2 Human-System Interface Design Review Guidelines
	The Confined Space Regulations 1997
	BS EN ISO 13857:2008 Safety of Machinery – Safety Distances to Prevent Hazard Zones Being Reached by Upper and Lower Limbs
3. Equipment Layout for Operability and Maintenance	US Department of Energy (DOE) DOE-HDBK-1140-2001 Human Factors/Ergonomics Handbook for the Design for Ease of Maintenance. (2001)
	HSE Provision and Use of Work Equipment Regulations 1998
	BS EN ISO 12100:2010 Safety of Machinery – General Principles for Design – Risk Assessment and Risk Reduction
	BS EN ISO 14119:2013 Safety of Machinery – Interlocking Devices Associated with Guards – Principles for Design and Selection
	American Bureau of Shipping Ergonomic Notations 2013
	BS EN 547-3:1996+A1:2008 Safety of Machinery – Human Body Measurements – Principles for Determining the Dimensions Required for Access Openings
	UK MoD DEF STAN 00-250 Human Factors for Designers of Systems Part 3: Technical Guidance. (2008)
	BS EN 13732-1 & -2 Ergonomics of the Thermal Environment – Methods for the Assessment of Human Responses to Contact with Surfaces
	UK Control of Noise at Work Regulations 2005
	BS EN ISO 15667:2000 Acoustics – Guidelines for Noise Control by Enclosures and Cabins
4. Electrical, Control & Instrumentation (EC&I) Equipment Installation	BS EN 60204-1:2006+A1:2009 Safety of Machinery – Electrical Equipment of Machines – General Requirements
5. Main Control Room and Supplementary Control Points	BS EN 60964:2010 Nuclear Power Plants – Control Rooms – Design
	BS EN ISO 11064-3 to -6 Ergonomic Design of Control Centres
	IAEA Safety Standards Series NS-G-1.3 Instrumentation and Control

Topics	References
	Systems Important to Safety in Nuclear Power Plants
	BS EN 60965:2011 Nuclear Power Plants – Control Rooms – Supplementary Control Points for Reactor Shutdown Without Access to the Main Control Room
	BS EN ISO 9241-5:1999 Ergonomic Requirements for Office Work with Visual Display Terminals – Workstation Layout and Postural Requirements
	BS EN 61772:2013 Nuclear Power Plants – Control Rooms – Application of Visual Display Units
	BS IEC 61227:2008 Nuclear Power Plants – Control Rooms – Operator Controls
6. Displays and Controls (Non-Control Room)	BS EN ISO 9241-303:2011 Ergonomics of Human-System Interaction – Requirements for Electronic Visual Displays
	BS EN 894-2 to -4 Safety of Machinery – Ergonomics Requirements for the Design of Displays and Control Actuators
	BS EN 1005-3:2002 Safety of Machinery – Human Physical Performance – Recommended Force Limits for Machinery Operation
	BS EN ISO 13850:2008 Safety of Machinery – Emergency Stop – Principles for Design
7. Alarms	EEMUA Publication 191 Alarm systems - a guide to design, management and procurement
	BS EN 61226:2010 Nuclear power plants. Instrumentation and control important to safety. Classification of instrumentation and control functions
	BS IEC 62241:2004 Nuclear power plants. Main control room. Alarm functions and presentation
8. Digital System Design	BS EN ISO 9241-12 to -16 Ergonomic Requirements for Office Work with Visual Display Terminals
	BS 8888:2013 Technical Product and Documentation Specification
	US. Government Printing Office Style Manual: An Official Guide to the Form and Style of Federal Government Printing, 2008
	BS EN ISO 9241-400:2007 Ergonomics of Human-System Interaction – Principles and Requirements for Physical Input Devices
	BS EN ISO 14915-1 to -3 Software Ergonomics for Multimedia User Interfaces
	BS ISO 14617-1 to -12 Graphical Symbols for Diagrams
9. Materials Handling	HSE Manual Handling Assessment Charts

Topics	References
	BS EN 13135:2013 Cranes – Safety – Design – Requirements for Equipment
	NS-TAST-GD-056 (Rev 3) Nuclear Lifting Operations
	HSE Lifting Operations and Lifting Equipment Regulations 1998 (LOLER)
	BS EN 12077-2:1998+A1:2008 Cranes Safety – Requirements for Health and Safety – Part 2: Limiting and Indicating Devices
	BS EN 15011:2011+A1:2014 Cranes – Bridge and Gantry Cranes
	BS EN 13557:2003+A2:2008 Cranes – Controls and Control Stations
	ISO 7752-1 to -3 Cranes – Control Layout and Characteristics
	BS EN 60204-32:2008 Safety of Machinery – Electrical Equipment of Machines – Requirements of Hoisting Machines
	BS EN 14238:2004+A1:2009 Cranes – Manually Controlled Load Manipulating Devices
10. Labelling and Signage	HSE The Health and Safety (Safety Signs and Signals) Regulations, 2nd Ed. 2009
11. Working Environment	HSE Control of Noise at Work Regulations 2005
	BS EN 12464-2:2014 Light and Lighting – Lighting of Work Places – Outdoor Work Places
	BS 5266-1:2011 Emergency Lighting – Code of Practice for the Emergency Escape Lighting of Premises
	BS EN 50172:2004 Emergency Escape Lighting Systems
	HSE Control of Vibration at Work Regulations 2005
	HSE The Control of Substances Hazardous to Health Regulations 2002
	HSE REACH and Safety Data Sheets
	HSE Chemicals (Hazard Information and Packaging for Supply) Regulations 2009

Appendix C: Document Map

The document map for the this chapter is shown below. The contribution of the documents to the substantiation of the HBSCs and justification of ALARP is described in Section 27.1.2. Following the document map is a short description of the purpose and content of each document.



PCSR:	Generic Pre-Construction Safety Report
HFIP:	Human Factors Integration Plan
HFMP:	Human Factors Methodology Plan
COR:	(HF) Concept of Operations Report
HFVP:	Human Factors V&V Plan
BAR:	Baseline Human Factors Assessment Report
HFIR:	Human Factors Issues Register (Report)
DER:	Human Factors Design and Engineering Report

HFE Spec:	Human Factors Engineering Specification
RCTM:	(HF) Requirements Compliance Tracking Matrix
HFAR:	Human Factors Assessment Report
AOFR:	Allocation of Function Report
HRAR:	Human Reliability Analysis Report
EOCA:	Errors of Commission Analysis (Report)
HBSC:	Human-Based Safety Claims (Report)
HFVR:	Human Factors V&V Report

Figure C-1: HF Topic Area Document Map

In addition to the Level 1 and Level 2 documents in the document map, as indicated and as described in the HFIP [Ref-6], each of the HFI Work Packages identified within the UK ABWR HFI programme has key outputs or deliverables that capture the activities and analysis undertaken throughout GDA. These act as sources of supporting evidence to this chapter of the PCSR, as shown in the map. These are also described below.

Human Factors Integration Plan (HFIP)

As described in above, the HFIP [Ref-6] outlines the UK ABWR HFI Programme plan including: scope of the programme, HF resource and organisation for GDA, management of HF activities and issues, scope and details of the HF activities (Work Packages), deliverables and schedule.

Human Factors Methodology Plan (HFMP)

As described in Section 27.3.3, the HFMP [Ref-7] details the processes, methods and tools to be used for GDA HF analysis and other activities (i.e. design support).

Human Factors Concept of Operations Report (COR)

In order to make appropriate decisions regarding the scope and nature of HF activities to be undertaken in the HFI programme, the operational context was defined to a level of detail appropriate to the project phase. This was done in consultation with suitable UK-experienced operational and organisational representatives and is captured in the COR [Ref-21]. The COR describes the assumed plant design, work environment, operational arrangements, and cognitive and physical capabilities of the system users. In addition, for defining the basis of the HFI programme, the information in the COR is used to underpin all relevant GDA HF analyses.

Baseline Human Factors Assessment Report (BAR)

At the start of GDA, Hitachi-GE already had a baseline design that incorporated elements of good HF engineering practice as an inherent part of the design process and that was improved continuously through its design life through the use of customer operational experience. In addition, the reference plant has an existing safety case. The first activities in the GDA HFI programme were to assess the current extent and effectiveness of implementation of HF in design, identifying gaps, in the context of the UK regulatory requirements, requiring further attention during GDA. The methodology, information collected, findings and conclusions from this review are captured in the Baseline HF Assessment Report (BAR) [Ref-5], which details the initial HF assessment of the baseline “reference” plant design (J-ABWR) and the existing HFE processes at Hitachi-GE.

Human Factors Issues and Assumptions Register (HFIR)

The HFIR [Ref-13] is a “live” document used for tracking and management of any identified issues related to HF, the recommended resolution of those issues, and justification of residual risk if any. The HFIR also contains the UK ABWR GDA HF Assumptions Register. The HF Assumptions Register is used as part of the clear and traceable handover from the Requesting Party to the future licensee in the forward stages of the HFI programme (i.e. post-GDA), forming part of the formal handover arrangements planned for the end of GDA. This will be used to ensure that the basis for the HF analyses and support provided during GDA can be understood and further validated as necessary in future stages of the plant lifecycle.

Human Factors Design and Engineering Report (DER)

The HF DER [Ref-8] describes the HF activities and analysis carried out in support of the design of UK ABWR; it includes HF analysis carried out in support of design decisions for elements of design

not related to specific safety case claims (as compared to that specifically in support of safety analysis (see HFAR below)). It also provides some of the evidence and substantiation for the HBSCs, particularly high-level design claims that support achievement of HF property claims.

Human Factors Engineering Specification (HFE Spec)

The HFE Spec [Ref-9] compiles the list of design-based HF requirements that derive from the UK HF standards and guidelines into one specification, for use by Hitachi-GE engineers, designers and their suppliers.

Human Factors Requirements Compliance Tracking Matrix (RCTM)

The RCTM [Ref-12] is a register of all the HF requirements (both HF in design and HF process requirements) for UK ABWR GDA and provides a clear audit trail as to how they are complied with.

Human Factors Assessment Report (HFAR)

The HFAR [Ref-10] largely summarises the HRAR (see below) but also captures the output from any other safety-related HF analysis such as AoF analysis, workload analysis, etc. Along with the HRAR, it provides most of the detailed evidence and substantiation for the HBSCs.

Allocation of Function Report (AOFR)

The AOFR [Ref-27] is a report of the outcome of the iterative AoF analyses carried out on existing (J-ABWR) and new (UK ABWR) design.

Human Reliability Analysis Report (HRAR)

The HRAR [Ref-11] presents the detailed qualitative and quantitative error analysis of all significant human failure events, which then form some of the functional HBSCs for UK ABWR. It also includes results from any error identification activities and human failure event screening, grouping, and bounding analysis.

Human-Based Safety Claims (HBSC) Report

The HBSC Report [Ref-1] presents a clear summary of the CAE for all HBSCs identified in the UK ABWR during GDA. It forms the BSC for the HF topic area and refers out to many system BSCs, topic reports and supporting reports that support understanding of the context and provide evidence for substantiation of the claims.

Human Factors V&V Plan (HFVP)

The HFVP [Ref-14] defines the scope and activities of V&V work related to HF that will be undertaken in GDA. This HFVP outlines the basic strategy and general process of GDA HF V&V as an overarching plan for the entire V&V programme; it provides a high-level indication of the nature and timing of activities to be undertaken, with a suitable level of justification for each activity as required. More specific plans and detailed descriptions of each of the V&V activities are described in other more detailed planning and procedure documents as appropriate.

Human Factors V&V Report(s) (HFVR(s))

The HFVR [Ref-15] presents a summary of plans, procedures, and results of each of the HF V&V activities undertaken for the design area as described in Section 27.5.4. Those HF V&V activities were planned and executed, taking into account of UK ABWR design maturity achieved in GDA. The details are recorded in individual reports that are referred out from the HFVR.

Human Factors ALARP Report

The HF ALARP Report [Ref-4] presents details of the ALARP position and the justification for the HF topic area, gathering all the substantiation and justification from underpinning reports and activities, plus provides a summary of the residual risks and known assumptions that are passed onto the site-specific stage.