Form10/00

HITACHI

UK ABWR

Document ID	:	GA91-9101-0101-21000
Document Number	:	3E-GD-A0060
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 21 : Human-Machine Interface

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

Table of Contents

Executive Summary

This chapter describes the safety case for the Human-Machine Interface HMI) systems for UK ABWR through which personnel interact with and control to the plant and processes.. It lists the Safety Functional Claims (SFCs) that are made on these HMIs, together with the Safety Property Claims (SPCs) that demonstrate compliance of these HMI systems with relevant Design Principles, as explained in PCSR Chapter 5. The information presented in this chapter demonstrates how the HMIs contribute to achieving the safety claims made on the related Control and Instrumentation (C&I) and mechanical systems that they monitor or control. The chapter also demonstrates how the HMIs support the actions performed on them that comprise the relevant Human-Based Safety Claims (HBSCs) within the safety case.

The information provided includes: system design including interfaces with C&I systems; consideration of Human Factors (HF) in design to optimise human performance when using HMIs; functionality in normal conditions and during fault conditions; safety categorisation and classification; important support systems; resistance to hazards; and summary of compliance with the principles of reducing risks “as low as reasonably practicable” (ALARP) and links to safety case Assumptions; Limits and Conditions for Operations.

The overall PCSR justification that the UK ABWR is safe and satisfies the principles of risk reduced ALARP is underpinned by hazards assessments, safety and HF analysis which demonstrate that the design of the HMI systems covered by this chapter are fault tolerant and optimised for human interactions.

The safety analysis and assessment described in PCSR Chapter 24:Design Basis Analysis, Chapter 25: Probabilistic Safety Assessment, Chapter 26: Beyond Design Basis and Severe Accident Analysis, and Chapter 27:HF), specify the SFCs and related HBSCs required to deliver safety function. In order to substantiate these claims for GDA the safety analysis has applied the conditions and assumptions consistent with the HMIs current design maturity, system information and safety claims.

ALARP assessments have led to risk-reduction measures to C&I systems for GDA, as described in PCSR Chapter 14:C&I. This has included the introduction of new diverse C&I systems with their own associated HMI systems. Further details of specific issues that have been considered for these new HMI systems and to align the HMIs with modern HF good practice are described in this chapter.

This chapter demonstrates that the risks associated with the design and the operation of the HMI systems for the UK ABWR are ALARP. Further work will be required post-GDA to develop the design and fully incorporate site-specific aspects and operating arrangements. This work will be the responsibility of a future licensee.

21.1 Introduction

This chapter provides an overview of the safety justification for the Human-Machine Interfaces (HMIs) on the plant for UK ABWR. It provides a high level description of the overall structure of the HMIs to demonstrate defence in depth for the safety case of them. Appendix C supports the demonstration by showing the links to a set of Level 2 documents which detail the arguments and evidence that make up the safety justification for this chapter.

21.1.1 Background

The HMIs are the main interfaces between users and the plant systems, structures and components (SSCs), through Control and Instrumentation (C&I) systems. The HMI is the principal mechanism through which personnel interact with the SSCs in order to monitor and control plant processes. The HMIs provide information and facilities for monitoring and actuation of SSCs in the form of displays, indicators, alarms and controls. The HMIs support the delivery of functions required for plant operation to deliver safety functions through user undertaking monitoring, decision-making, action and confirmation tasks. This chapter presents the key information for HMIs in the Main Control Room (MCR), other dedicated control centres, and for some locally controlled mechanical engineering systems with embedded C&I.

An overview of the control location where the key HMIs are installed is described below:

Main Control Room (MCR): The MCR is the place where plant operations related to aspects of the main nuclear power generation process and related to aspects of nuclear safety are conducted. The main HMIs installed in the MCR are: the Main Control Console (MCC); the Wide Display Panel (WDP); the Safety Auxiliary Panel (SAuxP); and the Hardwired Backup Panel (HWBP).

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

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

Radioactive Waste Building (Rw/B) Main Control Room (MCR): The C&I and HMIs related to processing of Radioactive Waste (Radwaste) management are required to perform the functions related to nuclear and environmental safety. The HMIs in the Rw/B MCR are used to monitor and control the C&I systems and plant associated with the management of Liquid Waste and some parts

of the Solid Waste management process. Some information and alarms associated with them are replicated through the HMIs in the MCR.

Local Control Locations: There are a number of Mechanical and Electrical Engineering systems and equipment in the UK ABWR design that perform nuclear safety functions but which have embedded C&I controlled through local HMIs, i.e., systems not controlled from the MCR through the main C&I (PCSR Chapter 14:C&I). These systems with local HMIs include:

- Chapter 15:Electrical Power Supplies- Electrical Power Supplies, Communications and Lighting Systems,
- Chapter 16:Auxiliary Systems- Heating Ventilation and Air Conditioning System (HVAC) and Diesel Generators,
- Chapter 18:Radioactive Waste Management- parts of the Solid Waste Management System (SWMS) in the Solid Waste Facility (SWF) Building, Intermediate Level Waste and High Level Waste (ILW & HLW) Stores, and
- Chapter 19:Fuel Storage and Handling- Fuel Route equipment such as the Fuel Handling and Fuel Preparation Machines (FHM & FPM) and Reactor Building Crane (RBC).

21.1.2 Document Structure

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

(1) Chapter 21 Overview

This chapter includes the following sections:

Section 21.2 Purpose and Scope: 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 are explained.

Section 21.3 Requirements and Claims for HMIs: The requirements for HMIs within UK ABWR are presented, and the structure of the Safety Functional Claims (SFCs) and Safety Property Claims (SPCs) for this topic area are described. This includes the particular relevance of two of the Human Factors 'property claims' from PCSR Chapter 27:HF, and explains how the claims substantiate that the two key risks identified in section 21.10 have been reduced to levels that are As Low as Reasonably Practicable (ALARP).

Section 21.4 through 21.8: These sections describe the HMIs to deliver High Level Safety Functions (HLSFs) and the Human-Based Safety Claims (HBSCs) in the key control rooms or areas and summarise the justification provided for each. The detailed claims, arguments and evidence for each HMI are given in the referenced BSC for each of these sections.

Section 21.9 Assumptions, Limits and Conditions for Operation: The main assumptions relevant to design and the usage of the HMIs are summarised, and the link to relevant Limits and Conditions for Operation (LCOs) in the corresponding section in PCSR Chapter 14:C&I is explained.

Section 21.10 Summary of ALARP Justification: This section identifies the key risks associated with design and the usage of the HMIs, and provides a summary of the ALARP justification for HMIs that is made throughout the support document such as the BSCs shown in Appendix C and other documents, as applicable.

Section 21.11 Conclusions: This section provides a summary of the main aspects of this chapter.

Section 21.12 References: This section lists documents referenced within this chapter.

Appendix A Safety Functional Claims: Comprehensive table of the SFCs is provided.

Appendix A1 Safety Functional Claim Table: The list of SFC for the HMIs in this chapter with the linkage of Fundamental Safety Function (FSF), HLSF, and relevant Front System (FS) is shown in Appendix A1.

Appendix A2 Front System and Initiating Fault/Event ID Linkage Table: The fault schedule related to each FS is identified.

Appendix B Safety Property Claims Table: The nine SPCs which are derived from C&I and define the design requirements applicable to the HMIs are identified. There are also two SPCs which are derived from Human Factors (HFs) to define the requirements in the aspect of HFs applicable to the HMI design. The tables of SPCs, shown in Appendix B, were derived for the topic covered in this chapter based on the 'guide word' approach specified in Hitachi-GE's Safety Case Development Manual (SCDM) [Ref-13], but are specific to the C&I topic area. Having derived the SPCs, a mapping exercise was undertaken to ensure that the SPCs fully cover the relevant Nuclear Safety and Environmental Design Principles (NSEDPs) applicable to the topic area. More information on the development of SPCs, and the coverage, at the more detailed level in the safety case, to demonstrate full compliance with the relevant NSEDPs is presented in Chapter 5.3.

Appendix C Document Map: The document map showing the Level 1 and Level 2 document structure for this chapter is provided.

(2) Chapter 21 Supporting Documents

The document structure for this chapter is simple in that it consists of the summary safety justification provided within this Level 1 document, supported by multiple Level 2 BSCs for each of the groups of HMIs summarised in Sections 21.4 through 21.8, as well as an overview BSC for the HMI. The list of supporting BSCs is as follows:

- Basis of Safety Cases on Overall Human-Machine Interface [Ref-1] ,
- Basis of Safety Cases on Main Control Room Human-Machine Interface [Ref-2],
- Basis of Safety Cases on Remote Shutdown System Human-Machine Interface [Ref-3], and
- Basis of Safety Cases on Backup Building Human-Machine Interface [Ref-4].

These BSCs provide the detailed arguments and evidence to substantiate the claims listed in Appendices A and B within this chapter. The BSCs are themselves supported by a variety of suitable Level 3 engineering documents and other supporting reports. Key Level 3 documents are also referenced in this chapter where appropriate.

(3) Links to Other Chapters and Documents

This chapter also provides links to other key chapters within the safety case presented in the PCSR that form part of or link to the safety case for the HMI topic area. The most significant links are to:

- PCSR 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 5.6. 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 5.7 to 5.9,
- PCSR Chapter 14:C&I - This presents the safety case for the C&I systems which the majority of HMIs within scope of this chapter interface to in order to control and feedback from the plant systems. The nine SPCs for the HMIs are derived from the list shown in Appendix B. The following C&I systems are described in PCSR Chapter 14:C&I and are the key systems that link to this chapter:
    - Safety System Logic and Control System (SSLC)
    - Plant Control System (PCntlS)
    - Reactor/Turbine Auxiliary Control System (ACS)
    - Plant Computer System (PCS)
    - Safety Auxiliary Control System (SACS)
    - Hardwired Backup System (HWBS)
    - Severe Accident C&I (SA C&I)
- PCSR Chapter 27:HF - which presents the safety case for the HF design and analysis topic area, particularly describing the human actions claimed throughout the safety case as being necessary to maintain plant safety. The actions to achieve the HBSCs are mainly performed on the HMIs within the scope of this chapter, so these two chapters are directly linked,

    Specific locations of the HMIs distributed throughout the plant are described at a level of detail appropriate to the maturity of the associated SSC or C&I design in GDA. Where the detailed assessment and safety substantiation of HBSCs (considered within scope of PCSR Chapter 27) uses a particular HMI then, where GDA design maturity allows, more detailed information on location within buildings are given (or assumed) within supporting documentation. Such information might be needed, for example, to enable understanding of travel times or security arrangements that might impact task performance.,
- PCSR Chapter 30:Operations - which presents the preliminary requirements and assumptions for operational arrangements that support the Generic PCSR in achieving its safety claims. Specifically the usage of the HMIs to achieve the required human actions is summarised to ensure a cohesive set of operational expectations is clearly laid out for future licensee,

- General requirements related to conventional safety aspects are described in PCSR Chapter 4:Safety Management throughout Plant Lifecycle, in particular Section 4.6.8,
- For generic links to the Generic Environmental Permit (GEP) and Conceptual Security Arrangements (CSA) documentation, please refer to Generic PCSR Chapter 1:Introduction, and
- Detailed design descriptions of the HMIs are not included within this chapter. Examples include the functional specifications and concept layout of elements such as displays and panels on the MCC which are shown in lower level documents such as Topic Reports or other supporting documents.

The Appendix C shows the links to them. It includes additional links which are indirectly provided through PCSR Chapters 14 and 27 to the fault analysis Chapters 24:Design Basis Analysis, 25:Probabilistic Safety Assessment and 26:Beyond Design Basis and Severe Accident Analysis, since the required reliability levels for the SSCs of the C&I systems are identified within, and the majority of HBSCs derive from those chapters.

There are systems that are not part of the scope of PCSR Chapter 14:C&I systems that nonetheless have HMIs that form part of the scope of this chapter, so there are further links to the following PCSR Chapters:

- Chapter 15:Electrical Power Supplies - The placement of HMIs within the control rooms have been developed taking into account the use of communications equipment and facilities. This includes a variety of systems, including for example, telephones, public address systems, emergency voice communication systems, radios, and video conferencing facilities. The operator communications systems and facilities that are used for the achievement of the HBSCs on the HMIs are important supporting systems, however these are not included within this chapter. The system descriptions of the communications systems are presented in PCSR Chapter 15:Electrical Power Supplies, specifically Section 15.4,
- Chapter 16:Auxiliary Systems - specifically Section 16.3 Water Systems which contains details of HVAC Emergency Cooling Water System (HECW) functions and Reactor Building Service Water System (RSW), which have claims against them for Local HMI usage,
- Chapter 18:Radioactive Waste Management – specifically Section 18.3 which contains the list of claims and associated supporting documents for the Liquid Waste Management System (LWMS) and parts of the SWMS that are supported by the HMIs in the Rw/B MCR. Other local HMIs include those for SWMS conducted from the SWF Building and in the ILW and HLW stores.

  The specific C&I, including HMI, for Radwaste facilities will be entirely integral to those systems in the post-GDA stage and the design and safety case for those systems, particularly related to their functionality, falls within the scope of the PCSR Chapter 18:Radioactive Waste. Although SFCs for Radwaste facilities are substantiated within PCSR Chapter 18 and its supporting documents, the general design principles for the HMIs in the control rooms of the Rw facilities are described within this chapter,

- Chapter 19:Fuel Storage and Handling - specifically its supporting BSC on Fuel Handling Systems and Overhead Crane Systems which provides details of the functions of the FHM and Reactor Building Crane (RBC), which have a remote control room and local HMIs.

21.2 Purpose and Scope

21.2.1 Purpose

The purpose of this chapter is to describe the system interfaces through which the human interacts with the plant and processes of the UK ABWR that are relevant to nuclear safety. The overall goal is to demonstrate that the design of the HMIs supports the required functionality and ensures the risk of human error is ALARP when performing human actions claimed as part of this Generic PCSR.

This chapter has the following specific objectives:

- Describe the HMIs which are used to achieve the human actions relevant to nuclear safety claims made in the GDA PCSR. Explain and define the level of design maturity for these HMIs in GDA.
- Describe the HMIs used in power operation, start-up, hot shutdown and cold shutdown, refuelling outages and in fault conditions.
- Identify all sources of HMI safety requirements, including reliability requirements, usability requirements, and requirements from relevant codes and standards.
- Identify the safety functions and specify the safety classifications of the HMIs that are within the scope of this chapter.
- Specify the relevant SFCs made on the systems that the HMIs are a part.
- Demonstrate how the SPCs that apply generally to C&I systems, are applied specifically to the HMIs, and provide reference to any HF-related "property" claims that apply to HMIs. Explain how these demonstrate that the key risks associated with use of HMIs have been reduced to levels that are ALARP, to the extent possible within GDA for the level of design maturity of the HMIs.
- Identify links to other chapters of the GDA PCSR to ensure consistency across the whole safety case, and to ensure the overall safety case presented is complete.
- Describe where the arguments and evidence that substantiate all relevant safety case claims for HMIs are presented in supporting documents.
- Provide or identify references to evidence required to demonstrate that the risks associated with use of the HMIs are ALARP, to the extent possible for HMI design maturity within the generic design stage.

Note that the HF-related design support and analysis activities that ensure the HMI designs will support effective human task performance in the UK ABWR plant are captured within PCSR Chapter 27, not this chapter (see Section 21.2.2:Scope for more detail).

21.2.2 Scope

There are a large number and wide variety of interfaces in the UK ABWR that allow users to interact with and control the plant and processes, both through direct interaction at equipment level and mostly through C&I systems. The scope of this chapter is only those HMIs through which personnel

interact with and control to the plant and the process related to nuclear safety, including use of HMIs to perform actions claimed as HBSCs.

Generally the scope of this chapter covers multi-function HMIs that include hardware in the form of indicators and controls. The HMIs support the monitoring or delivery of safety functions through the system user undertaking observation, analysis, decision-making, action and confirmation tasks.

This chapter includes HMIs distributed throughout the plant. The scope includes HMIs in the MCR, as well as at supplemental control locations (RSSR and the BBCR) that provide backup or alternative control locations should the MCR and RSSR need to be evacuated and/or relevant nuclear safety control functionality is lost. It also includes local HMIs at various control locations where human actions related to nuclear safety are performed using systems with embedded C&I, such as those in the Fuel Route (FHM, FPM, RBC) and for the management and storage of Radioactive Waste outside of the Rw/B MCR.

The placement of HMIs within the control rooms have been developed taking into account the use of communications equipment and facilities. This includes a variety of systems, including for example, telephones, public address systems, emergency voice communication systems, radios, and video conferencing facilities. The operator communications systems and facilities that are used for the achievement of the HBSCs on the HMIs are important supporting systems, however these are not included within this chapter. The system descriptions of the communications systems are presented in PCSR Chapter 15:Electrical Power Supplies.

The scope of UK ABWR HMI design maturity within the GDA stage is shown in Table 21.2-1.

Table 21.2-1: UK ABWR HMI design maturity within scope of GDA

Location	**MCR (in Control Building)**					**RSSRs (in R/B)**	**BBCR (in B/B)**	**Rw/B MCR (in Rw/B)**	**Local[*4]**
Panel	**MCC or WDP & MCC**			**HWBP**	**SAuxP**	**RSPs**	**BBCPs**		
C&I	SSLC SACS	PCntlS ACS	PCS	HWBS	Part of SSLC	Part of SSLC	SA C&I	Others	Others
Cat./Class	A1 B2/C3	Class3	Class3	A2	A1	A1	B2/B3	C3	A1 C3
Design basis	I	I	I	I	I	I	I	I	I
Functional Design[*1]	II	II	II	II	II	II	II	II	II
Functional specifications[*2]	III	IV[*5]	IV[*5]	III	III	III	III	III	IV
Concept layout[*3]	III	III	III	III	III	III	III	III	IV
Detailed design	IV	IV	IV	IV	IV	IV	IV	IV	IV

Table 21.2-1 Notes:

*1: C&I system and SSCs assigned to each HMI are identified for this step.

*2: Specific switches and indicators with technology for implementing them are decided in consideration of the constraints and requirements derived from the design of the associated plant and C&I systems, and HF basic principles.

*3: Area where the systems are assigned within the panel is shown as part of the Concept Layout for basic design.

*4: Claims for local HMIs are shown in Table 21.8-1 and Appendix A1.

*5: For PCntlS, ACS and PCS, a preliminary functional analysis has allowed for selection of general types of switch and indicator, and also those needed to support HBSCs have been identified during GDA. This allows for creation of the concept layout.

Table 21.2-1 Legend:

I: Summary information is shown in this chapter (Level 1 document), and detailed information which underpins the safety case described in the PCSR is provided in lower level documents (BSC, Topic Report (TR) or other support document).

II: Summary information is shown in the relevant HMI BSC; detailed information which underpins the safety case described in the BSC is shown in lower level documents (TRs or support documents).

III: Summary information is shown in a design document such as the System Design Description (SDD), Interlock Block Diagram (IBD), Instrument Electrical Diagram (IED), and/or instrument list which are submitted as TRs or support documents.

IV: Information will be provided post-GDA through design documents for construction and manufacturing.

(Note: Items identified as I to III are described to basic design level within GDA, to the extent appropriate for the type of document they are located within)

Generally speaking, the HMIs as designed for the Japanese ABWR (J-ABWR) reference plant were assumed, unless specifically identified as otherwise below, to be optimised in terms of their ability to support effective and safe operations to the levels of human performance required. The significant differences from HMIs for the J-ABWR are:

- The SACS was embedded in the SSLC for the J-ABWR, but they are separated for the UK ABWR, to comply with the requirements of the C&I SPC on segregation of systems of different Safety Classifications,
- The HWBP/HWBS, SAuxP and the BBCP/SA C&I are newly designed for the UK ABWR, and
- Touchscreen soft switches which are used for the J-ABWR is replaced by on-screen command which are actuated by a hardware-based input device for Class 1 digital HMI.

The development and strength of the safety case for the substantiation of claims that are made upon the cognitive processing and action of human operators described as HBSCs in Chapter 27 using HMIs to monitor, and initiate when required, the nuclear safety functions that are delivered by SSCs whose safety cases are identified in Technical System Chapters through their associated C&I, either main (Chapter 14) or embedded C&I (Auxiliary System Chapters), is dependent upon the design maturity of each element of this inter-related safety thread.

In particular, it is the design maturity of some UK ABWR systems with embedded C&I that is not connected to the main C&I (Chapter 14) which are immature for GDA. Typically this embedded C&I and, by inference, the local HMIs are integral to the supplier of the equipment, such as Emergency Diesel Generators (EDGs), FHM, and Lifting Equipment (e.g. the RBC).

Additionally, the design development of all UK ABWR facility buildings and their installed systems and equipment, and by inference their C&I architecture and associated HMIs, has progressed at different rates. The design maturity of SSCs, C&I and HMIs, which have SFCs and HBSCs placed upon them, will impact upon the level and strength of the arguments and evidence thread that can be produced in GDA to support or substantiate these claims.

In particular, many elements and sub-systems of the Radioactive Waste Management System for processing and storing Liquid, Gaseous and Solid waste streams are at different engineering concept or preliminary design phases (as specified in PCSR Chapter 18, Table 18.2-1). Similarly, compliance with modern, UK standards on nuclear safety C&I separation, redundancy and segregation have resulted in new additional and modified HMIs and control locations for UK ABWR. This means that HMIs for the main C&I system functionality are also at different stages of design maturity, system verification and validation (V&V). This is reflected in the following section on requirements and claims for HMI.

21.3 Requirements and Claims for HMIs

21.3.1 Requirements for HMIs

The requirements for the HMIs have arisen from;

- The HMIs are required to reflect many of the design features associated with the C&I architecture. These are documented in the BSCs on C&I Architecture [Ref-5].
- HMI requirements related to normal or routine plant and process operating requirements have been derived from the plant and process documentation which are generally captured in the relevant SDD documents, from the Allocation of Function (AoF) Report [Ref-6] and from the HF Concept of Operations Report (COR) [Ref-7].
- HMI requirements related to Design Basis Analysis (DBA) or SA have been derived from the Fault Schedule work documented in the TR on Fault Assessment [Ref-8].
- Where HBSCs have been made in the Safety Case, HMIs related to operator action have been identified and are documented in the supporting references that form the evidence reported in the HBSC Report [Ref-9]. These claims are underpinned and substantiated by suitable HF assessment, including human error analysis, as reported in the PCSR Chapter 27:HF, and its supporting documents.
- For the HBSCs where probabilistic claims have been made in the Probabilistic Safety Analysis (PSA) on any safety function involving the operator and the HMI, the Human Error Probability (HEP) of failure of that claimed human action has been derived and is documented in the Human Reliability Analysis (HRA) Report [Ref-10]. The probabilistic requirements for the HMI equipment are derived from and modelled within the PSA as described within Chapter 25:Probabilistic Safety Assessment, and its supporting documents.
- The HMIs are required to meet the requirements arising from good HF engineering practice that account for human cognitive and physical capabilities and limitations. These requirements are documented in the Human Factors Engineering (HFE) Specification [Ref-11], as summarised in Section 21.3.4.

21.3.2 Safety Functional Claims

The FSFs which the HMIs support are identified in the list of category and class in the PCSR Chapter 5.6:General Design Aspects, Categorisation and Classification of SSCs, and described below:

FSF1 - Control of reactivity,

FSF2 - Fuel cooling,

FSF3 - Long term heat removal,

FSF4 - Confinement/Containment of radioactive materials, and

FSF5 – Others.

These are supported by a set of HLSFs that are applied to each C&I system. These HLSFs are listed in Table 5.6-1 of the PCSR Chapter 5.6, and are applied accordingly to each system, including the HMIs.

A short description of the application of HLSFs in the development of the claims, arguments and evidence is provided in the PCSR Chapter 1:Introduction. The list of SFCs in this chapter and the linkage to corresponding HLSFs is shown in Appendix A.

Additionally each HMI is designed to a generic principle:

- The design, development and assessment of all HMIs address the SFCs made for the system that the HMI is part of and any HBSCs associated with the HMI.

Detailed safety case to substantiate SFCs are described in the BSCs on Overall HMI [Ref-1], MCR HMI [Ref-2], Remote Shutdown System (RSS) HMI [Ref-3] and B/B HMI [Ref-4]. These references directly provide the sub-claims and arguments that support the SFCs for the MCR HMI, RSS HMI and B/B HMI in Appendix A, and specify references to other documentation that provides the supporting evidence for those SFCs.

HMIs related to C&I that forms an integral part of SSCs throughout the plant are called "local" HMIs. This includes HMIs for various local Radwaste facilities, which are outside of the Rw/B MCR. The SFCs for these are identified as 'Local HMI' SFCs, which are described in the BSCs for the systems they are part of. Sections 21.7 and 21.8 give further details.

SFCs for HMIs in the Rw/B MCR are identified as 'Rw/B CR' SFCs.

21.3.3 Safety Property Claims

To underpin and achieve the identified SFCs of the HMIs described in Section 21.3.2, the selection and design of HMI physical components is guided by SPCs.

SPCs have been identified for the relevant C&I systems identified in Table 21.2-1 that are linked to the HMIs, based on good engineering practice from standards and guides.

The list of nine C&I SPCs provided in the GDA PCSR Chapter 14:C&I are applied unchanged to all the HMIs in scope of this chapter, since the hardware forming the HMIs is inherently part of the related C&I systems. To maintain continuity, the C&I prefix is not changed for these claims at PCSR chapter level. As appropriate, these SPCs are applied to the Overall HMI and to individual HMIs, although not all of the nine SPCs are relevant to both the Overall HMI and to individual HMIs (for further details see [Ref-1]). Each SPC sub-claim and argument is identified by a prefix relevant to the specific HMI (or 'Overall HMI') in the BSC document of the relevant HMI system.

The nine C&I SPCs, plus a description of how the HMIs relate to and supports each of the C&I SPCs are provided in Appendix B. Detailed safety case claims are described in the BSCs on Overall HMI [Ref-1], MCR HMI [Ref-2], RSS HMI [Ref-3], and B/B HMI [Ref-4]. These references directly provide the arguments that support each of the SPCs in Appendix B and specify references to the documentation that provides the supporting evidence for those SPCs.

All of the C&I SPCs provide support to the overarching claim in PCSR Chapter 1:Introduction that a UK ABWR constructed on a generic site within the UK, meets all safety targets for the public, workers and the environment, and satisfies the principle that all risks are ALARP for all operating and fault conditions. In particular, Appendix B explains how C&I SPC 3 demonstrates that the key risk associated with HMI of 'Non-availability of an HMI when required', identified in Section 21.10.1, has been reduced to levels that are ALARP, as far as is possible within GDA.

21.3.4 Consideration of Human Factors

The HMIs in each location (i.e. MCR, RSSR, BBCR, Rw/B MCR and Local) are designed to enable comfortable, logical and effective task performance for all users. This includes taking the environmental conditions, layout and workspace into consideration for both operators and maintenance personnel.

Further descriptions of the HF requirements and assessments that have been used to support the optimal HMI design can be found in the PCSR Chapter 27:HF and related supporting documents. The remainder of this section provides a summary of these considerations.

21.3.4.1 Human Factors Safety Property Claims

In addition to the physical properties of the HMI hardware to meet the requirements of the related C&I systems to which they are connected (C&I SPCs in Section 21.3.3), the design of the areas in which HMI are located and components on the HMIs also meet basic HF design requirements. The HF topic area has generated a set of HF SPCs, which are listed in the HBSC report [Ref-9]. Note that these claims apply to all aspects of SSCs with which human actions important to safety are performed, and across all relevant areas of plant.

Specifically, the two HF SPCs that apply to the design of HMIs are HFSPC 1 and HFSPC 3. They are listed with the C&I SPCs in Appendix B.

These two HF SPCs are linked to the overarching C&I SPC 7 for the HMI meeting required performance criteria to ensure SFCs are achieved and FSFs maintained, as described in Appendix B. In particular, these HFSPCs are an essential element to ensure that expected human performance of claimed actions within the UK ABWR safety case can be achieved at the relevant HMIs. Thus, HF SPCs 1 and 3, together with C&I SPC 7, demonstrate that the risk of the 'Possibility of the HMI inducing human error', identified in Section 21.10.1, has been reduced to levels that are ALARP, as far as is possible within GDA.

The following section provides a summary of the specific key HF design considerations that apply to the design of the UK ABWR HMIs in order to meet the above claims.

21.3.4.2 Summary of Key HF Design Considerations

In order to provide effective and reliable plant and process monitoring and control and support the achievement of HBSCs with human error related to HMI design reduced to ALARP, the UK ABWR design takes into account good-practice HFE principles as outlined in key reference standards and guidance documents. The HFE requirements for the entire plant design are distilled into the HFE

Specification [Ref-11] to be applied by all design teams within Hitachi-GE for UK ABWR. For the HMI design the following were considered to be the key areas of design to which the HFE Specification was applied:

- environment of HMI locations,
- layout of HMIs within each location,
- layout on each HMI of the individual components that form the interface, and
- selection and/or design of the individual interfacing components.

In addition to the application of basic HF principles given by standards and guidelines, in order to support effective and reliable task performance during human actions claimed within the safety case in which the HMIs described in this chapter are used, specific requirements for displays, controls and alarms are determined by considering the required tasks. Specifically function, task and error analysis is conducted of the preventive and mitigative actions required for the relevant fault. Any recommendations for the key areas of design listed above that result from the analyses are incorporated. This analysis is not covered within the scope of this chapter but is within the scope of Chapter 27:HF.

The remainder of Section 21.3.4 provides a further summary of the types of design considerations incorporated into the UK ABWR HMIs that reflect the basic good HF principles outlined in the HFE Specification [Ref-11]. Further detail of application of the HFE Specification to the UK ABWR design during GDA is provided in Chapter 27:HF and its supporting documents, particularly the HF Design and Engineering Report [Ref-14].

21.3.4.3 Environment of HMI Rooms/Areas

In order for the operators to comfortably operate in the various control rooms in UK ABWR, environmental factors such as temperature, lighting, noise and vibration have been taken into consideration, and the room and supporting systems have been designed accordingly.

Lighting is particularly important for safe, effective use of the HMIs. For UK ABWR, not only have overall normal and emergency light levels been suitably selected, the following have been considered in the design:

- making light levels adaptable to allow for different task conditions,
- the need for local task lighting, and
- reducing indirect and direct glare on displays (for both individual and team viewing conditions).

Temperature is maintained as defined for each room and the area where each HMI is installed by the supporting HVAC system as described in C&I SPC 1.2.

In HMI areas outside control rooms where HBSCs are claimed, environmental factors such as temperature, lighting, noise and vibration are likely more of an issue to operating the HMI, but also control of the environment for effective HMI usage is only needed when the HMIs are needed. Therefore suitable measures to manage working environment may include temporary measures either located nearby the HMI area or brought in specifically to conduct the claimed action (as determined by HF analysis based on importance of claim and time available).

In any HMI area where HBSCs are claimed, either inside control rooms or at local panels, the environment around and on at least one route to the claimed HMI is protected from personnel health hazards such as radioactive contamination, smoke, excessive heat or cold, etc., in assumed plant conditions, including during foreseeable events.

21.3.4.4 Workspace – Location and Layout of Control Rooms/HMI Areas

The workspace and layout of the HMIs within each of the various control rooms in UK ABWR are designed using workspace task-based analysis ("link analysis") as well as the basic requirements of the HFE Specification [Ref-11] for reach, clearance and viewing to facilitate the tasks assigned to the MCR personnel. This includes normal operations, routine and corrective maintenance, and post-fault actions.

In particular, the layout of the HMIs in the MCR, RSSRs and BBCR are designed to take into account the actions which personnel have to perform under accident conditions, and in the case of fault conditions that require manual operations, includes consideration of more interactive and timely team communications and joint working in circumstances where effective communications may be impacted by needing to respond quickly to degraded plant conditions.

The following are design features incorporated to enable effective workspaces in HMI areas:

- Adequate space and clearance are given around each HMI in the control room for the required number of personnel to work at the HMIs,
- Access to important control areas is controlled to minimise unnecessary interruptions and also prevent unwanted access to important HMIs,
- "Traffic" areas are separated from and behind any HMIs and large displays,
- HMIs are positioned such that personnel sat in their normal working positions can see any overview information and also other personnel, and
- Suitable size and number of overview panels including large display and Plant-level Flat Displays (PFDs) are provided in control rooms where teams work jointly and share information quickly and reliably.

In addition to the main control rooms, where necessary to support claimed human actions within the safety case, alternate or "backup" control rooms or HMI areas are provided (see Section 21.3.5 Strategy of HMI Usage). Alternate control rooms/HMI areas are established in a separate location with enough distance from the MCR and/or other HMIs postulated as impacted in each specific

scenario they are used in, such that the alternate control room/HMI area is not affected by the same hazard. They are also placed in a location that can be reached in the timescales in which the actions performed in them are required to be completed by in the fault scenarios where they are claimed. The route leading toward the alternate control room/HMI area is designed so as to be safe for the operators to transit from the MCR, in the postulated conditions that have made the original control room/HMI area uninhabitable.

In addition to their optimised location, access to the alternate control rooms/HMI areas is controlled to ensure protection of the backup functionality. Changeover switches need to be operated for the alternate locations to be used to control plant. This measure reduces the likelihood of accidental or deliberate inappropriate operation and meets current HF standards regarding prevention of more than one control point being active at any one time. Section 21.5.4 provides further details for the RSPs in the RSSRs.

21.3.4.5 Layout of Component Items on the HMIs

In order to minimise various types of errors (misinterpretation, omission, selection errors, etc.) by the operators, the design of the HMIs incorporates such HF good-practice principles as,

- enabling the group monitoring of key plant parameters,
- placing displays in logical relation to their associated plant equipment and controls,
- positioning frequently operated or important components in central locations, and
- grouping by function and task where appropriate, to make related tasks and sequential task steps easier to complete in a logical manner.

The above principles are not only applied to the layout of individual hardware components on the HMIs; they are also used in the arrangement of the graphical items on the Flat Displays (FDs) of the digital system. Where possible, and where appropriate to the related systems and tasks, the layout on both hardware- and software-based HMIs follows a “mimic” style where the processes of the system are represented in graphical format with the component items placed appropriate to their location within the process.

As much as possible, by using the HFE Specification [Ref-11] allows consistency in HMI layout style and components across all HMIs throughout the plant, including from digital FDs to hardware-based HMI panels.

21.3.4.6 Selection and Design of HMI Component Items

21.3.4.6.1 Alarms

Since UK ABWR is a highly-automated plant and most operator manual actions within the MCR relate to providing additional backup to safety systems, the alarm system is a key to ensuring expected user task performance. The alarm system within the MCR is designed in accordance with the HF good practice and guidance which is derived from:

- the HFE Specification [Ref-11], for physical design characteristics, including audible and visual indications for the varying alarm states, and
- the Alarm Processing and Presentation Strategy [Ref-15], for the alarm system logic and functionality, including definition of the basic alarm set, prioritisation and rationalisation of what alarms are presented at any given time and the HMI on which they should be presented.

In summary, the system is designed such that it:

- focuses operator attention on key important alarms,
- ensure only alarms relevant to the job role of the personnel receiving them are presented at any HMI location,
- minimises alarm "flooding", situations where too many alarms are presented at any one time,
- groups SSC-specific alarms by system,
- allows operator management of alarm display and audible features,
- prioritises alarms in a logical and consistent manner, and
- gives essential information on large tiles on the overview display (e.g. the WDP in the MCR or PFDs) to be visible by the whole team of personnel operating within the control room, with repeated presentation of those alarms, but with further detailed information, on the displays located on individual operator displays.

Further information regarding alarm functions is shown in the BSC on Overall HMI [Ref-1].

21.3.4.6.2 Displays

Displays are designed to be visible and legible from as great a range of angles as possible. If possible display heights and angles are positioned to accommodate the full range of users intended for UK ABWR.

Digital displays are selected with optimal visibility factors such as brightness, contrast, resolution, chromaticity, refresh rate and management of indirect and direct glare.

The displays of the information giving the state of plant systems and equipment, along with the information necessary for safety, are provided for operators in appropriate locations. They are displayed in a manner that is easy to understand and interpret.

The correct or optimal display type is selected for the type of information being presented. Dynamic displays act in ways that match the expectations of the user population. Where fixed acceptable operating ranges and limits exist for parameters being displayed, their normal and limiting values are clearly indicated.

Where related to automated functions, displays are selected to provide information such that they allow the operators to monitor and confirm the progression of those automatic operations. Where they relate to manual functions, the displays are clearly visible whilst using the related controls and provided timely feedback on the result of manual actions.

A unified logical overview display is provided in the front and centre of control rooms where teams are working (e.g. on the WDP the MCR) to focus attention on key plant (for the MCR, reactor; elsewhere, related process) parameters and allow all users to monitor and assess plant status simply and rapidly.

21.3.4.6.3 Controls

Control devices are selected/designed to be easy to operate and move in expected directions in order to minimise operator errors. They are positioned in logical relationship for sequential task step performance. In order to minimise commission errors by operators, including inadvertent operation controls are well-labelled, shape- and colour-coded where necessary and spaced adequately to ensure their function is understood and accidental operation of the wrong control is avoided.

Where misoperation of the control systems and equipment in the MCR can lead to potentially hazardous outcomes, appropriate considerations are given to providing protection covers, key attached switches or special labelling. On software-based graphic displays, such similar control features are protected by having on-screen "warnings" about the potential for hazardous outcomes, and having confirmation using an input device final actuation step. These features are in addition to various system interlocks and automatic overrides which prevent inappropriate actuation of systems based on plant status.

21.3.4.7 Verification and Validation

During Step 4 Hitachi-GE has conducted a suitably comprehensive and proportionate V&V programme for the level of design maturity available during GDA. The V&V Programme is described in more detail in PCSR Chapter 27:HF and its supporting documents; in particular, the UK ABWR GDA HF V&V Plan [Ref-19] clearly defines and justifies the scope of the programme. A brief summary of activities is provided here. These V&V activities included:

- an initial gap analysis between the HMI from the J-ABWR and UK design requirements as described in the HF Design and Engineering Report [Ref-14],
- iterative verification of revisions of HMI design against design requirements throughout GDA, and
- partial validation of the MCC and backup HMIs using task and scenario based testing, as necessary, using static mock-ups.

These partial validation activities primarily made use of experienced J-ABWR Operators as test subjects, due to their extensive familiarity with operating the plant and their ability to more effectively understand and "simulate" the tasks and scenarios, making them the most suitable and valid test subjects available. UK operator representatives reviewed the video recordings of the scenarios enacted by the test subjects, to ensure that the UK operational context was adequately considered. In addition, one testing scenario made use of the UK operator representatives, once they had completed a suite of J-ABWR systems courses.

The results of the V&V programme conducted by Hitachi-GE during GDA have helped to ensure that the current design supports the necessary actions and human performance required from the claimed HMI by Operators. These activities have provided partial levels of V&V of the UK ABWR HMI design at its current level of maturity. This has subsequently influenced the HMI design through changes/modifications, or where necessary issues being identified for transfer to and resolution by future licensee during the detailed design phase.

It is expected that future licensee will produce and conduct a more detailed V&V Programme with increasing levels of task fidelity, taking consideration of the GDA V&V results to date, to support the subsequent detailed design activities for HMIs and further HBSC substantiation. However, defining the scope of that future V&V programme and specifying the tools, mock-ups or simulation required are activities entirely under the remit of the future licensee and as such are not discussed further in this chapter or the rest of the GDA PCSR.

21.3.4.7.1 Communication Equipment

Although the physical properties of communications systems fall within the scope of PCSR Chapter 15:Electrical Power Supplies, the systems obviously are a form of "HMI" within the plant. More significantly to this chapter, the use of communication systems is needed for, and can impact some of the claimed human actions that are performed on the HMIs for plant control. The details of when communication systems are required to support HBSCs is covered in Chapter 27:HF. This section gives a brief summary of the design requirements for the provision of those systems and their interfacing components; the details of the communication system design requirements are implemented through the HFE Specification [Ref-11] to the extent applicable within GDA scope.

For operators or maintenance personnel (including test personnel) who are performing coordinated operations and maintenance activities in separate locations, the means for clear and effective communications between operations or maintenance personnel are provided. Specifically, adequate communications systems are provided as necessary and their design is of suitable usability, availability and reliability to ensure means of clear communication are provided in all of the conditions in which coordinated tasks claimed within the safety case are expected to be performed. For example, appropriate local-network mobile, hardwired or paging systems allow operators in remote control areas (i.e. control rooms separated visually from controlled equipment) to communicate effectively with operators who are performing tasks local to plant equipment.

21.3.5 Strategy of HMI Usage

Along with the fixed HF requirements for HMI design that are derived from international standards and guidance (described in Section 21.3.4), the HMIs provide the required functionality for the actions intended to be carried out on each interface, and in the plant conditions expected during those actions. Such expected usage for the main HMIs used in reactor operation is detailed in the BSC for MCR HMI [Ref-2] for normal operations, and in the Strategy of Use for HMIs [Ref-16] which explains the design intent for abnormal operations that has been assumed in GDA. The strategy for HMI usage in all conditions makes up an important part of the overall operational strategy for the UK ABWR that is described in GDA PCSR Chapter 30:Operations, and is consistent with the assumptions made in that Chapter.

This section provides a brief summary of the consideration of strategy of HMI usage assumed in the development of the GDA design of the UK ABWR HMIs.

The HMIs within the scope of this chapter are intended to be used for a variety of actions from normal operations through supporting EMIT to helping to mitigate fault and accident conditions during events. The C&I systems that are used for normal operation are the PCntlS, ACS and PCS, as described in section 14.6.1 of GDA PCSR Chapter 14:C&I. The HMIs for all of these are included on the MCC or WDP located in the MCR, as described in section 21.4.2, with more detail in the BSC for MCR HMI [Ref-2] and associated TRs for each of these C&I systems. Intended usage and operational flow for the HMIs for normal operations are assumed to be the same as J-ABWR design and assumed to be acceptable (as per the baseline HF assessment for UK ABWR reported in the Baseline HF Assessment Report (BAR) [Ref-18]).

Clearly not all usage of HMIs is related to human actions that are claimed within the UK ABWR safety case (i.e. HBSCs). Of relevance to the PCSR is the strategy for the intended use of the HMIs to conduct actions claimed as safety measures within the case, largely identified within the Deterministic Safety Analysis (DSA) and PSA (PCSR Chapters 24 and 25, respectively), and captured and substantiated in PCSR Chapter 27:HF. The Strategy of Use for HMIs [Ref-16] defines the overall functionality of each of the HMIs that are used for reactor operation, during reactor fault conditions, including severe accidents (i.e. Class 1 and 2 HMIs in the MCR; RSSR HMIs; and BBCR HMIs). This includes description of the design intent for user response to a range of HMI failures, and for the movement of operators through the various HMIs as faults progress.

The HMIs for UK ABWR are designed to provide the intended users with adequate information and control functions to be able to perform the required tasks, in an appropriate location under the assumed plant conditions that are specified in the Strategy of Use for HMIs [Ref-16].

In general, each HMI is designed in order that it achieves the following:

- Provides the indicators and controls required for functionality of C&I systems and to perform claimed human actions,
- Minimises the likelihood of user misinterpretation, errors and omissions,
- Provides ease of operation, in terms of the usability and maintainability,and

- Takes into account relevant experience from existing plants to improve the design to support improved task performance by users.

See discussion of the application of C&I SPC 7, HFSPC 1 and HFSPC 3 to HMIs in Appendix B, to address the key risk of 'Possibility of HMI inducing human error' that is identified in Section 21.10.1, to levels that are ALARP.

Each HMI has been assigned functionality, and the use of any particular HMI for monitoring and operation depends on the tasks to be performed and the plant status. Alternative and backup HMIs are provided based on the requirements of the safety analysis for each system (for example the SAuxP is able to control one division of the equipment associated with the SSLC). For Local HMIs and HMIs of the Radwaste facility, there are currently no identified safety requirements for backup HMIs.

The basic strategy of assignment of HMIs is decided taking into account the following:

- Objective of operation,
- The area where SSCs are installed (For SSCs not required for power operation),
- Plant operating condition,
- Environmental condition (Availability of the room in which the HMI is located),
- Availability of SSCs that are functional, and
- Provision of sufficient defence-in-depth levels of availability of usable HMIs in any abnormal conditions. See discussion of the application of C&I SPC 3 to HMIs in Appendix B, to address the key risk of 'Non-availability of an HMI when required', that is identified in Section 21.10.1, to levels that are ALARP.

Figure 21.3-1 shows an overview of the intended usage considered during design of the HMIs, taking account of their availability for use in each plant state. The logic presented in this diagram is fully explained in the Strategy of Use for HMIs [Ref-16], which demonstrates that suitable and sufficient HMIs are available in all plant conditions.

The Strategy of Use for HMIs [Ref-16] expands on this by providing a more detailed flow diagram to explain the design intent for how the operators would decisions regarding which HMIs to use in a range of fault conditions, dependent on combinations of alarms, monitored plant conditions and indications that SSCs are unavailable.

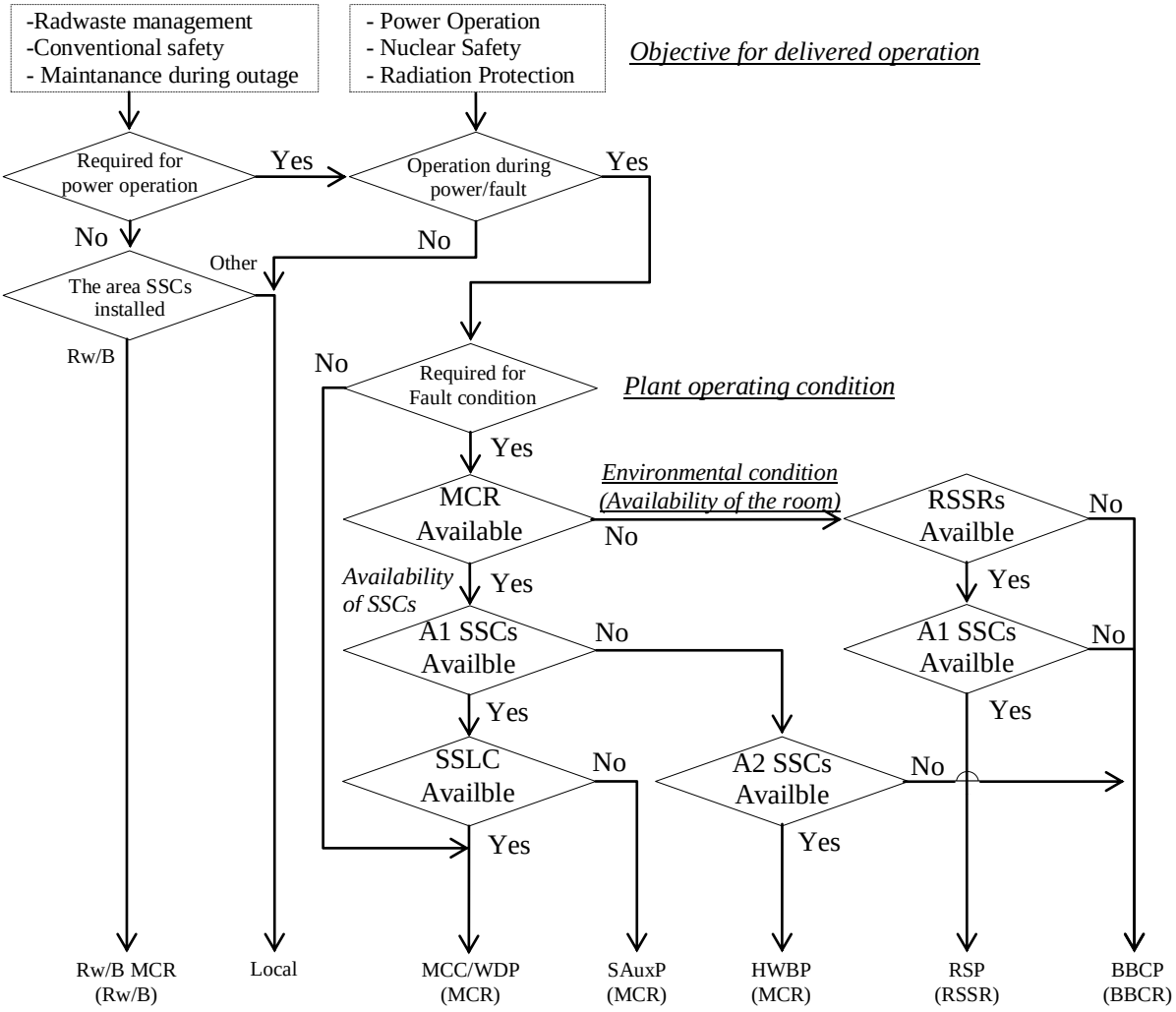


Figure 21.3-1: Overview of HMI usage strategy for design

21.3.6 Reference Standards

The reference standards that have been considered as part of the design of the HMI are listed below. Note that only the key HF standards that relate to HMI design are listed below; further information and standards relating to consideration of HF within the design of control areas and HMIs (i.e. access, reach, clearance, noise, lighting, etc.) are listed as part of the HFE Specification [Ref-11].

1. BS EN 61772:2013 "Nuclear Power Plants – Control Rooms – Application of Visual Display Units", March 2013
2. BS EN ISO 9241-(various) "Ergonomic Requirements for Office Work with Visual Display Terminals/Ergonomics of Human-System Interaction" (various relevant sub-topics)
3. BS EN ISO 11064-(various) "Ergonomic design of control centres" (various relevant sub-topics)
4. BS EN ISO 14915-(various) "Software Ergonomics for Multimedia User Interfaces" (various sub-topics)
5. EEMUA 191 "Alarm Systems – A Guide to Design, Management and Procurement", 3rd Edition, June 2013
6. IAEA Safety Standards Series No. SSG-39, "Design of Instrumentation and Control Systems for Nuclear Power Plants", April 2016
7. IEC60964 "Nuclear power plants – Control rooms – Design", 2nd Edition, February 2009
8. IEC60965 "Nuclear power plants – Control rooms – Supplementary control points for reactor shutdown without access to the main control room" 2nd Edition, July 2009
9. IEC61226 "Nuclear power plants – instrumentation and control systems important for safety – classification of instrumentation and control functions", 3rd Edition, July 2009
10. IEC61227 "Nuclear Power Plants – Control Rooms – Operator Controls", 2nd Edition, April 2008
11. IEC 61508 "Functional safety of electrical/electronic/programmable safety-related systems" 2nd Edition, April 2010
12. IEC61513 "Nuclear power plants – Instrumentation and Control important to safety – General requirements for systems" 2nd Edition, August 2011
13. IEC62241 "Nuclear power plants. Main control room. Alarm functions and presentation" 1st Edition, November 2004
14. NUREG-0700 "Human-System Interface Design Review Guidelines", Rev.2 2002
15. WENRA Issue E (Design Basis Envelope for Existing Reactors) "Instrumentation and Control systems and control room"
16. WENRA Issue F (Design Extension of Existing Reactors) "Instrumentation for the management of beyond design basis accident conditions"

21.4 HMIs in the Main Control Room

21.4.1 Introduction

This section outlines the HMIs in the MCR. The details are described in the BSC on MCR HMI [Ref-2].

The main HMI of the nuclear reactor and power generation systems is established in the MCR. This is in order to allow the main human actions required for monitoring and controlling the plant to take place in one appropriately-designed facility.

The MCR contains HMIs related to the following C&I systems:

- SSLC (associated HMIs are the MCC, WDP and SAuxP),
- HWBS (associated HMI is the HWBP),
- SACS (associated HMI is the MCC and WDP),
- PCntlS (associated HMI is the MCC),
- ACS (associated HMI is the MCC and WDP), and
- PCS (associated HMI is the MCC and WDP).

The operators in the MCR monitor and control the plant and processes during a plant start-up, hot/cold shutdown, power operation, fault conditions, and during refuelling outages (see Figure 21.3-1 in Section 21.3.5).

Note that many of the refuelling activities are controlled locally, including through the FHM remote control room. Other plant processes are also supported by HMIs in other control rooms or local control panels, as described in Section 21.7 of this chapter.

The MCR is designed to enable the required complement of operational and support personnel (see the PCSR Chapter 30:Operation regarding minimum MCR crew complement) to remain in the room, performing necessary tasks, even in the event of foreseeable accidents. The layout of the HMIs in the MCR supports the workflows and communication needs of the crew for required operations during assumed plant states, including maintenance, as demonstrated by the HF support and analysis conducted as part of the UK ABWR integrated HF programme (see Section 21.4.3 and the PCSR Chapter 27:HF).

In addition, the HMIs in the MCR are designed with suitable and sufficient features to support the required tasks in the assumed plant conditions required (as specified in the Strategy of Use for HMIs [Ref-16], and summarised in Figure 21.3-1), and to help reduce the risk of operator errors to levels that are ALARP. The MCR and its HMIs are designed to minimise operator misinterpretation, errors and omissions. The HMIs located in the MCR are designed to enable adequate and appropriate communication among operators.

The requirements and principles for consideration of the relevant HFE aspects for the HMIs in the MCR are summarised in Section 21.3.4, detailed in the HFE Specification [Ref-11] and take account of the necessary functions as per the operating aspects specified in the HF COR [Ref-7].

21.4.2 MCR and MCR HMIs Structure

The MCC, the WDP, the SAuxP, HWBP, a Control Room Operator (CRO) operator desk, and the Main Control Room Supervisor (MCRS) desk are installed in the MCR.

(1) MCC

The MCC provides operators with indicators and controls for plant operation to ensure safety during power operation, start-up, hot/cold shutdown operation, refuelling outages and during fault conditions. This includes DBA and BDBA/SA so long as it is possible for the operators to remain in the MCR. Therefore, HMIs on the MCC are in continuous operation regardless of operating condition. The MCC consists of FDs and a variety of hardwired indicators/controls.

(2) WDP

The WDP provides operators with information for plant operation to ensure safety during power operation, start-up, hot/cold shutdown, refuelling outage, and fault conditions when the MCR remains habitable and functional, in order that operators can understand overall plant status and share information between themselves in the MCR. Therefore, HMIs on the WDP are under continuous operation regardless of operating condition. The WDP consists of FDs and a variety of hardwired indicators/controls.

(3) SAuxP

The Class 1 SAuxP HMI is hardwired and addresses the possible Common Cause Failure (CCF) of the digital HMIs for the SSLC to allow the plant to be kept operational and steady for a defined period whilst the main digital HMI functionality is restored. Priority of operation is switched from digital controls of the SSLC to the hardwired logics by transfer switches on the SAuxP. During power operation and fault conditions when the SSLC is operational, the SAuxP is on standby with power continuously supplied. However, the function of indicators and switches isn't activated until the transfer switches are operated.

(4) HWBP

The HWBPs are provided as HMIs for HWBS which controls Category A Class 2 SSCs. They also provide hardwired indicators and controls for the SA C&I of which some SSCs are shared between HWBS and SA C&I. Some of the SSCs which are controlled by the HWBS are required to be continuously operated. Therefore, HWBPs are under continuous operation during power operation, start-up, hot/cold shutdown, and refuelling outage as well as in fault conditions when operations with the HWBPs are required. No programmable technology or FDs are used for the HWBP to support claims on security, diversity and avoidance of CCF.

(5) Desks

A MCRS desk is provided, with a MCRS workstation, to allow for oversight and monitoring of activities within the MCR, as well as enough room to perform the various paperwork and referencing duties performed by the MCRS.

Desks are provided taking the following factors into consideration:

- Writing and laying down of documents and hard-copy procedures, and
- Communication between operators (including the CRO and MCRS).

The above workstations and desks are appropriately divided and arranged in accordance with their functions. This is to optimise the operational effectiveness and to reduce the probability of operator error, through separation and grouping of HMIs related to safety versus plant control, and grouping of the most important displays and controls to safety in order to focus operator attention accordingly.

The arrangement is designed to enable the CRO and MCRS to adequately communicate with each other. The design also provides all of the MCR personnel with good visibility and usability of the WDP, and further provides the MCRS with a clear overview of the MCC activity as well.

The basic layout of the MCR is shown in Figure 21.4-1. Further information regarding the layout of MCR is shown in the BSC on MCR HMI [Ref-2].

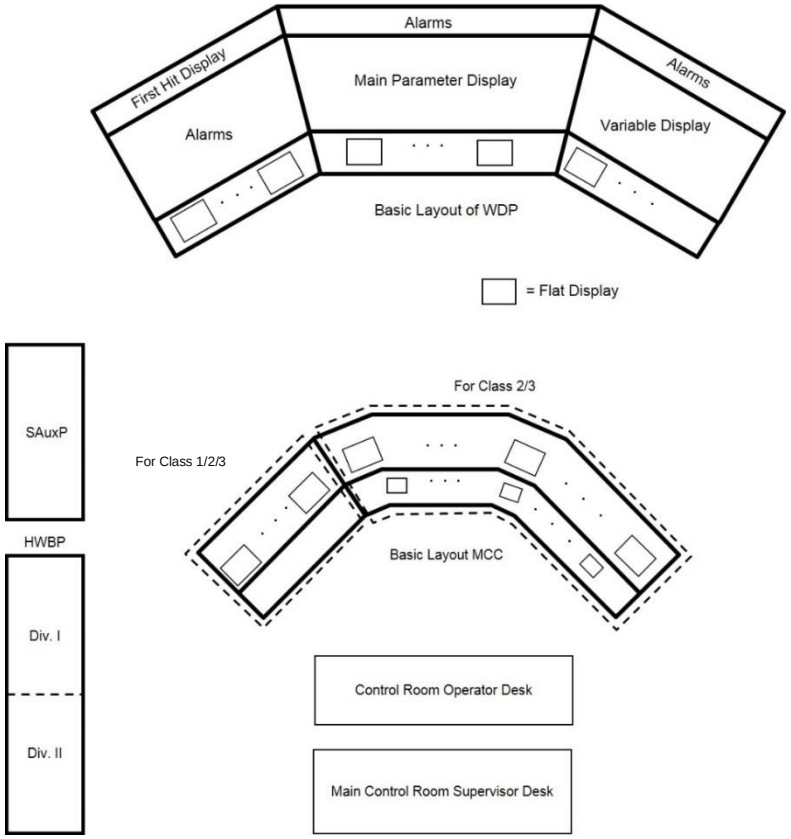


Figure 21.4-1: Basic layout of MCR

The allocation to HMI by C&I system is as follows:

SSLC

- The HMIs for SSLC (Divisions 1, 2 and 3), containing indicators and controls, are included on the MCC and WDP. Alarms and indications from the SSLC are included on the WDP and repeated on alarms lists on the MCC. Some specific SSLC indicators and controls are included on the SAuxP.

HWBS

- The HWBS consists of various indicators, controls and alarms required for important manual backup actions in the case of postulated events with concurrent loss of the Class 1 (SSLC) functionality. These are contained on the HWBP.

SACS

- Class 2/3 SACS HMIs, including indicators and controls, are included on the MCC and WDP. These HMIs are display screen based, based on the same technology as the SSLC HMIs on the MCC.

PCntlS

- Class 3 PCntlS HMIs, including indicators and controls, are included on the MCC. These HMIs are display screen based, using touch-screen interfaces.

ACS

- Class 3 ACS HMIs, including indicators and controls, are included on the MCC and WDP. These HMIs are display screen based, using touch screen interfaces.

PCS

- Class 3 PCS HMIs, including indicators, are included on the MCC and WDP. These HMIs are display screen based, using touch screen interfaces.

Further information of allocation of HMI in the MCR by the above C&I systems is provided in the BSC on MCR HMI [Ref-2].

HF support to the development of the HMIs for the UK ABWR and related HF analyses have been conducted during GDA. The HFE Specification [Ref-11] details basic generic HF requirements to meet modern standards and good practice guidance in HMI design as described in Section 21.3.4.

The results of the HF assessment and analysis for the operability of the HMIs performed in GDA are reflected in the HMI design, including use of consistency, suitable colour coding and labelling, where appropriate. These design considerations relevant to the HF analysis are applied to not only the design of the HMIs in the MCR, but also the design of other control rooms, including RSSRs, BBCR and Rw/B MCR for consistency in consideration of user task performance. This is summarised in Section 21.3.4.

Further details on the analysis and design support, and the arguments and evidence relating to the HBSCs linked to these HMIs are given in the BSCs for MCR HMI [Ref-2] and the PCSR Chapter 27:HF, including its supporting documents.

21.4.3 MCR HMI Functions

The HMIs in the MCR allow the operators to monitor operating conditions and important parameters in the reactor and other plant, processes and facilities.

The HMIs in the MCR support achieving the FSFs identified in Section 21.3.2.

The FSFs which are associated with the HMIs in the MCR are described below:

FSF1 – Control of reactivity,

FSF2 – Fuel cooling,

FSF3 – Long term heat removal,

FSF4 – Confinement/Containment of radioactive materials, and

FSF5 – Others (including the monitoring of key plant parameters).

In order to achieve the safety functions mentioned above, adequate HMIs associated with operations and monitoring of systems/equipment are installed in the MCR. This is demonstrated through the HF analysis and substantiation work given in the PCSR Chapter 27:HF, with arguments and evidence to support the HBSCs related to the HMIs given in the supporting documents to that chapter.

Details of C&I systems relevant to the FSFs mentioned above are shown in the PCSR Chapter 14:C&I. Further descriptions of the functionality which HMIs in the MCR deliver are shown in the BSC on MCR HMI [Ref-2].

21.5 HMIs in the Remote Shutdown System Panel Rooms

21.5.1 Introduction

The RSSRs are located in the R/B separate from the MCR but along a access route to ensure accessibility for the operators in the fault and hazard conditions that require use of an RSP. The HMIs are intended to allow the reactor to be brought into a state of cold shutdown from the hot shutdown state following an automatic or manual reactor scram operation.

The HMIs in each of the RSSRs are designed to enable the operators to monitor and control the plant shutdown process. The HMIs in the RSSRs are not intended to maintain the plant in operation or at hot shutdown conditions for any extended length of time. This section outlines the HMIs in the two RSSRs. The details are described in the BSC on RSS HMI [Ref-3].

21.5.2 RSSR and RSP Structure

Each of the two Class 1 Divisions of the RSS has its own set of panel controls and indications which is located in its own segregated room. The segregation is arranged to prevent internal hazards from affecting more than one division of the SSCs that interface with the RSP.

There is a single team of operators sent to the RSS in the event of either the need to evacuate the MCR or the CCF of the SSLC. There will be no confusion for the operators about the roles of each room or the need to divide the team as safety is maintained by the operation of a single division of Emergency Core Cooling System (ECCS) equipment from just one control panel. So the operators will be trained to use one room and one panel to control the ECCS safety functions and they would only need to move to the second RSSR in the event of failures in the first RSSR. The functionality and design within the two rooms is identical.

Each RSSR is equipped with a RSP and a desk. Priority of operation is transferred from digital controls of the SSLC to the hardwired logic in the RSSR by switching the multiple Remote Shutdown Transfer Switches (RSTSs) located on the RSPs from MCR operation mode to RSS operation mode [Ref-3]. The RSTSs are the only means of transferring the monitoring inputs and activation outputs from the MCR to the RSP, as there is no functionality to perform such a transfer of control from within the MCR. During power operation and fault conditions when the SSLC remains operational and the MCR can achieve its function, the RSSRs are unmanned with the RSPs on standby with electrical power continuously supplied. However, the function of indicators and switches is not activated until the multiple RSTSs are operated.

Further information on the transfer switches is given in the Basis of Safety Cases on SSLC [Ref-21].

The RSSRs and their HMI are designed to minimise operator misinterpretation, errors and omissions. The RSP and other equipment located in the RSSRs are designed to enable adequate and appropriate communication among operators.

The requirements and principles for consideration of the relevant HFE aspects for the HMIs in the RSSRs are summarised in Section 21.3.4, detailed in the HFE Specification [Ref-11] and take account of the necessary functions as per the operating aspects specified in the HF COR [Ref-7].

(1) RSPs

The two RSPs are provided as alternative HMI for A1 SSCs that deliver FSF2 and FSF3, for manual operation in the case that the operators are forced to evacuate from the MCR due to an internal hazard in the MCR, or the MCR functions are inoperable due to a fault. They interface with the Residual Heat Removal (RHR), High Pressure Core Flooder (HPCF), Reactor Core Isolation Cooling (RCIC) and Nuclear Boiler (NB) systems, plus their required water supply and electrical power supply supporting systems, including the EDGs.

A RSP is located in each of the two RSSRs, which allows the operators to carry out monitoring and control. In order to perform the required functionality, the each RSP consists of the following:

Monitoring Area

- Equipment is installed to provide monitoring of the reactor plant and process during the transition from a hot shutdown state to a cold shutdown state.

Operation Area

- Operational equipment is installed to allow the reactor to be brought into a cold shutdown state from a hot shutdown state.

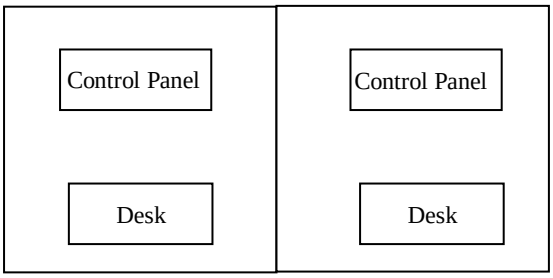
No alarms are provided on the RSPs as the need for alarms has not been identified as required to respond to any fault scenarios in the GDA fault assessments.

(2) Desks

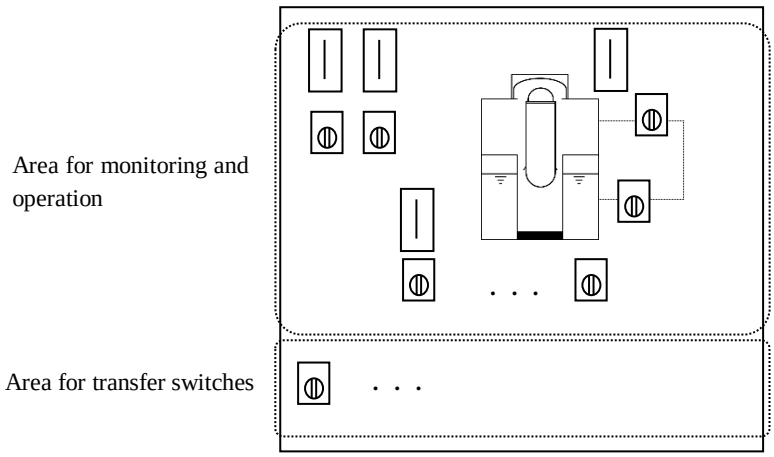
Desks are provided taking the following factors into consideration:

- Writing and laying down documents and hard-copy procedures
- Communication between operators

The basic layout of RSSRs is shown in Figure 21.5-1. The two divisions are separated by a fire barrier. Further information regarding the layout of RSSRs is shown in the BSC on RSS HMI [Ref-3].



Layout of the two RSSRs



Concept layout of each RSP

Figure 21.5-1: Basic layout of RSSRs

21.5.3 RSSR HMI Functions

When an evacuation from the MCR is necessary and a reactor scram does not occur automatically, the design intent is that the operators will attempt to manually scram the reactor from within the MCR.

Currently the RSSRs are intended for use in only two specific internal hazard scenarios, which are fire or internal missile in the MCR. These are unlikely to generate automatic reactor scram, and so it is anticipated for the site specific design that the operators will be provided with an alternate control for manual reactor scram along the access route to the RSSRs or within the RSSRs themselves. However, this functionality has not been developed in GDA, so is not part of the current GDA functional design of the RSPs.

The HMIs in the RSSRs support achieving the FSFs identified in Section 21.3.2.

The FSF which is associated with the HMIs in the RSSRs is described below:

FSF5 – Others

Immediately following scram, RSS functions are required to bring the reactor to a cold shutdown state from the hot shutdown state from outside the MCR.

In order to achieve the safety function mentioned above, adequate HMIs associated with operations and monitoring of the essential systems/equipment for the scenarios in which this HMI is intended to be used are installed in the RSSRs.

Details of C&I systems relevant to the FSF mentioned above are shown in the PCSR Chapter 14:C&I. Further descriptions of the functionality which HMIs in the RSSRs deliver are shown in the BSC on RSS HMI [Ref-3].

21.5.4 Independence from MCR Control Functions

The RSPs can control the A1 SSCs listed in 21.5.2 that are normally controlled from the MCR, but these alternate panels are only intended to be used when the MCR becomes uninhabitable with the A1 SSCs themselves still available, as shown in Fig 21.3-1. It is therefore important to minimise the potential for the RSPs to override or impair control of their associated SSCs from the MCR at any time when the MCR is habitable. This is achieved by the following design features:

- The RSPs can only take control of the associated SSCs by switching the RSTSs from MCR operation mode to RSS operation mode,

- By locating the RSTSs within the RSSRs, this means that deliberate switching of the RSTSs can only be performed by operators who have transferred from the MCR to one of the RSSRs. The RSSRs are normally unmanned, and access to the rooms is controlled with a lock, so operators would only be in an RSSR in circumstances where the MCR has become uninhabitable, when control of the A1 SSCs from the RSP is required,

- The potential for internal hazards to cause inadvertent operation of the transfer of control has been minimised as follows:

  - Most sources of risk from internal hazards in the RSSRs have been eliminated from the UK ABWR design such that the only remaining significant risk is from a fire in one of the RSSRs,

  - The risk of internal fire in the RSSRs is minimised by application of the standard measures to minimise fire sources in these two rooms,

  - Segregation between the RSSRs means that an internal fire will only affect one of the two rooms. Each room is connected to only one of the three independent divisions of the associated A1 SSCs. Hence even in the worst case internal hazard scenario two out of three of the divisions will remain under full MCR control, and

- The unlikely event of spurious actuation of A1 SSCs from an RSP is considered in the Failure Modes and Effects Analysis (FMEA) for CCF of support systems and the identified bounding fault is included in the fault schedule described in PCSR Chapter 24:Design Basis Analysis. That PCSR Chapter presents analysis that demonstrates that all bounding design basis faults in the fault schedule meet the relevant acceptance criteria.

21.6 HMIs in the Backup Building Control Panel Room

21.6.1 Introduction

There is a single BBCR on the plant site within the B/B. This section outlines the HMIs in the BBCR. The details are described in the BSC on B/B HMI [Ref-4].

C&I systems are provided in the BBCR to deliver the SA and other C&I safety measures identified and allocated to the BBCR. The HMIs provide appropriate operation, monitoring and manual control facilities to interface with those systems.

21.6.2 BBCR and BBCP Structure

The BBCR holds some BBCPs and a desk.

The BBCR and its HMI are designed to minimise operator misinterpretation, errors and omissions. The requirements and principles for consideration of the relevant HFE aspects for the HMIs in the BBCR are summarised in Section 21.3.4, detailed in the HFE Specification [Ref-11] and take account of the necessary functions as per the operating aspects defined in the HF COR [Ref-7].

(1) BBCP

The BBCPs are provided as HMI for B2/B3 SSCs in the case that A1 SSCs and A2 SSCs are unavailable during certain assumed conditions, for example, Station Blackout (SBO) design basis faults, BDBAs and SAs.

Priority of operation is transferred from the HWBPs in the MCR to the BBCPs by switching the Backup Building Transfer Switches (BBTSs) located on the BBCPs. The BBTSs are the only means of transferring operation from the MCR to the BBCP, as there is no functionality to perform such a transfer of control from within the MCR.

Further information on the transfer switches is given in the Basis of Safety Cases on SA C&I [Ref-22].

The BBCP consists of the following indicators and controls, selected to provide required functionality during a SA coupled with evacuation from the MCR.

Alarm Display Area

- An alarm display is installed to alert operators in the BBCR to plant, process or system conditions requiring operator attention or action.

Monitoring Area

- Monitoring equipment is installed to let the operators in the BBCR monitor the plant in the B/B and key plant and process conditions in the R/B.

Operation Area

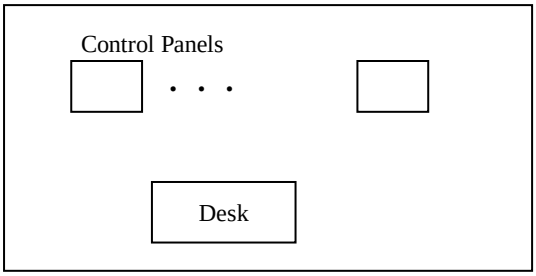
- Operational equipment is installed to allow the operators in the BBCR to control the plant from the B/B.

(2) Desk

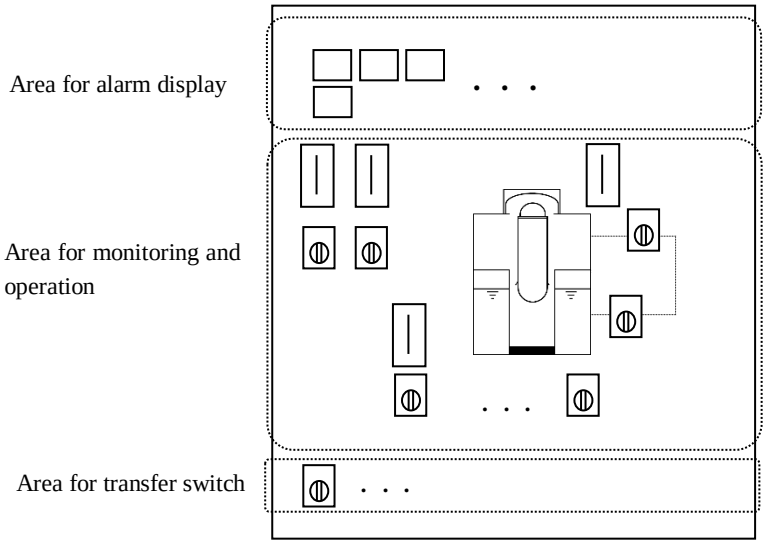
A desk is installed taking the following factors into consideration:

- Writing and laying down documents and hard-copy procedures, and
- Communication between operators.

The basic layout of the BBCR is shown in Figure 21.6-1. Further information regarding the layout of the BBCR is shown in the BSC on B/B HMI [Ref-4].



Layout in the BBCR



Concept layout of BBCP

Figure 21.6-1: Basic layout of BBCR

21.6.3 BBCR HMI Functions

The HMIs in the BBCR allow operators to monitor and control key operating conditions in certain fault conditions and during a SA, when the MCR and/or R/B are not inhabitable.

The HMIs in the BBCR support achieving the FSFs identified in Section 21.3.2.

The FSFs which are associated with the HMIs in the BBCR are described below:

FSF2 – Fuel cooling: Alternative means using the Flooding System of Specific Safety Facility (FLSS), Reactor Depressurization Control Facility (RDCF),

FSF3 – Long term heat removal: Through the Filtered Containment Venting System (FCVS),

FSF4 – Confinement/Containment of radioactive materials: Using FLSS, and

FSF5 – Others: Especially the monitoring of key SA plant parameters during accidents.

The FLSS and RDCF are described in PCSR Chapter 16.7: Severe Accident Mechanical Systems.

In order to achieve the safety functions mentioned above, adequate HMIs associated with operations and monitoring of the essential systems/equipment for the scenarios in which this HMI is intended to be used are installed in the BBCR.

Details of C&I systems relevant to the FSFs mentioned above are shown in the PCSR Chapter 14:C&I. Further descriptions of the functionality which HMIs in the BBCR deliver are shown in the BSC on B/B HMI [Ref-4].

21.6.4 Independence from MCR Control Functions

The BBCPs are the HMI to control the B2/B3 SSCs listed in 21.6.3. The alternate BBCPs are only intended to be used in the case of multiple failure events, such as MCR and R/B becoming uninhabitable and/or loss of required functionality from the MCR and RSSRs, encountered in certain fault conditions and beyond design basis conditions including severe accidents.

Some SSCs are shared between the SA C&I and the HWBS, and so some of the BBCP HMIs are duplicated and normally controlled from the MCR. It is therefore important to minimise the potential for the BBCP to override or impair the control of these shared SSCs at any time when the MCR is habitable and the MCR HMIs intended to be used. This is achieved by the following features:

- Control is switched from the MCR in the Control Building (C/B) to the BBCR using transfer switches located on the BBCPs, and
- The C&I architecture of the BBCR transfer switches is arranged so that even in the event of an unintended/unrequested transfer of HMI control to the BBCPs this does not disable the automatic actuation of the A2 SSCs.

21.7 HMIs for the Radwaste Facilities

21.7.1 Introduction

There are planned to be some control sites for various Radwaste facilities, as follows:

- Rw/B MCR; this holds control consoles of the LWMS and part of SWMS sub-systems,
- Control site in ILW Store; this holds controls and monitoring devices for the ILW store,
- Control site in HLW Store; this holds controls and monitoring devices for the HLW store,
- Control site in SWF Building; this holds controls and monitoring devices for the solid waste processing, and
- MCR; this holds HMIs for gaseous waste management or "off-gas" process equipment and selected information which are transferred from the Radwaste facilities.

The specific C&I, including HMI, will be entirely integral to those systems in the post-GDA stage and the design and safety case for those systems, particularly related to their functionality, falls within the scope of the PCSR Chapter 18:Radioactive Waste Management. Although SFCs for Radwaste facilities are substantiated within PCSR Chapter 18 and its supporting documents, the general design principles for the HMIs in the control rooms of the Rw facilities are described within this chapter.

21.7.2 Rw/B HMI Structure

The control room in the Rw/B contains operator consoles and a desk.

The operator consoles are designed to minimise operator misinterpretation, errors and omissions. They are consistent with the relevant requirements and principles for consideration in the HFE Specification [Ref-11] and take account of the necessary functions as per the design intent for operating aspects defined in the HF COR [Ref-7].

(1) Operator Console

The Operator consoles are composed of a number of Visual Display Units (VDU) that allow the operator to monitor and control C3 SSCs of Radwaste facilities during power operation.

(2) Desk

A desk is installed taking the following factors into consideration:

- Writing and laying down documents and hard-copy procedures
- Communication between operators

21.7.3 Rw/B HMI Function

The operator console for the LWMS is designed to be equipped with those functions necessary to enable operator monitoring and controlling of the normal operating conditions and any foreseeable fault condition of the LWMS facilities.

The HMIs in the Rw/B MCR support achieving the FSFs identified in section 21.3.2. The FSF which is associated with the HMIs in the Rw/B MCR is identified below:

FSF4 - Confinement/Containment of radioactive materials (which is relevant to LWMS and part of SWMS), and

FSF 5 – Others.

In order to achieve the safety functions mentioned above, adequate HMIs associated with operations and monitoring of the required functions of the LWMS systems/equipment and part of the SWMS are installed in the Rw/B MCR. Table 21.7-1 shows the list of SFCs delivered in the Rw/B MCR. Specific functions for Rw/B MCR are described in PCSR Chapter 18:Radioactive Waste, and further justification will be provided post-GDA.

Table 21.7-1 List of SFCs for Rw/B HMIs

SSCs	HMI SFC	Mechanical Engineering SFC	PCSR Chapter Reference
LWMS	Rw/B CR HMI SFC 4-12.1	LWMS SFC 4-12.1~7	18
	Rw/B CR HMI SFC 5-9.1	LWMS SFC 5-9.1	18
SWMS	Rw/B CR HMI SFC 4-13.1	SWMS SFC 4-13.1, 4-13.2, 4-13.4	18

21.8 HMIs in Local Control Locations

21.8.1 Introduction

In addition to the HMIs described in the previous sections (HMIs in the MCR, RSSRs, and BBCR), there are several types of local panels and relevant HMIs that are installed in other local areas within the plant. This section outlines the HMIs associated with the relevant SSCs which have nuclear safety claims and are controlled and monitored locally.

Because these local HMIs are based on C&I that is integral to the specific SSCs they support, the safety justification for their C&I is outside of the scope of PCSR Chapter 14 (although some is covered under the "Other" C&I category, where there is a specific link to the C&I in scope). As such, the justification of their functionality is outside of the main HMI BSCs that form part of this chapter. However, their physical design in still underpinned by the requirements and claims.

21.8.2 Design Requirements of HMIs in Local Control Locations

Regardless of where HMIs are located and where their SFCs are substantiated, the general design principles relating to the SPCs are driven by C&I and HF requirements, i.e. the generic HMI physical hardware design properties that relate to Category and Class and the generic features that support usability.

21.8.3 Local Control Location HMI Functions

Adequate HMIs associated with the operations and/or monitoring of the systems/equipment which are relevant to the local control are installed in each local control location. The HMIs in each local control location allow operators to control and/or monitor functions locally. Local control locations are provided or enabled where there is an advantage to providing local control facilities and where provision of such facilities does not lead to an undesirable risk of inappropriate operation. Where appropriate, local control locations are alarmed to the MCR.

In line with the SCDM [Ref-13], HMIs required to implement the functions claimed for the SSCs within the scope of this chapter are identified as arguments within the relevant BSCs that support this chapter. Although such arguments are in essence SFCs on the HMIs that are required by this chapter, for local HMIs, the case for these functional claims is presented within the BSCs supporting this chapter not in this Chapter.

The list of SSCs which are controlled by local HMIs and their related SFCs, including those related to the Rw facilities is given in Table 21.8-1.

Table 21.8-1 List of SFCs for local HMIs

SSCs	HMI SFC	Mechanical Engineering SFC	PCSR Chapter Reference
HECW	Local HMI SFC 5-18.1	HECW SFC 5-18.1 ~ 2	16
RSW	Local HMI SFC 5-2.1	RSW SFC 5-2.1 ~ 5	16
SWMS	-	-	-
SWF	Local HMI SFC 4-13.1	SWMS SFC 4-13.6	18
ILW	Local HMI SFC 4-13.2	SWMS SFC 4-13.7	18
FHM	Local HMI SFC 5-6.1	FHM SFC 5-6.1 ~ 3	19
FPM	Local HMI SFC 5-6.1	FPM SFC 5-6.1 ~ 2	19
RBC	Local HMI SFC 5-6.1	RBC SFC 5-6.1 ~ 2	19

Note that, as per Table 21.2-1 regarding design maturity within GDA, the C&I and HMI design maturity for these local HMIs is less than that for the main and backup plant control HMIs whose functionality descriptions and BSCs fall within the scope of this chapter. As such the list of local HMIs and their SFCs is expected to be developed further by future licensee in the site-specific stage.

21.9 Assumptions, Limits and Conditions for Operation

The strategy of HMI usage described in Section 21.3.5 and the Strategy of Use for HMIs [Ref-16], and the input to the concept HMI designs that derives from it, are based on a number of assumptions made for GDA.

The main relevant assumptions include such things as;

- Recognition that the description of the overall operational strategy for the UK ABWR in GDA PCSR Chapter 30:Operations specifies many assumptions that set the wider context within which the HMIs are used,
- The GDA design intent in the Strategy of Use for HMIs [Ref-16] will be adopted by a future licensee,
- The extent to which J-ABWR design of HMIs has been assumed in GDA is explained in Section 21.2.2 of this chapter,
- Assumed site staff complement and their associated roles and responsibilities in GDA – details are in [Ref-7],
- Expectations that development by a future licensee of site-specific operating procedures that are relevant to the use of HMIs and to transfers between HMI locations in accident scenarios will be in line with HF best practice – see 'assumptive' HFSPC 6 in GDA PCSR Chapter 27:HF,
- UK HMI user group assumptions and typical expectations as described in [Ref-7],
- Expectations for future work related to HMI design and substantiation by a future licensee that builds on the GDA work, as explained in Section 21.2.2 of this chapter,
- Expectations for competency and training of operators on use of HMIs in line with HF best practice – see 'assumptive' HFSPC 7 in GDA PCSR Chapter 27:HF, and
- Future licensee adoption of any LCOs developed in GDA and presented in other chapters of this GDA PCSR that affect functionality requirements of HMIs on operating ABWR stations.

In addition to the mainly generic considerations above, the individual task analyses performed in GDA to assess usability of HMIs have in many cases made HF related assumptions that are identified in the GDA documents that support PCSR Chapter 27:HF.

There are no specific LCOs of HMIs, but there are LCOs for the C&I systems that the HMI are considered to be part of. For discussion of those LCOs see GDA PCSR Chapter 14.12:Assumptions, LCOs.

21.10 Summary of ALARP Justification

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

PCSR Chapter 28:ALARP Evaluation - presents the high level approach taken for demonstrating ALARP across all aspects of the design and operation. It presents an overview of how the UK ABWR design has evolved, the further options that have been considered across all technical areas resulting 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-17] and SCDM [Ref-13].

For the HMI systems topic area, ALARP consists of the following steps:

- Establishing the role of the UK ABWR HMIs in controlling risks to safety,
- Undertaking a gap analysis of the reference J-ABWR HMI design to UK Relevant Good Practice (RGP),
- Undertaking an options analysis for closing gaps, and
- Selecting and implementing the optimal ALARP solution.

21.10.1 Key Risks Related to HMIs

PCSR Chapter 14 demonstrates that the C&I, to which the HMIs link, plays a significant role in "defence in depth" for the UK ABWR safety case. Obviously each HMI as hardware forms part of the whole of the C&I system to which that HMI is linked, either contributing to the support of the safety requirements of the C&I system or at least not detracting from it.

Specifically, in the HMI topic area, the key risks which are identified, understood and managed in order to justify the design is ALARP, are:

- Possibility of HMI inducing human error: HMIs fail to support the required human performance, including achievability and required human reliability of claims. The risk is that the HMIs lack a usable design and contain features that are more likely to lead to human errors during operations and maintenance. These human errors then have the potential to either contribute to the initiation of faults or events, or lead to the failure of a required safety measure when it is required to mitigate a fault or event (either through SSC unavailability or failed human action). This leads to increased risk of loss of the FSFs, and
- Non-availability of an HMI when required: The risk is that components of HMI do not match the reliability and diversity requirements of the C&I and other SSCs to which they are linked and the HMI is not suitably isolated, meaning that the HMI might introduce faults within the C&I system that decrease system availability and reliability to lower than that required.

21.10.2 RGP and Gap Analysis of the Reference Plant Design

In terms of hardware, as per the C&I that the HMIs interface to (as described in greater detail in PCSR Chapter 14), for UK Nuclear Power Plants (NPPs) key aspects of RGP relate to the independence required between systems, in addition to other important expectations such as standards and application of the single failure criterion. The independence requirements are summarised as follows:

- High standards of segregation and separation of the three main systems (i.e. PCntlS, SSLC and HWBS),
- High standards of electrical isolation,
- Where data networks are used, high standards of data isolation with strict one-way communication enforced by data-diodes in connections to the Class 1 system,
- Each of the three main C&I systems is based on platforms employing diverse technology, and
- A strong expectation that at least one system would employ simple hardwired technology.

The above is not a comprehensive list of requirements for independence, which are covered in more detail in PCSR Chapter 14 and in its supporting BSCs and TRs (as per its reference section). Similarly PCSR Chapter 14 and its supporting references also provide more information for safety claims.

In terms of the HF aspects of the HMIs, the RGP relates to their design to ensure human performance is supported and human error is minimised.

Generally speaking, the HMIs as designed for the J-ABWR reference plant were assumed, unless specifically identified as otherwise in Section 21.2.2, to be optimised in terms of their ability to support effective and safe operations to the levels of human performance required. Many years of operating experience and design evolution to improve the ability of the human users to monitor and control the plant are demonstrated through Operational Experience (OPEX). This OPEX was assessed by UK HF SQEP (Suitably Qualified and Experienced Personnel) at the start of GDA, as reported in the BAR [Ref-18].

However, due to the differences in UK regulatory expectations, UK user population and UK Concept of Operations (as captured in the HF COR [Ref-7]), gaps in the HMI design were identified that related to the linked SSC design and/or the UK user group as follows:

The gaps in C&I design aspects of the HMI systems also relate to the gaps identified for the reference plant C&I systems design, as compared against UK RGP. As per PCSR Chapter 14, these are as follows:

- Lack of diversity between the PCntlS and the SSLC,
- Use of two-way data communication networks between the SSLC and the lower safety class PCntlS and use of two-way communication with NPP data networks that are not involved in plant control, and
- Lack of automation in many of the manual hardwired backup functions.

21.10.3 Options Analysis to Address the Gaps

The most significant options analysis undertaken within the C&I topic area regarding the design of the C&I systems design (and therefore clearly impacting the hardware selection and design for the associated HMIs) related to the diversity of technology and segregation of lower Category and Class systems from the Cat./Class A1 systems of the SSLC. This involved consideration of four platform technology options, along with other options assessments, described in detail within the ALARP summary of PCSR Chapter 14. Of most significance to the HMI, were the following conclusions of the options analysis:

- To ensure the diversity from the PCntlS, a decision was taken to avoid the combination of microprocessors and software and instead Field Programmable Gate Array (FPGA) technology was chosen for the new Class 1 FPGA SSLC platform,
- To separate the Category B and C functions from the SSLC they were implemented in a new Class 2 system (i.e. the SACS),
- To implement manual direct hardwired monitoring and control functions to Class 1 systems. This supports manual action claims within the DSA faults relating to design basis faults with CCF of the SSLC, and
- To ensure risks from the reference design and new hardwired system were ALARP, the decision was made to modify the existing J-ABWR manual controls into an overall integrated Category A, Class 2 system. This system is the Hardwired Backup System (HWBS) and includes additional automation of safety systems that were previously only manually-actuated in the reference plant design (see below regarding Allocation of Function (AoF) analysis options).

The impact of this technology and architecture options analysis on the HMI design itself had potentially negative impact on the usability of the design as follows:

- The FPGA platform, whilst providing the required diversity and ability to perform more stringent C&I system design verification, created limitations within the HMI design as compared to the modern touchscreen interface of the reference plant design.
- The SACS required a completely new HMI for functions that had previously been logically grouped (for operability purposes) with the SSLC functions that they supported.
- The manual actions claimed during CCF of SSLC concurrent with a set of design basis faults required a new HMI, which was implemented as the SAuxP (as described in Section 21.4).

The HWBS required conventional HMI which are independent from the SSLC, separate from the Class 1 SAuxP hardwired panel; this was implemented as the HWBP (as described in Section 21.4).

21.10.4 Implementing an Optimised Solution for UK ABWR HMI Systems

Through the optioneering exercises and other design activities described above and in related supporting references, the design of the modified and new HMIs was able to consider usability as a key requirement throughout. Options chosen were considered those that would reduce risk of human

error to ALARP, given the constraints on the design from the C&I technology selected to meet important UK safety requirements.

The following features highlight the optimised solution chosen, including the use of HF-led basic design philosophies to ensure adequate consideration of the user in each HMI design:

- Where possible, proven and optimised reference plant HMI design was maintained within UK ABWR,
- Where changes to HMIs or new HMIs needed to be designed, the basic design rules (design philosophy and style guide) from the J-ABWR reference plant design were applied to ensure consistency in the look and "feel" of new HMIs with existing plant,
- Consideration was given to required functionality and tasks performed on new or changed HMIs with the resulting inventory and layout reflecting the HMI use, particularly for key tasks important to safety,
- Design of the new Class 1 SSLC HMI reflects as much consistency as possible with the existing Class 3 touchscreen reference plant design to allow smooth transition to its operation if necessary,
- Location of the new SACS HMI on the MCC is separated from the SSLC and placed at the end on one side, leaving the main sections of the MCC identical in position and orientation to the reference plant design (particularly important for power operation, start-up, hot/cold shutdown and refuelling outage and viewing the WDP effectively),
- Location of the SAuxP and HWBP within the MCR is optimised to take account of flow of movement and expected frequency of use, and
- Design of the new hardwired backup panels (SAuxP, HWBP and BBCP) layout at basic design level takes into account the functionality of each panel and expected tasks to be conducted there.

21.10.5 Summary of GDA ALARP Position and Justification

Hitachi-GE has undertaken a comprehensive programme of work during GDA, from both the hardware design and the HF engineering and design support points of view, to optimise the design of the UK ABWR HMIs. This work is based on an in-depth gap analysis by comparing UK relevant good practice for NPP C&I systems and for HF consideration within design against the reference design for the J-ABWR. Where gaps were found, design changes were proposed and have been implemented at a level of detail consistent with a GDA PCSR stage of a project. Generally speaking the hardware changes and options were driven by the related C&I systems linked to the HMI. Where design changes from the C&I systems and other SSCs have impacted on HMIs, options have been duly considered to optimise the HMI within the constraints of the other changes.

HMIs clearly play a pivotal role in the safety of the plant, especially ensuring the achievability of the claimed manual actions within the DSA and PSA, and thus the ability to maintain the FSFs. This chapter and its supporting references have shown that the design of the UK ABWR HMIs ensures that the risks to plant safety from either failures of the HMI hardware or failures in the humans using the HMI, i.e. potential human errors caused by the HMI design itself, have been reduced to ALARP.

21.11 Conclusions

This chapter and it's supporting documents defines for GDA the scope of HMIs that are required to monitor the safe operating parameters and control the systems necessary to operate the UK ABWR safely and efficiently, providing sufficient defence in depth under normal and fault conditions. It specifies the SFCs and SPCs made on these HMIs, and identifies where the arguments that support these claims are presented.

The scope of HMIs in this chapter reflects in its design the changes to the C&I architecture compared with the J-ABWR design that have resulted from specific UK regulatory requirements, in particular response to severe accidents; anticipated end-user requirements; application of modern standards; and from the analysis of faults and allocation of function conducted in GDA. In addition, the results of the V&V programme conducted by Hitachi-GE during GDA have helped to ensure that the current design supports the necessary actions and reliability of human performance required from the claimed HMI by operators.

This chapter provides a link between, and takes account of the design maturity within the C&I (Chapter14), and for integration of the concept of operations (Chapter 30) and HFs in design and the substantiation of control room HBSCs (Chapter 27).

In this way, it has been demonstrated that the design, scope and intended use of the HMIs for UK ABWR meets the principles of managing risks ALARP, as far as is possible given the level of design maturity available for GDA.

21.12 References

[Ref-1] Hitachi-GE Nuclear Energy, Ltd., "Basis of Safety Cases on Overall Human-machine Interface", GA91-9201-0002-00109 (3E-GD-A0166) Rev.1, April 2017.

[Ref-2] Hitachi-GE Nuclear Energy, Ltd., "Basis of Safety Cases on Main Control Room Human-machine Interface", GA91-9201-0002-00060 (3E-GD-A0029) Rev.2, April 2017.

[Ref-3] Hitachi-GE Nuclear Energy, Ltd., "Basis of Safety Cases on Remote Shutdown System Human-machine Interface", GA91-9201-0002-00061 (3E-GD-A0030) Rev.2, April 2017.

[Ref-4] Hitachi-GE Nuclear Energy, Ltd., "Basis of Safety Cases on Backup Building Human-machine Interface", GA91-9201-0002-00062 (3E-GD-A0031) Rev.2, May 2017.

[Ref-5] Hitachi-GE Nuclear Energy, Ltd., "Basis of Safety Cases on Control and Instrumentation Architecture", GA91-9201-0002-00022 (3D-GD-A0001) Rev.4, June 2017.

[Ref-6] Hitachi-GE Nuclear Energy, Ltd., "Allocation of Function Report", GA91-9201-0001-00040 (HFE-GD-0063) Rev.D, September 2016.

[Ref-7] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Concept of Operations Report", GA91-9201-0001-00034 (HFE-GD-0060) Rev.E, April 2017.

[Ref-8] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Fault Assessment", GA91-9201-0001-00022 (UE-GD-0071) Rev.6, July 2017.

[Ref-9] Hitachi-GE Nuclear Energy, Ltd., "Human-Based Safety Claims Report", GA91-9201-0001-00043 (HFE-GD-0064) Rev.D, July 2017.

[Ref-10] Hitachi-GE Nuclear Energy, Ltd., "Human Reliability Analysis Report", GA91-9201-0001-00041 (HFE-GD-0066) Rev.E, January 2017.

[Ref-11] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Engineering Specification", GA91-9201-0001-00037 (HFD-GD-0001) Rev.D, January 2017.

[Ref-12] Vacant Number

[Ref-13] Hitachi-GE Nuclear Energy, Ltd., "GDA Safety Case Development Manual", GA10-0511-0006-00001 (XD-GD-0036) Rev.3, June 2017.

[Ref-14] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Design and Engineering Report", GA91-9201-0001-00039 (HFE-GD-0065) Rev.B, January 2016.

[Ref-15] Hitachi-GE Nuclear Energy, Ltd., "Alarm Processing and Presentation Strategy", GA91-9201-0003-01919 (HFE-GD-0474) Rev.A, March 2017.

[Ref-16] Hitachi-GE Nuclear Energy, Ltd., "Strategy of Use for HMIs", GA91-9201-0003-01462 (HFE-GD-0360) Rev.B, August 2017.

[Ref-17] Hitachi-GE Nuclear Energy, Ltd, "GDA ALARP Methodology", GA10-0511-0004-00001 (XD-GD-0037) Rev.1, November 2015.

[Ref-18] Hitachi-GE Nuclear Energy, Ltd., "Baseline Human Factors Assessment Report", GA91-9201-0001-00032 (HFE-GD-0068) Rev.B, August 2015.

[Ref-19] Hitachi-GE Nuclear Energy, Ltd., ”Human Factors Verification and Validation Plan”, GA91-9201-0003-01353 (HFE-GD-0232), Rev A, October 2016.

[Ref-20] Hitachi-GE Nuclear Energy, Ltd., “List of Safety Category and Class for UK ABWR”, GA91-9201-0003-00266 (AE-GD-0224), Rev.4, August 2017.

[Ref-21] Hitachi-GE Nuclear Energy, Ltd., ”Basis of Safety Cases on Safety System Logic and Control System”, GA91-9201-0002-00073 (3D-GD-A0008), Rev 4, June 2017.

[Ref-22] Hitachi-GE Nuclear Energy, Ltd., “Basis of Safety Cases on Severe Accident C&I System”, GA91-9201-0002-00110 (3D-GD-A0015), Rev.3, May 2017.

Appendix A: Safety Functional Claims

A1: Safety Functional Claim Table

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
1	1	Control of Reactivity	1-1	Functions to prevent excessive reactivity insertion	-	-	-	-	No Claim on HMI	-	-
2			1-2	Functions to maintain core geometry	-	-	-	-	No Claim on HMI	-	-
3			1-3	Emergency shutdown of the reactor	FS1	RPS Scram (A1)	Fault Conditions	MCR HMI SFC 1-3.1	The HMI for the SSLC provides indicators and controls to perform and monitor an emergency shutdown of the reactor.	A	1
4			1-4	Functions to maintain sub-criticality	-	-	-	-	No Claims on HMI	-	-
5			1-5	Function of alternative reactivity control	FS2 FS3 FS4 FS5	SLC (A2) ATWS-RPT (A2) FWSTP (A2) ARI (A2)	Fault Conditions	MCR HMI SFC 1-5.1	The HMI for the HWBS provides indicators and controls for the equipment and systems for alternative means to control reactivity.	A	2
6					-	-	Fault Conditions	MCR HMI SFC 1-5.2	The HMI for the PCntlS provides indicators for the equipment and systems for alternative means to control reactivity.	-	3
7			1-6	Functions to circulate reactor coolant (functions to control reactivity of the core in normal operational states)	-	-	Normal Conditions	MCR HMI SFC 1-6.1	The HMI for the PCntlS provides indicators and controls for the equipment and systems to control reactivity during power operation, start-up, and hot/cold shutdown by circulating reactor coolant.	-	3
8					-	-	Normal Conditions	MCR HMI SFC 1-6.2	The HMI for the ACS provides indicators for the equipment and systems to control reactivity during power operation, start-up, and hot/cold shutdown.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
9			1-7	Functions to plant instrument and control (except for safety protection function) (Functions to control reactivity of the core in normal operational states)	-	-	Normal Conditions	MCR HMI SFC 1-7.1	The HMI for the PCntlS provides indicators and controls for the equipment and systems to control the reactivity of the core during power operation.	-	3
10			1-8	Functions to suppress reactor power increase with other system	-	-	Fault Conditions	MCR HMI SFC 1-8.1	The HMI for the PCntlS provides indicators and controls for the equipment and systems to suppress inappropriate reactor power increase.	-	3
11			1-9	Functions to maintain sub-criticality of spent fuel outside the reactor coolant system	-	-	-	-	No Claim on HMI	-	-
12			1-10	Functions to maintain sub-criticality of spent fuel during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	No Claim on HMI	-	-
13	2	Fuel Cooling	2-1	Functions to cool reactor core	FS6 FS7 FS9 FS10	RCIC(A1) HPCF(A1) ADS(A1) LPFL(A1)	Fault Conditions	MCR HMI SFC 2-1.1	The HMI for the SSLC provides indicators and controls for the equipment and systems to cool reactor core.	A	1
							Fault Conditions	MCR HMI SFC 2-1.2	The SAuxP provides indicators and controls for the equipment and systems to cool reactor core.	A	1
14					-	-	Fault Conditions	MCR HMI SFC 2-1.3	The HMI for the other C&I provides indicators and controls for the equipment and systems to cool reactor core.	C	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
15			2-2	Function of alternative fuel cooling	FS11 FS12	RDCF(A2) FLSS(A2)	Fault Conditions	MCR HMI SFC 2-2.1	The HMI for the HWBS provides indicators and controls for the equipment and systems to inject water into the reactor pressure vessel as alternative measure.	A	2
16					-	-	Fault Conditions	B/B HMI SFC 2-2.1	The HMI for the SA C&I provides indicators and controls for the equipment and systems to inject water into the reactor pressure vessel as alternative measure.	B	2
17			2-3	Function to make up reactor coolant with other system	-	-	Fault Conditions	MCR HMI SFC 2-3.1	The HMI for the ACS provides indicators for the equipment and systems to make up reactor coolant with other system.	-	3
18					-	-	Fault Conditions	MCR HMI SFC 2-3.2	The HMI for the other C&I provides indicators and controls for the equipment and systems to make up reactor coolant, if available.	C	3
19			2-4	Function to cool spent fuel outside the reactor coolant system	-	-	Normal /Fault Conditions	MCR HMI SFC 2-4.1	The HMI for the SSLC provides indicators and controls for the equipment and systems to cool spent fuel pool.	A	1
20			2-5	Functions to make up water for spent fuel pool	-	-	Fault Conditions	MCR HMI SFC 2-5.1	The HMI for the HWBS provides indicators and controls for the equipment and systems to make up water for spent fuel pool.	A	2
21					-	-	Fault Conditions	MCR HMI SFC 2-5.2	The HMI for the SACS provides indicators and controls for the equipment and systems to make up water for spent fuel pool.	C	3
22					-	-	Fault Conditions	MCR HMI SFC 2-5.3	The HMI for the ACS provides indicators and controls for the equipment and systems to make up water for spent fuel pool.	-	3
23							Fault Conditions	MCR HMI SFC 2-5.4	The HMI for the other C&I provides indicators and controls for the equipment and the systems to make up water for spent fuel pool.	-	3
24					-	-	Fault Conditions	B/B HMI SFC 2-5.1	The HMI for the SA C&I provides indicators and controls for the equipment and systems to make up water for spent fuel pool.	B	2

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
25			2-6	Functions to maintain spent fuel temperature during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	No Claim on HMI	-	-
26	3	Long term heat removal	3-1	Functions to remove residual heat after shutdown	FS13 FS14	SRV –Manual depressurization– (A1) RHR(A1)	Fault Conditions	MCR HMI SFC 3-1.1	The HMI for the SSLC provides indicators and controls for the equipment and systems to remove heat from the reactor core.	A	1
							Fault Conditions	MCR HMI SFC 3-1.2	The SAuxP provides indicators and controls for the equipment and systems to remove heat from the reactor core.	A	1
27			3-2	Function of alternative containment cooling and decay heat removal	FS15	Containment venting(A2)	Fault Conditions	MCR HMI SFC 3-2.1	The HMI for the HWBS provides indicators and controls for the equipment and systems to remove residual heat as alternative measure.	A	2
					-	-	Fault Conditions	B/B HMI SFC 3-2.1	The HMI for the SA C&I provides indicators and controls for the equipment and systems to remove residual heat as alternative measure.	B	2
29	4	Confinement/Containment of radioactive materials	4-1	Functions to form reactor coolant pressure boundary	-	-	-	-	No Claim on HMI	-	-
30			4-2	Functions to prevent overpressure within the reactor coolant pressure boundary	-	-	-	-	No Claim on HMI	-	-
31			4-3	Functions to contain reactor coolant outside the RCPB	-	-	Normal /Fault Conditions	MCR HMI SFC 4-3.1	The HMI for the ACS provides indicators for the systems to contain reactor coolant.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
32			4-4	Functions to contain radioactive material	-	-	-	-	No Claim on HMI	-	-
33			4-5	Functions to reseat safety valves and relief valves	-	-	-	-	No Claim on HMI	-	-
34			4-6	Functions to mitigate reactor pressure increase with other system (other than No.4-2)	-	-	Fault Conditions	MCR HMI SFC 4-6.1	The HMI for the other C&I provides indicators and controls for the equipment and systems to mitigate reactor pressure increase with other system.	C	3
35					-	-	Fault Conditions	MCR HMI SFC 4-6.2	The HMI for the PCntlS provides indicators for the equipment and systems to mitigate reactor pressure increase with other system.	-	3
36			4-7	Functions to confine radioactive materials, shield radiation, and reduce radioactive release	FS16 FS17	MSIV(A1) PCIS(A1)	Fault Conditions	MCR HMI SFC 4-7.1	The HMI for the SSLC provides indicators and controls for the equipment and systems to confine radioactive materials, shield of radiation and to reduce radioactive release.	A	1
37					-	-	Fault Conditions	MCR HMI SFC 4-7.2	The HMI for the SSLC provides indicators and controls for the equipment and systems to suppress PCV atmosphere pressure and to remove fission products.	B	2
38					-	-	Fault Conditions	MCR HMI SFC 4-7.3	The HMI for the SACS provides indicators and controls for the equipment and systems to confine radioactive materials and to reduce radioactive release.	B	2
39					Part of FS17	Part of PCIS(A1)	Fault Conditions	MCR HMI SFC 4-7.4	The SAuxP provides indicators and controls for the isolation valves to confine radioactive materials.	A	1
40					-	-	Normal Conditions	MCR HMI SFC 4-7.5	The HMI for the ACS provides indicators for the equipment and systems to confine radioactive materials.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
41			4-8	Functions to minimise the release of radioactive gases	-	-	Fault Conditions	MCR HMI SFC 4-8.1	The HMI for the SACS provides indicators and controls for the equipment and systems to minimise the release of radioactive gases.	B	2
42							Fault Conditions	B/B HMI SFC 4-8.1	The HMI for the SA C&I provides indicators and controls for the equipment and systems to minimise the release of radioactive gases.	B	2
43			4-9	Functions to contain radioactive materials in the event of a severe accident	-	-	Fault Conditions	B/B HMI SFC 4-9.1	The HMI for the SA C&I provides indicators and controls for the equipment and systems to contain radioactive materials in the event of a severe accident.	B	2/3
44					-	-	Fault Conditions	MCR HMI SFC 4-9.1	The HMI for the SA C&I provides indicators and controls for the equipment and systems to contain radioactive materials in the event of a severe accident.	B	2/3
45			4-10	Functions to prevent the dispersion of fission products into reactor coolant and spent fuel pool	-	-	-	-	No Claim on HMI	-	-
46			4-11	Functions to store the radioactive materials as gaseous waste	-	-	Normal Conditions	MCR HMI SFC 4-11.1	The HMI for the ACS provides indicators and controls for the equipment and systems to store the radioactive materials as gaseous waste.	-	3
47					-	-	Fault Conditions	MCR HMI SFC 4-11.2	The HMI for the SACS provides indicators and controls for the equipment and systems to store the radioactive material as gaseous waste.	B	2
48			4-12	Functions to store the radioactive materials as liquid wastes	-	-	Normal Conditions	MCR HMI SFC 4-12.1	The HMI for other C&I provides some selected information for the systems to store the radioactive materials as solid wastes.	C	3
49					-	-	Normal Conditions	MCR HMI SFC 4-12.2	The HMI for the ACS provides indicators for the equipment and systems to store the radioactive materials as liquid wastes and to transfer to the LWMS.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
50					-	-	Normal Conditions	Rw/B CR HMI SFC 4-12.1	The HMI for the other C&I provides indicators and controls for the systems to store the radioactive materials as liquid wastes.	C	3
51			4-13	Functions to store the radioactive materials as solid wastes	-	-	Normal Conditions	MCR HMI SFC 4-13.1	The HMI for other C&I provides some selected information for the systems to store the radioactive materials as solid wastes.	C	3
52					-	-	Normal Conditions	Rw/B CR HMI SFC 4-13.1	The HMI for other C&I provides indicator and controls for the systems to store the radioactive materials as solid wastes.	C	3
53					-	-	Normal Conditions	Local HMI SFC 4-13.1	The HMI for the other C&I provides indicators and controls for the systems to store the radioactive material as solid waste at the control area in the ILW store.	C	3
54					-	-	Normal Conditions	Local HMI SFC 4-13.2	The HMI for the other C&I provides indicators and controls for the systems to store the radioactive material as solid waste at the control area in SWF building.	C	3
55			4-14	Functions to provide containment barrier during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	No Claim on HMI	-	-
56			4-15	Unused number	-	-	-	-	No Claim on HMI	-	-
57			4-16	Functions to provide radiation shield during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	No Claim on HMI	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
58			4-17	Functions to maintain PCV atmosphere in an inert state for preventing hydrogen combustion	-	-	Normal /Fault Conditions	MCR HMI SFC 4-17.1	The HMI for the ACS provides indicators and controls for the systems to maintain PCV atmosphere in an inert state for preventing hydrogen combustion.	-	3
59	5	Others	5-1	Functions to generate actuation signals for the engineered safety features and reactor shutdown systems	-	-	Fault Conditions	MCR HMI SFC 5-1.1	The HMI for the SSLC provides information of the actuation signals for engineered safety features and reactor shutdown.	A	1
					-	-	Fault Conditions	MCR HMI SFC 5-1.2	The HMI for the HWBS provides information of the actuation signals for engineered safety features and reactor shutdown.	A	2
					-	-	Fault Conditions	MCR HMI SFC 5-1.3	The HMI for the SACS provides information of the actuation signals for engineered safety features and reactor shutdown.	B	2
60			5-2	Supporting functions especially important to safety	-	-	Fault Conditions	MCR HMI SFC 5-2.1	The HMI for the SSLC provides indicators and controls for the supporting functions especially important to safety.	A	1
61					-	-	Fault Conditions	MCR HMI SFC 5-2.2	The HMI for the other C&I provides indicators and controls for the supporting functions especially important to safety.	A	1
62					-	-	Normal /Fault Conditions	Local HMI SFC 5-2.1	The HMI for the other C&I provides indicators and controls for the supporting functions especially important to safety.	A	1
63			5-3	Function of alternative supporting system	-	-	Fault Conditions	MCR HMI SFC 5-3.1	The HMI for the HWBS provides indicators and controls for the supporting functions for alternative measures.	A	2
64					-	-	Fault Conditions	MCR HMI SFC 5-3.2	The HMI for the other provides indicators and controls for the supporting functions for alternative measures.	B	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
65					-	-	Fault Conditions	MCR HMI SFC 5-3.3	The HMI for the SACS provides indicators and controls for the supporting functions for alternative measures.	C	3
66					-	-	Fault Conditions	B/B HMI SFC 5-3.1	The HMI for the SA C&I provides indicators and controls for the supporting functions for alternative measures.	B	2
67			5-4	Monitoring functions of plant conditions to support operator actions	-	-	Normal /Fault Conditions	MCR HMI SFC 5-4.1	The HMI for the SSLC provides information to monitor the key plant conditions in the event of a fault condition.	B	2
68					-	-	Fault Conditions	MCR HMI SFC 5-4.2	The HMI for the HWBS provides information to monitor the key plant conditions in the event of a fault condition.	B	2
69					-	-	Normal /Fault Conditions	MCR HMI SFC 5-4.3	The HMI for the SACS provides information to monitor the key plant conditions in the event of a fault condition.	B	2
70					-	-	Fault Conditions	MCR HMI SFC 5-4.4	The HMI for the SAuxP provides information to monitor the key plant conditions in the event of a fault condition.	B	2
71					-	-	Normal /Fault Conditions	MCR HMI SFC 5-4.5	The HMI for the ACS provides information to monitor the key plant conditions in the event of a fault condition.	-	3
72					-	-	Fault Conditions	B/B HMI SFC 5-4.1	The HMI for the SA C&I provides information to monitor the key plant conditions in the event of a fault condition.	B	2
73			5-5	Functions to shut down safely from outside the control room	-	-	Fault Conditions	RSS HMI SFC 5-5.1	The RSP provides indicators and controls to bring safe shutdown from outside the control room.	A	1

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
74			5-6	Functions to handle fuel and heavy equipment safely	-	-	Normal Conditions	Local HMI SFC 5-6.1	The HMI for the other C&I provides indicators and controls to handle fuel safely.	C	3
75			5-7	Functions to limit the effect of hazard	-	-	Normal Conditions	MCR HMI SFC 5.7-1	The HMI for the other C&I provides information to the operator on the status of watertight and/or fire resistant doors.	B	2
76			5-8	Functions to clean up reactor coolant	-	-	Normal Conditions	MCR HMI SFC 5-8.1	The HMI for the ACS provides indicators for the equipment and systems to clean up reactor coolant.	-	3
77					-	-	Normal Conditions	Local HMI SFC 5-8.1	The HMI for the other C&I provides indicators and controls for the equipment and systems to clean up reactor coolant.	C	3
78			5-9	Functions to clean up water except for reactor coolant	-	-	Normal Conditions	MCR HMI SFC 5-9.1	The HMI for the SACS provides indicators and controls for the equipment and systems to clean up water except for reactor coolant..	C	3
79					-	-	Normal Conditions	Local HMI SFC 5-9.1	The HMI for the other C&I provides indicators and controls for the equipment and systems to clean up water except for reactor coolant.	C	3
80					-	-	Normal Conditions	Rw/B CR HMI SFC 5-9.1	The HMI for the Other C&I provides indicators and controls for the LWMS to clean up water except for reactor coolant.	C	3
81			5-10	Functions to supply electric power (except for emergency supply)	-	-	Normal Conditions	MCR HMI SFC 5-10.1	The HMI for the PCntlS provides indictors and controls for the equipment and systems to supply electric power.	-	3
82					-	-	Normal Conditions	MCR HMI SFC 5-10.2	The HMI for the ACS provides indictors for the equipment and systems to supply electric power.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
83			5-11	Supporting functions to supply power (except for emergency supply)	-	-	Normal Conditions	MCR HMI SFC 5-11.1	The HMI for the ACS provides indicators for the key supporting functions to supply power.	-	3
84					-	-	Normal Conditions	MCR HMI SFC 5-11.2	The HMI for the other C&I provides indicators and controls for the equipment and systems to support supplying electrical power.	C	3
85			5-12	Supporting functions for management of normal operation	-	-	Normal Conditions	MCR HMI SFC 5-12.1	The HMI for the PCS provides information for the reactor plant control functions and systems.	-	3
86			5-13	Auxiliary functions for plant operation	-	-	Normal Conditions	MCR HMI SFC 5-13.1	The HMI for the SACS provides indicators and controls for auxiliary functions for plant operation.	C	3
87					-	-	Normal Conditions	MCR HMI SFC 5-13.2	The HMI for the ACS provides indicators and controls for auxiliary functions for plant operation.	-	3
88			5-14	Supporting functions for on-site emergency preparedness	-	-	Fault Conditions	MCR HMI SFC 5-14.1	The HMI for the other C&I provides indicators to monitor and assess radiation and contamination levels at site boundary under fault conditions.	C	3
89							Fault Conditions	MCR HMI SFC 5-14.2	The HMI for the ERF provides indicators to monitor plant conditions during fault condition.	C	3
90							Fault Conditions	MCR HMI SFC 5-14.3	The HMI for the other C&I provides indicators and controls for fire protection system.	C	3
91			5-15	Functions to control hydrogen concentration in fault conditions	-	-	-	-	No Claim on HMI	-	-
92			5-16	Functions to provide handling and retrievability during processes of spent fuel removal from cask pit to storage area and during interim storage period	-	-	-	-	No Claim on HMI	-	-

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
93			5-17	Function to provide structural support to SSCs	-	-	-	-	No Claim on HMI	-	-
94			5-18	Function to maintain internal building environment appropriate for SSC	-	-	Normal /Fault Conditions	MCR HMI SFC 5-18.1	The HMI for the SSLC provides indicators and controls to maintain internal building environment.	A	1
95					-	-	Normal /Fault Conditions	MCR HMI SFC 5-18.2	The HMI for the HWBS provides indicators and controls to maintain internal building environment.	A	2
96					-	-	Normal Conditions	MCR HMI SFC 5-18.3	The HMI for the ACS provides indicators to maintain internal building environment.	-	3
97					-	-	Fault Conditions	MCR HMI SFC 5-18.4	The HMI for the SACS provides indicators and controls to maintain internal building environment.	B	2
98					-	-	Normal /Fault Conditions	Local HMI SFC 5-18.1	The HMI for the other C&I provides indicators and controls to maintain internal building environment.	A	1
99					-	-	Fault Conditions	B/B HMI SFC 5-18.1	The HMI for the SA C&I provides indicators and controls to maintain internal building environment.	B	2
100			5-19	Monitoring functions of radioactive discharge to the environment	-	-	Fault Conditions	MCR HMI SFC 5-19.1	The HMI for the other C&I provides information for monitoring radioactive discharge to the environment. .	C	3
101							Fault Conditions	B/B HMI SFC 5-18.1	The HMI for the SA C&I provides information for monitoring radioactive discharge to the environment. .	C	3
102			5-20	Functions to maintain availability of CRs hydraulic insertion function and to recover CRs to normal unlatched state after rapid insertion	-	-	Normal Condition	MCR HMI SFC 5-20.1-	The HMI for the ACS provides indicators and controls for the equipment and the systems to support the deliver of reactor rapid shutdown.	-	3

	Top Claim for Control and Instrumentation System						Safety Functional Claims for Human-machine Interface (SFC)				
	Fundamental Safety Function (FSF)		High Level Safety Function (HLSF)		Fault Schedule(Bounding Fault)						
	PCSR Ch.5 Section 6 Table 5.6-1: High Level Safety Functions in UK ABWR		PCSR Ch.5 Section 6 Table 5.6-1: High level Safety Functions in UK ABWR		Topic Report on Fault Assessment Table.4.2-1 Fault Schedule (UE-GD-0071) Appendix A2 (Definition of FSs)		State	Claim ID	Claim Contents	Cat.	Class
103							Normal Condition	MCR HMI SFC 5-20.2	The HMI for the PCntlS provides indicators and controls for the equipment and the systems to recover of CRs to normal unlatched insertion.	-	3
104			5-21	Function to retain water for provision of radiation shield during the refuelling process	-	-	-	-	No Claim on HMI	-	-
105			5-22	Function to limit deceleration loading to canister containment boundary during credible cask drop faults	-	-	-	-	No Claim on HMI	-	-
106			5-23	Monitoring functions of occupational and public radiation exposures	-	-	Normal /Fault Condition	MCR HMI SFC 5-23.1	The HMI for the other C&I provides monitoring functions of occupational and public radiation exposures.	C	3
107			5-24	Functions to limit worker access into high dose area	-	-	-	-	No Claim on HMI	-	-

A2: Front System and Initiating Fault/Event ID Linkage Table

*Refer to Appendix A1 for the relevant SFCs

No.*	Front System	Initiating Fault / Event ID From Topic Report of Fault Assessment [Ref-8]	Remarks
FS1	RPS Scram (A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2.2, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.3, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 5.2.1, 5.3.1, 5.3.4, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.1.2,	
FS2	SLC(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2.2, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.2, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.4.1, 11.5, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	
FS3	ATWS-RPT(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.4, 1.5, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.4.1, 4.2.5.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.4.1, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	
FS4	FWSTP(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.4, 1.5, 1.7, 1.8, 2.1, 2.2, 2.3, 4.2.3.1, 4.2.4.1, 4.2.5.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 1.4.2, 2.1.2, 11.3, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	
FS5	ARI(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.1, 4.2.2, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.2, 11.3, 11.4.1, 11.5, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1	

*Refer to Appendix A1 for the relevant SFCs

No.*	Front System	Initiating Fault / Event ID From Topic Report of Fault Assessment [Ref-8]	Remarks
FS6	RCIC(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.3, 10.1, 10.2, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 2.1.2, 11.1, 11.2, 11.3, 11.5, 11.8.1, 11.10.1, 11.11.1,, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.6, 18.1.1, 18.2.1, 18.3.1	
FS7	HPCF(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.2, 5.1.3, 5.2.2, 5.2.3, 5.3.2, 5.3.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 2.1.2, 11.1, 11.2, 11.3, 11.4, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.5.1.1, 13.5.1.2, 13.5.1.3 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1.1, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.3, 13.17.4, 13.18.1, 13.18.2, 13.18.3, 13.18.4, 11.4.2.1, 11.4.2.2, 11.4.2.3, 17.1.2.1, 17.1.2.2, 17.1.2.4, 17.2.2.1, 17.2.2.2, 17.2.2.4, 17.3.2.1, 17.3.2.2, 17.3.2.4, 17.4.2.1, 17.4.2.2, 17.4.2.3, 17.4.2.4, 17.4.2.5, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.3, 17.5.2.4, 17.5.2.5, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.3, 18.1.2.4, 18.1.2.5, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.3, 18.2.2.4, 18.2.2.5, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6	
FS8	SRV -Safety valve function- (A1)	No claim	
FS9	ADS(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.2, 5.2.2, 5.3.2, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.3, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1	

*Refer to Appendix A1 for the relevant SFCs

No.*	Front System	Initiating Fault / Event ID From Topic Report of Fault Assessment [Ref-8]	Remarks
FS10	LPFL(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.2.2, 5.3.2, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.2, 11.3, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.2, 13.3.6, 13.5.1.1, 13.5.1.2, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.6, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1,1, 13. 8.1,2, 13. 8.1,3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.6, 13.18.1, 13.18.2, 13.18.6, 17.1.2.1, 17.1.2.2, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.6	Requirements as LPFL (B2) are below: 1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.2, 5.1.2, 5.2.2, 5.3.2, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.3, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.5.1.2, 13.5.1.6, 13.5.1.7 Remark: Requirements as LPFL (A1) are below: 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 11.2, 13.3.1, 13.3.2, 13.3.6, 13.5.1.1, 13.5.2.1, 13.5.2.2, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.6, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1,1, 13. 8.1,2, 13. 8.1,3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.6, 13.18.1, 13.18.2, 13.18.6, 17.1.2.1, 17.1.2.2, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.6
FS11	Alternative SRV (RDCF)(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.3, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.6, 13.4.1, 13.4.6, 13.5.1.1, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.6, 13.6.1,1, 13.6.1,5, 13.6.1,6, 13.6.2,1, 13.6.2,5, 13.6.2,6, 13.6.3,1, 13.6.3,5, 13.7.1, 13.7.6, 13.12.1, 13.12.2, 13.17.1, 13.17.6, 13.18.1, 13.18.6, 11.6.1, 11.6.6, 11.7.1, 11.7.4, 11.8.2.1, 11.8.2.6, 11.10.2.1, 11.10.2.6, 11.11.2.1, 11.11.2.6, 11.12.2.1, 11.12.2.6, 17.1.2.1, 17.1.2.6, 17.2.2.1, 17.2.2.6, 17.3.2.1, 17.3.2.6, 17.4.2.1, 17.4.2.6, 17.5.2.1, 17.5.2.6, 18.1.2.1, 18.1.2.6, 18.2.2.1, 18.2.2.6, 18.3.2.1, 18.3.2.6	Requirements as RDCF (B2) are below: 4.2.5.1, 4.2.5.2, 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.4, 11.3, 11.6, 11.7, 11.8, 17.2.1, 18.3.1, 4.2.6, 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 5.2.1, 5.3.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 11.3, 11.6, 11.7, 11.8, 17.2.1, 18.3.1 13.4.1, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.6, 17.5.2.1, 17.5.2.6, 18.3.2.1, 18.3.2.6

*Refer to Appendix A1 for the relevant SFCs

No.*	Front System	Initiating Fault / Event ID From Topic Report of Fault Assessment [Ref-8]	Remarks
FS12	FLSS(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2,, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.2, 11.3, 11.4.1, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.5.1.1, 13.5.1.2, 13.5.1.3, 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.6.1.1, 13.6.1.2, 13.6.1.3, 13.6.1.4, 13.6.1.5, 13.6.1.6, 13.6.2.1, 13.6.2.2, 13.6.2.3, 13.6.2.4, 13.6.2.5, 13.6.2.6, 13.6.3.1, 13.6.3.2, 13.6.3.3, 13.6.3.4, 13.6.3.5, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6, 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.3, 13.17.4, 13.17.5, 13.17.6, 13.18.1, 13.18.2, 13.18.3, 13.18.4, 13.18.5, 13.18.6, 11.4.2.1, 11.4.2.2, 11.4.2.3, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.8.2.1, 11.8.2.2, 11.8.2.3, 11.8.2.4, 11.8.2.5, 11.8.2.6, 11.10.2.1, 11.10.2.2, 11.10.2.3, 11.10.2.4, 11.10.2.5, 11.10.2.6, 11.11.2.1, 11.11.2.2, 11.11.2.3, 11.11.2.4, 11.11.2.5, 11.11.2.6, 11.12.2.1, 11.12.2.2, 11.12.2.3, 11.12.2.4, 11.12.2.5, 11.12.2.6, 17.1.2.1, 17.1.2.2, 17.1.2.3, 17.1.2.4, 17.1.2.5, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.3, 17.2.2.4, 17.2.2.5, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.3, 17.3.2.4, 17.3.2.5, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.3, 17.4.2.4, 17.4.2.5, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.3, 17.5.2.4, 17.5.2.5, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.3, 18.1.2.4, 18.1.2.5, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.3, 18.2.2.4, 18.2.2.5, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6,	Requirements as FLSS (B2) are below: 4.2.5.1, 4.2.5.2, 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 11.2, 11.3, 17.2.1, 18.3.1, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.4.1, 13.4.3, 13.4.4, 13.4.5, 13.5.1.2, 13.5.1.3, 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.6.1.2, 13.6.1.3, 13.6.1.4, 13.6.1.5, 13.6.1.6, 13.6.2.3, 13.6.2.4, 13.6.3.3, 13.6.3.4, 13.7.3, 13.7.4, 13.7.5, 13.8.1.2, 13.8.1.3, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.6, 13.9.1, 13.9.2,13.9.4, 13.9.6, 13.10.1, 13.10.2, 13.10.4, 13.10.6, 13.11.1, 13.11.2, 13.11.4, 13.11.6, 13.13.1, 13.13.2, 13.14.1, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.3, 13.17.4, 13.17.5, 13.18.3, 13.18.4, 13.18.5, 11.6.3, 11.6.4, 11.6.5, 18.2.2.3, 18.2.2.4, 18.2.2.5, 11.10.2.4, 11.10.2.5, 11.11.2.4, 11.11.2.5, 11.12.2.3, 11.12.2.4, 11.12.2.5, 18.3.2.1, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6,
FS13	SRV –Manual depressurization– (A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.2, 10.1, 10.2, 10.3, 10.4, 5.1.1, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 11.1, 11.3, 11.5, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.3.6, 13.4.1, 13.4.6, 13.5.1.1, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.6, 13.7.1, 13.7.6, 13.12.1, 13.12.2, 13.17.1, 13.17.6, 13.18.1, 13.18.6, 11.7.1, 11.7.4, 17.1.2.1, 17.1.2.6, 17.2.2.1, 17.2.2.6, 17.3.2.1, 17.3.2.6, 17.4.2.1, 17.4.2.6, 17.5.2.1, 17.5.2.6, 18.1.2.1, 18.1.2.6, 18.2.2.1, 18.2.2.6, 18.3.2.1, 18.3.2.6	

*Refer to Appendix A1 for the relevant SFCs

No.*	Front System	Initiating Fault / Event ID From Topic Report of Fault Assessment [Ref-8]	Remarks
FS14	RHR(A1)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 11.1, 11.2, 11.3, 11.4.1, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1 13.3.1, 13.3.2, 13.3.3, 13.3.4, 13.3.5, 13.3.6, 13.4.1, 13.4.2, 13.4.3, 13.4.4, 13.4.5, 13.4.6, 13.5.1.1, 13.5.1.2, 13.5.1.3, 13.5.1.4, 13.5.1.5, 13.5.1.6, 13.5.1.7, 13.5.2.1, 13.5.2.2, 13.5.2.3, 13.5.2.4, 13.5.2.5, 13.5.2.6, 13.5.2.7, 13.5.3.1, 13.5.3.2, 13.5.3.3, 13.5.3.4, 13.5.3.5, 13.5.3.6, 13.6.1.1, 13.6.1.2, 13.6.1.3, 13.6.1.4, 13.6.1.5, 13.6.2.1, 13.6.2.2, 13.6.2.3, 13.6.2.4, 13.6.2.5, 13.6.2.6, 13.6.3.1, 13.6.3.2, 13.6.3.3, 13.6.3.4, 13.6.3.5, 13.7.1, 13.7.2, 13.7.3, 13.7.4, 13.7.5, 13.7.6, 13.8.1.2, 13.8.1.3, 13.8.1.4, 13.8.1.5, 13.8.1.6, 13.8.2.1, 13.8.2.2, 13.8.2.3, 13.8.2.4, 13.8.2.5, 13.8.2.6, 13.9.1, 13.9.2, 13.9.3, 13.9.4, 13.9.5, 13.9.6, 13.10.1, 13.10.2, 13.10.3, 13.10.4, 13.10.5, 13.10.6, 13.11.1, 13.11.2, 13.11.3, 13.11.4, 13.11.5, 13.11.6, 13.12.1, 13.12.2, 13.13.1, 13.13.2, 13.14.1, 13.14.2, 13.15.1, 13.15.2, 13.16.1, 13.16.2, 13.16.3, 13.17.1, 13.17.2, 13.17.3, 13.17.4, 13.17.5, 13.17.6, 13.18.1, 13.18.2, 13.18.3, 13.18.4, 13.18.5, 13.18.6, 11.4.2.1, 11.4.2.2, 11.4.2.3, 11.6.1, 11.6.2, 11.6.3, 11.6.4, 11.6.5, 11.6.6, 11.7.1, 11.7.3, 11.7.4, 11.8.2.1, 11.8.2.2, 11.8.2.3, 11.8.2.4, 11.8.2.5, 11.8.2.6, 11.10.2.1, 11.10.2.2, 11.10.2.3, 11.10.2.4, 11.10.2.5, 11.10.2.6, 11.11.2.1, 11.11.2.2, 11.11.2.3, 11.11.2.4, 11.11.2.5, 11.11.2.6, 11.12.2.1, 11.12.2.2, 11.12.2.3, 11.12.2.4, 11.12.2.5, 11.12.2.6, 17.1.2.1, 17.1.2.2, 17.1.2.3, 17.1.2.4, 17.1.2.5, 17.1.2.6, 17.2.2.1, 17.2.2.2, 17.2.2.3, 17.2.2.4, 17.2.2.5, 17.2.2.6, 17.3.2.1, 17.3.2.2, 17.3.2.3, 17.3.2.4, 17.3.2.5, 17.3.2.6, 17.4.2.1, 17.4.2.2, 17.4.2.3, 17.4.2.4, 17.4.2.5, 17.4.2.6, 17.5.2.1, 17.5.2.2, 17.5.2.4, 17.5.2.5, 17.5.2.6, 18.1.2.1, 18.1.2.2, 18.1.2.3, 18.1.2.4, 18.1.2.5, 18.1.2.6, 18.2.2.1, 18.2.2.2, 18.2.2.3, 18.2.2.4, 18.2.2.5, 18.2.2.6, 18.3.2.1, 18.3.2.2, 18.3.2.3, 18.3.2.4, 18.3.2.5, 18.3.2.6,	
FS15	Containment venting(A2)	1.1, 1.1.1 (12.1), 1.1.2 (12.2), 1.2.1, 1.2.2, 1.3, 1.3.1.1 (12.3), 1.3.1.2 (12.3), 1.4, 1.5, 1.6.1, 1.6.2, 1.7, 1.8, 2.1, 2.2, 2.3, 3.1, 4.2.3.1, 4.2.3.2, 4.2.4.1, 4.2.4.2, 4.2.5.1, 4.2.5.2, 4.4, 4.5, 4.6, 5.1, 5.2, 5.3, 6.1, 7.1, 7.2, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.1, 11.2, 11.3, 11.4.1, 11.5, 11.6, 11.7, 11.8.1, 11.9, 11.10.1, 11.11.1, 11.12.1, 17.1.1, 17.2.1, 17.3.1, 17.4.1, 17.5.1, 17.6, 18.1.1, 18.2.1, 18.3.1, 13.3.1, 13.4.1, 13.5.2.1, 13.5.3.1, 13.6.2.1, 13.6.3.1, 13.7.1, 13.8.1.1, 13.8.2.1, 13.9.1, 13.10.1, 13.11.1, 13.12.2, 13.17.1, 13.18.1, 11.6.1, 11.8.2.1, 11.10.2.1, 11.11.2.1, 11.12.2.1, 17.1.2.1, 17.2.2.1, 17.3.2.1, 17.4.2.1. 17.5.2.1, 18.1.2.1, 18.2.2.1, 18.3.2.1	Requirements as Containment venting (B2) are below: 4.5, 4.6, 5.3, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 5.1.1, 5.1.2, 5.1.3, 5.2.2, 5.2.3, 5.3.2, 5.3.3, 5.3.4, 1.1.1, 1.4.1, 1.5.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 11.4.1, 11.5, 18.3.1, 13.4.1, 13.5.3.1, 13.8.1.1, 13.8.2.1, 13.9.1, 13.10.1, 13.11.1, 13.17.1, 13.18.1, 17.5.2.1, 18.3.2.1

*Refer to Appendix A1 for the relevant SFCs

No.*	Front System	Initiating Fault / Event ID From Topic Report of Fault Assessment [Ref-8]	Remarks
FS16	MSIV(A1)	2.1, 2.2, 2.3, 3.1, 4.6, 5.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 5.1.1, 5.1.2, 5.1.3, 5.2.1, 5.2.2, 5.2.3, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 2.2.1, 2.3.1, 5.1.3, 3.1.1, 2.1.2, 11.2, 11.4.1, 11.8.1, 11.9, , 15.1.1, 15.1.2, 15.1.3, 17.6, 18.1.1, 18.2.1, 18.3.1	MSIV closure due to initiator (No description of Cat./Class) are below: 11.10.1, 11.11.1, 11.12.1, 18.1.1
FS17	PCIS(A1)	2.1, 2.2, 2.3, 3.1, 4.6, 5.1, 7.1, 8.1, 8.2, 9.1.1, 9.1.2, 9.2, 9.3, 10.1, 10.2, 10.3, 10.4, 5.1.2, 5.2.2, 5.3.2, 1.1.1, 1.4.1, 2.1.1, 2.2.1, 2.3.1, 5.1.3, 1.4.2, 3.1.1, 2.1.2, 11.2, 18.1.1, 18.2.1, 18.3.1	

Appendix B: Safety Property Claims Table

SPC	Safety Property Claims (SPC) Contents
C&I SPC 1	The safety functions allocated to C&I systems and their support systems have been categorised and the SSCs classified in accordance with their significance to safety.
C&I SPC 2	The C&I achieves the reliability requirements assigned to the SSCs which C&I controls.
C&I SPC 3	The C&I System has sufficient defence in depth to meet relevant operating conditions.
C&I SPC 4	The C&I systems have the appropriate level of redundancy to protect against single failure.
C&I SPC 5	The C&I is robust to specified internal hazards.
C&I SPC 6	The C&I is robust to specified external hazards.
C&I SPC 7	The C&I has adequate performance to execute the assigned nuclear safety functions and meet operational requirements.
C&I SPC 8	The C&I continues to meet its functional safety requirements throughout its operational life.
C&I SPC 9	The design, development and implementation processes of the C&I SSCs comply with standards and good practice set by their classification and the systems' role in the architecture.
HFSPC	

Relevant C&I Safety Property Claims

The nine standard C&I SPCs listed above are from Appendix B of GDA PCSR Chapter 14:C&I. The application of each one to the concept design of HMIs for GDA is described briefly below. A more detailed breakdown of how HMI SPCs, including sub-claims, are derived from the C&I SPCs is provided in the BSC for Overall HMI [Ref-1].

The arguments and evidence to support these claims and sub-claims for the overall HMI architecture are provided in the [Ref-1]. Similarly, the arguments and evidence to support each of these claims for the individual main HMIs in the scope of this chapter are provided in the BSCs for those HMIs – [Ref-2], [Ref-3], and [Ref-4].

C&I SPC 1: *The safety functions allocated to C&I systems and their support systems have been categorised and the SSCs classified in accordance with their significance to safety.*

C&I SPC 1 is underpinned by two sub-claims; sub-claim 1.1 for the safety Cat and Class of the HMIs themselves, and the sub-claim 1.2 for the safety Classification of the support systems that are required to function to ensure the required performance of the HMIs.

Each HMI and its support systems such as the electrical power system and HVAC are classified on the basis of the category of the delivered safety functions and the importance to the safety contribution. This classification is in accordance with the methodology which is described in GDA PCSR Chapter 5.6.

> Application of this SPC means that the safety classification of HMIs is always at least as high as the highest classification of the C&I systems to which those HMIs interface. This is captured in 'Overall HMI SPC 1.1' in the BSC on Overall HMI [Ref-1]. Hence the design eliminates the use of lower integrity systems to actuate functions important to safety that require higher integrity.

C&I SPC 2: *The C&I achieves the reliability requirements assigned to the SSCs which C&I controls.*

With respect to hardware of the HMIs, the reliability target for each C&I system is calculated over a chain of systems which includes the associated HMI. Therefore, the HMI portion of the reliability target forms an integral part of, and is not explicitly demonstrated separately from the reliability of the C&I controller and field equipment; the arguments and evidence for this SPC are therefore given by SPC 2 of GDA PCSR Chapter 14:C&I and its supporting documents.

The aspects of reliability of specific claimed human actions when using HMIs are demonstrated qualitatively and/or quantitatively (depending on risk importance) as detailed within the HBSC Report [Ref-9]. Specifically, quantitative assessment of human actions important to the PSA is presented in the Human Reliability Analysis Report [Ref-10]. Both of these reports are key supporting documents for PCSR Chapter 27:HF.

The combined reliability of the human actions with the relevant elements of their respective HMIs is modelled in the scope of the PSA, described in PCSR Chapter 25:Probabilistic Safety Assessment.

C&I SPC 3: *The C&I System has sufficient defence in depth to meet relevant operating conditions.*

This SPC focuses on provision of sufficient defence in depth of the Overall C&I architecture, and the associated HMIs within that architecture.

The C&I architecture includes 3 independent groups in order to have sufficient defence in depth for UK ABWR. HMIs which are provided for each C&I system are designed and implemented taking account of the following considerations, in order to protect against fault propagation and minimise the risk of CCF of the HMIs functionality. This is achieved through:

- Using different technology to implement HMIs for the Class 1 system (SSLC) from HMIs of other C&I systems such as PCntlS, ACS, and PCS. Hitachi-GE is developing an HMI architecture based on the Class 1 FPGA platform, reusing several modules already developed for the SSLC and some additional HMI specific modules required to provide visual displays. The HMI specific modules will only be developed post-GDA.
- The HMIs of the PCntlS, ACS and PCS use digital technology. In contrast, the HMIs of the Category A Class 2 system (HWBS), which controls second line provisions of safety systems, is implemented by conventional, non-digital technology, which prevents the simultaneous loss of

HWBS HMIs with HMIs for the SSLC which controls the first provisions of safety systems. It also prevents simultaneous loss with other HMIs for the PCntlS, ACS, and PCS from CCF of digital systems.

In addition to this technology diversity, alternative independent HMIs in the MCR or other separate control sites are provided to deliver Category A safety functions, as illustrated in Figure 21.3-1.

- The SAuxP for Category A Class 1 SSCs is provided as defence-in-depth against CCF in the digital C&I system in the MCR. This panel uses conventional, non-digital technology which is diverse from the SSLC technology. Therefore, it enables the operators to perform manual operations.

- The RSP which use conventional, non-digital technology which is diverse from the SSLC technology are located outside of the secondary containment of the R/B.

Further information of HMI technology is shown in the related BSCs, [Ref-1], [Ref-2], and [Ref-3].

The BSC on Overall HMI [Ref-1] includes sub-claims, arguments and evidence to support the application of C&I SPC 3 for the overall architecture of HMIs ('Overall HMI SPC 3.1 to 3.4'). The arguments and evidence to support these sub-claims demonstrates that all C&I and associated HMI systems that are safety Class 2 are independent of C&I/HMI systems that are safety Class 1. Similarly it is demonstrated that all C&I and associated HMI systems that are Class 3 are independent of C&I/HMI systems that have a higher safety classification. Hence the design eliminates the possibility that failures of lower class HMIs could adversely affect HMIs of a higher classification. The sub-claims also demonstrate significant diversity of HMI technology.

Taken together these support C&I SPC 3 to demonstrate sufficient defence in depth of availability of HMIs in all conditions. Application of this SPC, as described in [Ref-1], ensures that the key risk of non-availability of an HMI when required that is identified in the ALARP justification in Section 21.10.1 is minimised.

C&I SPC 4: *The C&I systems have the appropriate level of redundancy to protect against single failure.*

This SPC is underpinned by two sub-claims: The first is that the HMI architecture matches the features of the associated C&I system in the overall C&I architecture to provide equivalent redundancy. The second is that the HMIs are physically separated among divisions according to the rule of separation to maintain the required overall divisional redundancy.

C&I SPC 5: *The C&I is robust to specified internal hazards.*

The HMIs installed in control room locations are in areas not prone to internal hazards such as flood, fire, missile, dropped loads or pipe whip. These HMIs also maintain the divisional or channel separation as far as is practicable through the use of electrical separation and, as far as is practicable, physical separation and barriers.

The HMI design and installation consider the effects of internal Electromagnetic Interference (EMI) in the context of the resistance to EMI of the C&I system that the HMI is part of.

For local control panels the vulnerability and robustness to internal hazards is considered in the safety case of the C&I system that the HMI is part of. In the case of a local panel being located away from the system, this may require different hazards to be considered.

Basically, the consequences of any internal hazard are limited to the division of origin of the hazard by segregation barriers or separation. Whilst there is exception to segregation and separation on the configuration of HMI in the MCR, this is mitigated by alternative HMIs in the other control points that are provided to perform defined safety functions.

C&I SPC 6: *The C&I is robust to specified external hazards.*

The HMIs installed in control room locations are in areas with some degree of protection against the effects of external hazards such as aircraft or other vehicle impact or seismic events. These HMIs also maintain the divisional or channel separation as far as is practicable through the use of electrical separation and, as far as is practicable, physical separation and barriers.

The HMI design and installation consider the effects of external EMI in the context of the resistance to EMI of the C&I system that the HMI is part of.

For local control panels the vulnerability and robustness to external hazards is considered in the context of the C&I system that the HMI is part of and is therefore not covered separately within the HMI documentation.

C&I SPC 7: *The C&I has adequate performance to execute the assigned nuclear safety functions and meet operational requirements.*

With regards to the physical elements of the HMIs, they form an inherent part of the relevant C&I systems which they are related to. The capability and functionality of the HMIs to achieve the assigned SFCs matches that for the overall related C&I system.

The role of the HMI in respect of human performance is considered through the use of HF processes, guidance, good practice and expertise. This SPC is further implemented through the two Level 2 HBSCs that act as HFSPCs, listed below. These claims are further detailed and substantiated within PCSR Chapter 27:HF.

The BSC on Overall HMI [Ref-1] includes sub-claims, arguments and evidence to support the application of C&I SPC 7 for the overall architecture of HMIs. These include:

> ‘Overall HMI SPC 7.2’ – ‘HMIs deliver their safety function against the environmental condition at the installed location’
>
> ‘Overall HMI SPC 7.5’ – ‘HMI has been designed to take Human Factors good practice into account’

Application of this SPC, as described in [Ref-1], together with HFSPC 1 and HFSPC 3 listed below, ensures that the key risk of the possibility of HMI inducing human error that is identified in the ALARP justification in Section 21.10.1 is minimised.

C&I SPC 8: *The C&I continues to meet its functional safety requirements throughout its operational life.*

Test and maintenance activities, including replacement, are carried out through the use of appropriate interfaces. The HMIs provide indicators and switches for operators and maintenance personnel to perform functional tests defined for each SSC and C&I system and maintenance works including detection of a failure. Components of the HMIs are also tested, inspected, and replaced as a part of C&I systems according to the management plans which will be specified for each HMI post-GDA.

C&I SPC 9: *The design, development and implementation processes of the C&I SSCs comply with standards and good practice set by their classification and the systems' role in the architecture.*

The HMIs are designed, developed, and implemented to support C&I systems, which comply with IEC 61513 and other international standards and guidance determined by their category and class defined under IEC 61226.

Relevant Human Factors Safety Property Claims

Section 21.3.4.1 identifies the following HFSPCs that specifically apply to HMIs.

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.

[Related to C&I SPC 7.5 for HMI]

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.

[Related to C&I SPC 1.2 application of appropriate classification of HVAC for HMI, and to C&I SPC 7.2 related to continued availability of functioning HMI in the working environment]

Appendix C: Document Map