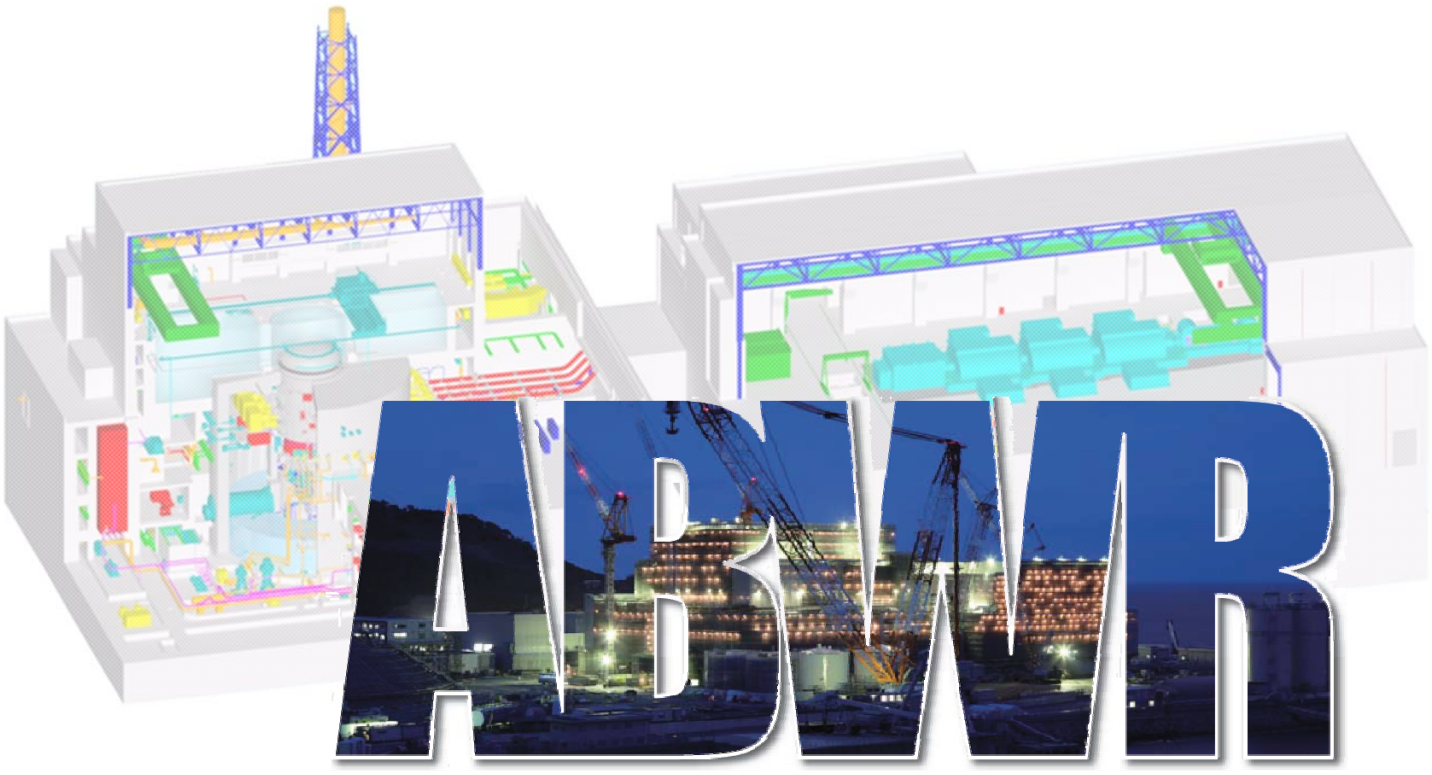
Form10/00

UK ABWR

Document ID	:	GA91-9101-0101-30000
Document Number	:	QGI-GD-0012
Revision Number	:	C

UK ABWR Generic Design Assessment

Generic PCSR Chapter 30 : Operation



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 assumed generic approach to operational aspects that is expected to be followed by the future licensee. It demonstrates that, within the scope of what can be considered for future operations at Generic Design Assessment (GDA) stage, the UK ABWR will be able to be operated safely.

The aim of identifying the operational arrangements within GDA is to ensure that a UK ABWR plant will remain within the safe operating envelope that is defined and justified in the GDA safety case, as presented in the other PCSR chapters. During GDA, it is only possible to describe operational principles at a conceptual level, and the future licensee will need to build on these to produce their own more detailed operating arrangements.

All aspects of UK ABWR plant operations, from the end of commissioning to the start of decommissioning, are considered. However, the main focus for this chapter in GDA is on reactor operations and the organisation and responsibilities of control room personnel, because these are related to the highest risks within the plant. In addition, the chapter includes limited consideration of maintenance. Chemistry control and radiation protection during operation are discussed separately in PCSR chapters 23: Reactor Chemistry and chapter 20: Radiation Protection, respectively.

The overall strategy and underlying philosophy of the approach to operations that have been assumed in undertaking design in the GDA stage is explained. This includes the level of plant automation and the roles and responsibilities of the operations personnel in maintaining the plant within the safe operating envelope, which bounds conditions that have been demonstrated to be safe in the GDA PCSR. The assumed use of operating documentation, including Operating Procedures for a range of plant states, Technical Specifications, and Maintenance, Test and Inspection procedures, is explained. This includes a description of the purpose of the Generic Technical Specifications (GTS) produced in GDA and how these will ultimately provide input to the site-specific Operational Technical Specifications.

The responsibility of future operations personnel for the control and monitoring of the plant status is described, and the minimum required complement of operations personnel is specified, based on GDA assumptions and analysis. Various UK ABWR design features to enhance effective control and monitoring are explained, together with the use of Human-Machine Interfaces in the Main Control Room, Remote Shutdown System Panel rooms, and Backup Building Control Panel room.

Links between assumptions made in the safety case, the Limits and Conditions for Operation (LCOs) that input to the Generic Technical Specifications, and the safety analysis are described. Assumptions that are specific to this chapter are listed. The chapter also explains how the LCOs and safety case assumptions will be supported by the results of further post-GDA verification and validation of operational arrangements through various means including the commissioning tests described in PCSR chapter 29: Commissioning.

A short description of the current As Low as Reasonably Practicable (ALARP) position is provided, which concludes that the risks associated with operation of the UK ABWR have been reduced to levels that are ALARP as far as is possible for operations at the GDA stage. It is also concluded that future operational arrangements will be supported by the generic design and preliminary operational arrangements. This in turn

will help to ensure that future operating arrangements on a licensed site can be implemented in such a way that will reduce the site-specific operations risks to levels that are ALARP.

The further work that will be required post GDA to develop the site-specific operational arrangements should be the responsibility of any future licensee. The contents of this chapter will form the basis for the development of those site-specific operations processes and procedures as the site-specific design and safety case are developed.

30.1 Introduction

The objective of this Operation chapter is to describe the generic approach to operation (principles, programmes, processes, operating arrangements, organisation, roles, responsibilities, etc.) required for safely operating a UK ABWR.

The scope of the chapter is to include all pertinent issues related to operational aspects and to discuss the overall safety case elements for operations of the UK ABWR.

This chapter contains a description of the generic approach to operations which should be developed further by the future licensee. Because this GDA PCSR is based on the generic design and is prepared by the Requesting Party (RP), the descriptions contained in this chapter are the operational assumptions that underpin the plant design basis for safety. In order to ensure alignment with current UK modern nuclear industry good practice for operations, these operational assumptions have been developed with the participation of specialists with a knowledge of UK-based reactor operational experience. These assumptions, based on UK based operational experience, are included in this chapter, 'Human Factors Concept of Operations Report' [Ref-2]; and 'Maintenance Philosophy' [Ref-12].

It should be noted that although the information in this chapter is weighted towards plant operations and control room personnel, as these are related to the highest risks and most significant claims related to safety, "operations" should be taken to mean the following aspects of plant operations:

- Plant operation – control of plant system, equipment and of the plant status, i.e. it means engineered plant operating process.

- Operational activities – this is taken to mean human activities relating to plant operation, e.g. operator activities, administrative control staff's activities, etc

Also in this chapter, 'normal operation' means normal conditions of the plant.

It should be noted that the conduct of operations and the plant design features that support it can only be described at a conceptual level at this stage.

30.1.1 Background

The GDA process involves regulatory assessment of the safety, environmental and security safety case for the UK ABWR. Primarily this is an assessment of the deterministic and probabilistic safety analysis plus consideration of hazards, etc. Other important aspects are the arrangements that enable the UK ABWR to be operated and maintained in accordance with this safety case.

However, the responsibility for safety on a future licensed site and for operation of the UK ABWR in accordance with the safety case will rest with the nuclear site licence holder. In the UK regulatory framework, the future licensee needs to comply with the Energy Act 2013, Nuclear Installations Act

1965, and have appropriate arrangements to operate the plant in compliance with the Site Licence and its 36 licence conditions.

Therefore, at the GDA PCSR stage it is not possible to describe all of the arrangements that will need to be in place to operate a UK ABWR safely on a future nuclear licensed site. However, in GDA, Hitachi-GE has identified the generic approach to operation and the operational assumptions that underpin the plant design basis for safety. These include the generic principles, programmes, processes, operating arrangements, organisation, roles, responsibilities, etc. required by design for safely operating a UK ABWR.

To help ensure alignment with current UK modern nuclear industry good practice for operations the generic approach to operation and the operational assumptions have been developed based on UK-based reactor operational experience.

As the conduct of operations and the plant design features that support it can only be described at a conceptual level at this stage then there are no formal claims made in this chapter and no directly supporting topic report (as would be expected in strict compliance with the safety case development manual [Ref-16]). However, reference is made to other PCSR chapters where related claims are made and topic reports are provided.

Given this background, it is therefore the intention of this GDA PCSR chapter to describe the expectations for safe operation of a UK ABWR, so far as is appropriate for the GDA stage.

30.1.2 Document Structure

The following sections are included in this chapter:

Section 30.2 Purpose and Scope: This section sets out the purpose and scope of the operations PCSR chapter for GDA and identifies what is not included. It also identifies the most significant links to other GDA PCSR chapters.

Section 30.3 Operational Strategy: This section describes the overall strategy and underlying philosophy of the approach to operations assumed during the design of the generic UK ABWR. It covers the level of automation, the role of operations personnel to maintaining the plant within safe conditions for operation, the philosophy for Command and Control and requirements for effective communications.

Section 30.4 Operating System: This section describes the various elements of the plant operating system (Main Control Room (MCR), operating procedures, Technical Specifications, Maintenance and Inspection programme) and provides a summary of how these systems relate to the operational strategy.

Section 30.5 Plant Status Control: This section describes how the operators are responsible for the control and monitoring of the status of the plant and are required to be fully aware of the operational state and availability/operability of Structures, Systems and Components (SSCs). It also describes how various design features, such as interlocks and automatic realignment, ensure that the required minimum plant availability/operability is achieved at all times.

Section 30.6 UK ABWR Operations Personnel Description: This section provides a high-level description of the minimum complement of personnel who will be responsible for operational activities of the UK ABWR, to the extent they can be determined within GDA, noting that many aspects of the operating organisation can only be developed fully by the future licensee. It also describes the roles and responsibilities for this minimum complement of operations personnel.

Section 30.7 Assumptions, Limits and Conditions for Operation: This section will list any assumptions specific to the Operations topic area, and summarise how the assumptions and LCOs made in the safety case are utilised to ensure safe operation of UK ABWR. In addition, the general principles for the identification of Assumptions and Limits and Conditions for Operation within other chapters of GDA PCSR, are described in Generic PCSR Chapter 4: Safety Management throughout Plant Lifecycle, section 4.12.

Section 30.8 Summary of ALARP justification: This section presents a high level overview of how the ALARP principle has been applied for the Operations topic area within the GDA PCSR and how this contributes to the overall ALARP argument for the UK ABWR.

Section 30.9 Conclusions: This section provides a summary of the main aspects of this chapter.

Section 30.10 References: This section lists documents referenced within this chapter.

Other relevant information is captured in Appendices as follows:

Appendix A - Document Map of supporting evidence in Level 2 GDA documents

The chapter does not cover the following:

- definition and description of the operating modes (see PCSR Chapter 5: General Design Aspects)
- details of site-wide emergency arrangements or emergency preparedness plan (see PCSR Chapter 22: Emergency Preparedness)
- security requirements/aspects for operational activities
- requirements for operational arrangements relating to environmental hazards
- identification and assessment of conventional health and safety related hazards

- detailed description, arguments and evidence for the human-based safety claims (HBSCs) related to operation activities (PCSR Chapter 27: Human Factors)
- details of organisational structures (e.g. organisation charts), which should be the responsibility of the future operator.
- chemistry control (PCSR Chapter 23: Reactor Chemistry)
- radiation protection (PCSR Chapter 20: Radiation Protection)

For generic links to Generic Environmental Permit (GEP), and Conceptual Security Arrangements (CSA) documentation, please refer to Generic PCSR Chapter 1: Introduction. For GEP, where specific references are required, for example in Radioactive Waste Management, Radiation Protection, Decommissioning, these will be included in the specific sections within the relevant chapter.

This Chapter 30 also links with a number of other PCSR chapters, in particular

- PCSR Chapter 4: Safety Management throughout Plant Lifecycle
- PCSR Chapter 5: General Design Aspects (Reference information on the approach to compliance with NSEDPs in operation and general requirements for Examination, Maintenance Inspection and Testing (EMIT))
- Systems Chapters from PCSR chapter 11 to 19 (for assumptions and LCOs that drive the GTS [Ref-1] and operational requirements for safety)
- PCSR Chapter 20: Radiation Protection (Input to radiation control arrangements on plant operation for the future licensee)
- PCSR Chapter 21: Human Machine Interface
- PCSR Chapter 22: Emergency Preparedness
- PCSR Chapter 23: Reactor Chemistry (Input to chemistry control arrangements on plant operation for the future licensee)
- PCSR Chapters 24, 25 and 26: Design Basis Analysis, Probabilistic Safety Analysis, and Beyond Design Basis Analysis and Severe Analysis (respectively)
- PCSR Chapter 27: Human Factors
- PCSR Chapter 28: ALARP Evaluation

- PCSR Chapter 31: Decommissioning (Chapter 31 discusses the importance of good record management during operations on future decommissioning planning.)

30.2 Purpose and Scope

30.2.1 Purpose

The objective of this Operation chapter is to describe the generic approach to operation required for safely operating a UK ABWR.

Specific objectives of this GDA PCSR chapter are to describe, to the extent possible for GDA, the:

- Overall strategy and underlying philosophy of the approach to operations assumed during the design of the generic UK ABWR,
- Operating organisation and their roles, responsibilities,
- How automation is used to assist the operators,
- Main operating documentation,
- That the risks associated with operating the UK ABWR (as related to the operational arrangements) will be ALARP,
- Links to relevant content of other GDA PCSR chapters, to ensure consistency across the whole safety case, and to ensure the overall safety case presented is complete, and
- Location of additional detailed supporting information in Level 2 and Level 3 GDA documents.

It should be noted that the future licensee should have prime responsibility for all site activities that may affect safety including plant operations and that this cannot be delegated.

30.2.2 Scope

The scope of the chapter is to include all pertinent issues related to operational aspects and to discuss the overall safety case elements for operations of the UK ABWR, to the extent they can be determined within GDA, noting that many aspects of the operating organisation can only be fully developed by the future licensee.

In this chapter, “operations” is taken to mean plant operation and operational activities (see section 30.1 above). This chapter covers the operational activities from the end of the Commissioning, identified as the Commercial Operation Date (COD) hold point, until the start of the Decommissioning phase.

30.3 Operational Strategy

This section describes the overall strategy and underlying philosophy of the approach to operations assumed during the design of the generic UK ABWR. The assumptions around all operational aspects of the plant that derive from this strategy are captured in greater detail within the Human Factors Concept of Operations Report (COR) [Ref-2].

Through these assumptions, the operational strategy has been used to support human factors (HF) analyses and other activities that form part of the UK ABWR GDA HF Integration (HFI) programme, as detailed in the HFI Plan (HFIP) [Ref-3]. This strategy also underpins safety analyses throughout the topic areas, including for example fault assessment, equipment failure and reliability analysis, and radiation protection. In this way, the strategy feeds into the design features and plant functional requirements put in place to support safe operation and personnel contribution to plant safety goals. Finally, because it forms the basis of the HF analyses and requirements, the operational strategy underpins all of the specific human actions that are claimed within this safety case; these are the HBSCs that are stated in GDA PCSR Chapter 27: Human Factors and its supporting report on HBSCs [Ref-4].

Site-specific safety cases will present the operational programmes (i.e. training, plant ageing management, configuration control, use of operating experience feedback, fire protection, etc.) supporting the plant's safe operation, to achieve the underpinning objectives of any future licensee's conduct of operation philosophy.

The overall operational strategy is that the actions of all the plant systems, including the personnel interfacing with them, will:

- Keep the plant operating normally,
- Failing this, where expected events occur, e.g. plant disturbances, restore the plant to normal operation,
- Failing this, for accidents, e.g. LOCA, LOOP, restore the plant to a safe state, and
- Failing this, minimise the severity of any accident.

The operational strategy is based on the following basic operating principles:

- The level of automation during normal operations and fault scenarios effectively uses the strengths of each of the "equipment" (i.e. the mechanical, Control & Instrumentation (C&I), electrical components, etc.) and human elements of the plant operation. Automation is optimised to achieve a balanced workload for personnel and to allow them to maintain awareness of plant state at all times.

- The hierarchy of control is followed, in terms of required operations, in that measures important to maintaining the plant in, or bringing it back to a safe state are automated rather than manual. The manual actions available provide defence in depth to back up the

automated systems but are not the primary claimed measures in fault situations where risk-based analysis determines that would not align with ALARP principles.

- The SSCs are designed in accordance with the principles of redundancy, diversity and separation to allow those SSCs to be reliable and available as required to fulfil their role in achieving the fundamental safety functions (FSFs). Taking actions to ensure that the SSCs are available as required and to operate the plant in the required configuration and power level given the availability of those SSCs, as required by the LCOs and GTSs, will be the primary role of operations and maintenance personnel.

- Specific actions claimed of plant personnel to meet the safety goals of the plant and the requirements of the safety case are clearly documented. The plant is then designed to support the required performance of these actions. Achievement of the claimed actions is expected to be further supported by operational arrangements developed by the future licensee.

- Operations and maintenance will be conducted using a suite of clearly-written, verified and validated documents which detail the conditions in which the plant is safe and make clear the assumptions and basis of the safety case; all relevant personnel will be suitably trained in the contents and usage of these documents.

- The normal operation and maintenance of the plant in all states will employ some form of formal risk-based operational decision-making process that allows competent and authorised operations personnel to prioritise any potentially conflicting tasks based on clear understanding of the safety case and plant risks.

- The SSCs throughout the plant will be clearly linked, through nuclear safety Category and Classification (see Chapter 5: General Design Aspects), to the claims for safety made on them in the deterministic case. Their importance will be made clear in the relevant operating and maintenance documentation and on the SSCs themselves, such that all personnel are clearly aware of the role of SSCs in achieving the plant's safety goals.

- The maintenance philosophy will be optimised through the use of reliability-based and condition-based maintenance programmes that will minimise the use of invasive maintenance tasks that introduce risk to both the SSCs (risk of decreased availability) and personnel (risk of increased unnecessary dose uptake).

- Local operations, surveillance and maintenance tasks will be undertaken both at power and during outage; as such, therefore the plant layout, including support systems and equipment such as HVAC, lighting, lifting equipment, etc., will be designed to enhance both access and radiation protection in doing required tasks. Personnel safety and radiation protection are maximised, and time at risk and potential radiation exposure are reduced.

It is assumed any future licensee will adopt these principles to underpin the development of their operational arrangements in the post GDA phase. These principles and related operational aspects are explored in more detail in the remainder of this section.

30.3.1 Level of Automation

For the current generation of J-ABWR plants, which form the reference design for the UK ABWR, a high level of automation has been the general overall concept of operations for the design, particularly for plant operations. Normal plant operation can be conducted automatically from cold start-up to rated power, during full power operation and from rated power operation to plant shutdown. Operator burden has been minimised for all safety-related normal tasks, through carefully selected "breakpoints" requiring operator attention ("acknowledgment") between automation sequences during normal operations. Safety-related Reactor Protection system (RPS), Emergency Core Cooling system (ECCS) protection and control rod movement block protection functions are not lost in automatic plant operation, and the plant can be converted back to manual operation for any operator decision or control rod block that requires operator intervention. Operator burden is also reduced in abnormal events through automation of plant responses, particularly immediately following a reactor scram. This general strategy for the reference design has been carried through to the UK ABWR design.

To balance the level of plant automation during operation against an objective to ensure the operator retains an adequate level of situational awareness, key "supervisory" actions are required and confirmation of successful implementation of automated sequences is maintained as part of the operator's role. As described in GDA PCSR Chapter 21: Human-Machine Interface, HMIs within the MCR, in particular the large overview Wide Display Panel (WDP), have been designed to ensure that any failures within the automated operations and any incursions into abnormal plant states are immediately revealed and signalled to all operators within the MCR. The design of the WDP includes the following key features for maintaining plant status awareness in all instances:

- the first-hit and important alarms are displayed on the left side of the panel.
- all key plant parameters are presented in a logical intuitive mimic display in the centre fixed panel.
- context-sensitive trend and other plant item displays automatically appear on the large variable display to the right, and
- system-level alarm tiles are located across the top of the entire WDP.

This design of the WDP has been assessed through HF Verification and Validation (V&V) activities and simulator sessions as part of the baseline HF assessment, as summarised in the Baseline Assessment Report (BAR) [Ref-5]. This has demonstrated that the WDP is successful in supporting key communications and operator situational awareness, particularly in fault conditions. Further details on the operating system and how it supports required operations are given in Section 30.4.

The above strategy is based on the general automation level for the current functions defined within the reference plant design (J-ABWR). The allocation of these functions for the UK ABWR has been confirmed and justified, or if necessary, their allocation modified, through HF and other design

activities within GDA, described in GDA PCSR Chapter 27: Human Factors. Any new functions have also been allocated appropriately according to this strategy.

The level of automation may change at the detail level as the design develops further beyond GDA. However, for the purposes of this GDA PCSR, the level of automation is assumed to be generally the same as for the J-ABWR with the exception of known improvements to further automate some safety system initiation, as described in GDA PCSR Chapter 27. Therefore, the operational strategy above remains generally applicable to the UK ABWR.

30.3.2 Contribution to Plant Safety Goals

In addition to minimizing operational burden whilst maintaining sufficient situational awareness, the operational strategy for the ABWR plant includes an assumed level of contribution from the operations personnel (including maintenance) to keeping the plant within its Limits and Conditions for Operations (LCOs - described in section 30.7), thereby supporting the achievement of the plant safety goals. Suitable facilities, controls and plant design features (e.g. bypass systems, test modes, connection points for equipment calibration, etc.) are provided for the regular testing, inspection and calibration of safety-related SSCs.

The specific actions and related plant design features required to meet this contribution from operations personnel have been determined through the results of the evolving safety analyses (fault studies, PSA, reliability-centred maintenance review, etc.) for the UK ABWR. Assessment of the required human actions necessary to achieve the safety goals of the plant is reported in the HBSC report [Ref-4]. However, these human actions in plant operation and operational activities in normal operation generally constitute the following:

- Regular, frequent, non-invasive testing of identified SSCs from the MCR or using local-to-plant HMIs with the plant “in service” (i.e. running at power).
- Regular visual inspection to check the healthy status, availability and operability of identified SSCs through frequent (shiftly or daily) plant walk-arounds or “patrols”.
- Regular monitoring and recording of key parameters within the MCR or from key SSCs (visually or through remote monitoring equipment) to allow monitoring of conditions and early identification of potential deterioration of expected plant conditions.
- Ensuring the required plant configuration and extent of equipment in service, as specified through LCOs, are met at all times (see also Plant Status Control, Section 30.5).
- When the reactor is shut down periodically for a “Refuelling outage” (to remove spent fuel, and replace it with new fuel) more complex and invasive maintenance can be conducted that cannot be undertaken with the plant at power, including equipment removal, overhaul and approved upgrades.

30.3.3 Command and Control

International good practice in nuclear power operations dictates that the operating organisation has a Command and Control philosophy. A clear definition of responsibilities and lines of authority is important to the safe operation of the plant, particularly in abnormal and fault conditions. The Command and Control philosophy adopted for the UK ABWR is assumed to be similar to that used in existing UK nuclear power plants as follows:

- During normal and fault conditions the Control Room Operators (CROs; see Section 30.6.3 regarding roles), or if applicable, the nominal lead CRO, are responsible for control of their reactor unit and will refer to procedures and other documents as required to keep or return the plant to within its defined safe operating envelope. The MCR Supervisor (MCRS) establishes command and control by providing support, oversight and if necessary direction to the CROs and field operators (FOs) who perform supporting operations local to plant.

- If an event progresses beyond the conditions considered in the PCSR design basis, and in particular, if it develops into a severe accident, the CROs or if applicable, the nominal lead CRO, are still responsible for implementing specific emergency operating procedures and responding to emerging plant conditions as required. However, the MCRS Supervisor and the Shift Manager are assumed to have a greater role in developing and directing the response strategy, and keeping a broader overview based on the status of the entire station in the context of the conditions emerging throughout the event.

- The Shift Manager maintains overall command and control and is assumed to be the acting Initial Emergency Controller when a site incident is declared and the Emergency Control Centre (ECC – described in GDA PCSR Chapter 22: Emergency Preparedness) is established.

- There are assumed to be sufficient numbers of emergency crews, who are assumed to be given regular and adequate training to provide them with the skills to perform the emergency duties (see also GDA PCSR Chapter 22).

- Any centrally-located/off-site and externally-managed emergency response support centre (i.e. Technical Support Centre, etc.) is outside the remit of this chapter.

The above philosophy is described in greater detail with respect to Roles and Responsibilities within the COR [Ref-2].

30.3.4 Communications

Key to safe operations within the UK ABWR plant is clear, effective communications. The plant operating and maintenance organisations need to keep in regular communication, both within and between teams, as well as with the various support teams available to them. This is particularly true when performing tasks related to safety and when dealing with fault conditions.

The HF analysis and design support activities for GDA have included consideration of the communications requirements in general, through the use of requirements specified in the HF Engineering Specification (HFE Spec) [Ref-5], as well as in detail for key tasks, particularly those that have related HBSCs in [Ref-4]. The design of the plant therefore takes these communication requirements into account. Specifically, the following features have been incorporated into the UK ABWR design:

- A MCR that is designed to operate with low ambient noise levels, even in plant fault conditions, to help permit clear communications and instructions,
- Any other local control rooms, plant equipment rooms, local control panels, and external facilities or equipment housings have the means to provide clear communication routes to the MCR or alternative main control point (i.e. Remote Shutdown System (RSS) room, Backup Building (B/B)).,
- Where necessary, based on the safety significance of tasks being conducted, such communication means are suitably robust and diverse from other systems that might be impacted by fault scenarios in which human actions are claimed within the safety analysis, and
- Where local ambient noise conditions are high (equipment rooms) and frequent, safety-related tasks need to be carried out, suitable acoustic insulation or noise enclosures are added to the design, without creating any other operability and maintainability issues.

Portable communications equipment is assumed to meet the same requirements for availability and clarity as the equipment that is a permanent part of the UK ABWR plant. (see also Chapter 15: Electrical Power Supplies, section 15.4.10 Communication System)

In addition to these design features, the operations strategy for GDA assumes that effective communications management policies should be put in place by the future licensee. These measures are assumed to include the following:

- Techniques to minimise human performance errors when verbally communicating important information and operating instructions, such as hand-raising/single-person speaking, use of the phonetic alphabet and three way communications. Other examples of techniques assumed to be used are given in industry good practice guidance document, INPO 06-002 [Ref-7],

- Effective shift handover arrangements: handover from an outgoing shift to an oncoming shift is expected to be formally trained, managed and documented, in accordance with good shift handover practices. It is assumed that shift handover arrangements are such that they do not negatively impact the successful transfer of key items of information from shift to shift, particularly during abnormal, fault or accident scenarios,

- Use of a "visible safety case" programme to ensure that all claimed human actions from the case, and their consequences if not performed correctly, are clearly communicated to all relevant personnel through training and documentation,

- Use of suitably graded procedures to control all activities where personnel interact with the plant. Grading of procedures is expected to relate to consequences of failing to perform the task correctly. An example of such a grading scheme is detailed in the industry guidance document INPO 11-003 [Ref-8], and

- Suitable procedure development and configuration control and management, such that all written operating instructions will be duly authorised, validated and approved prior to their use.

30.4 Operating System

It is assumed that the future licensee will implement a risk-based operational decision-making policy that will underpin daily management of the plant. Operational decisions concerning normal and degraded plant conditions that could affect safe plant operation are assumed to be made based on an in-depth understanding of short- and long-term operational risks, as well as the potential effects of alternative operational options. This type of operating policy ensures that decisions are made such that the plant is operated with margin to the design limits. Where there is doubt over safety margins, conservative decisions are expected to be made to optimise the route to a known safe state. This decision-making is expected to be underpinned by the information generated by the safety analyses conducted in GDA as outlined in this PCSR and future operational documentation, including additional site-specific safety analyses.

During GDA, HF design activities have focussed on ensuring that the plant operating systems are designed to effectively support these risk-based decisions, such that:

- The state of the plant can be clearly determined at any time and in any conditions,
- The various systems and equipment can be controlled effectively to within the required limits, and
- The effectiveness of any actions can be monitored until the condition is resolved and the plant returned to a safe state.

These plant operating systems are described more fully in the various engineering sections within GDA PCSR Chapter 21: Human-Machine Interface and its supporting references (e.g. Strategy of HMI Use [Ref-9]). A summary is given here in terms of how these systems relate to the operational strategy outlined in Section 30.3.

The MCR is located in the Control Building (C/B) and is central to the plant operating system for the UK ABWR, containing both the operations personnel and the main HMIs for monitoring and controlling the plant. The MCR equipment provides the crew on duty with suitable visual and audible information to allow them to monitor the performance of the automated features of the plant, provide “supervisory” control to automated sequences when required, conduct routine surveillance tests, and respond appropriately to plant conditions that deviate from what is expected. The arrangement of displays and controls on the Main Control Console (MCC) allows the CROs to focus on reactor, turbine and balance of plant during all plant operating conditions. The Supervisor station behind the MCC allows the MCRS to have the required oversight of all operations and equipment.

The two Remote Shutdown System Panel Rooms (RSSRs) are established in a separate location with enough distance from the MCR so that the RSSRs and MCR are not simultaneously affected by the same hazard. Each of the two RSSRs has full functionality to provide redundancy, and they are located adjacent to each other. The access route leading to the RSSRs from the MCR is safe for the operators during the expected hazard conditions in which an RSSR is intended to be used. In order to

ensure an RSSR is available at all times in the state required for its important safety-related functions, entry to the RSSRs is restricted by locked access.

In the case of a foreseeable accident where there is a potential threat to MCR habitability, the operator is able to relocate to one of the RSSRs to continue to monitor and, if necessary, make a transition from a hot shutdown state to a cold shutdown state. The RSS interface to the operator is through the Remote Shutdown Panels (RSPs) located in the RSSRs.

In the case of a Severe Accident (SA), operators can monitor and control key plant safety and accident management related functions from the Backup Building Control Panel Room (BBCR). In addition to SA conditions, there are some other accident scenarios identified in the UK ABWR Fault Studies and Probabilistic Safety Analysis (PSA) work, described in GDA PCSR Chapters 24: Design Basis Analysis, Chapter 25: Probabilistic Safety Assessment, and chapter 26: Beyond Design Basis and Severe Accident Analysis, that require Control and Instrumentation (C&I) safety measures which have been allocated to the BBCR.

The B/B is a self-contained building located on site completely separate from the R/B and C/B with enough distance from the MCR and combination-structures of the R/B so they are not both affected simultaneously by the same hazard. It is located close enough however to still allow it to function to the high degree of reliability required, taking account of ease of access for the operators. The access route leading to the B/B is designed to be kept safe for personnel usage in all foreseeable accident conditions. The B/B contains all the controls and displays required for its intended function on the B/B Control Panels (BBCPs).

As described in 30.3.1, the UK ABWR has a large degree of automation, and the contribution of the operations team with respect to the operational safety goals of the plant during normal operations (including start-up and shut down modes) consists largely of monitoring the plant to ensure it stays within its safe operating envelope. The crew in the MCR monitor plant parameters at a frequency based on importance to safety and plant conditions. It is assumed that crew members communicate effectively to each other, as described in Section 30.3.4, when they need to share important information, seek confirmation of diagnosis and action needed, and/or to have verification of an action taken.

During abnormal and accident conditions, the role of the crew with regards to the plant changes, and they are required to take a more active role in maintaining or returning the plant to safe conditions. Their monitoring context changes from “normal” plant to needing a heightened awareness required to ensure automated safety systems have correctly initiated and, where necessary, diagnose alarms and implement abnormal and/or emergency operating procedures accordingly.

The operating system functionality includes an alarm system that directs the MCR personnel attention to any changing conditions that may challenge safety. The alarm system is designed wherever possible to ensure that:

- alarm conditions are clearly indicated, in priority order based on importance,

- nuisance alarms are minimised,
- alarms are limited to situations where action is required, and
- alarm "flooding" is minimised by showing only the highest priority alarms first during upsets that trigger multiple alarm conditions.

Because the UK ABWR is a highly-automated plant, often the "actions" required of the operator during alarm states are limited to a change monitoring "regime". In other words, the operators need to make themselves aware of the change in conditions that might threaten plant safety and monitor the automated system(s) response to ensure they operate correctly. In some cases, specific operator actions are required to maintain or restore the plant in a safe state. These are detailed in the list of HBSCs for UK ABWR as described in Chapter 27: Human Factors and in the HBSC Report [Ref-4].

As described in Section 30.3, it is assumed that during normal and fault conditions, the CRO(s) are responsible for control of the unit and will refer to approved procedures and other operating documents as required to keep or return the plant to within its defined safe operating envelope. They are supported as required by the FOs who will monitor and control the plant at local control panels or at the plant equipment itself. The MCRS provides support and oversight to the CROs and FOs.

If an event progresses beyond conditions considered in the design basis, and in particular if it develops into a severe accident, the operators are assumed responsible for implementing the applicable emergency operating procedures, and severe accident management guidelines, responding to emerging degraded plant conditions as required. The general Command and Control philosophy assumed to be in place for such events is described in 30.3.3.

The generic approach to plant operation for the UK ABWR, i.e. expected control sequence for plant start-up and shutdown, is stated in the Topic Report on Approach to Operation of UK ABWR [Ref-10]. This document describes the generic normal start-up procedure from plant start-up preparation to rated power operation, normal shutdown procedure from rated power, summary of basic procedure at reactor scram event, and assumed generic maintenance sequence. Although based on the reference J-ABWR operating policy, this provides a basis for the development of the future licensee's operations philosophy.

30.4.1 Operating Documentation

Requirements and assumptions claimed in the overall safety case are reflected in the operating documents in order to ensure the plant is operated consistently with them.

Plant operating procedures should be further developed by the future licensee based on assumptions and requirements identified in plant design and safety case documents, i.e. Human Factors Engineering Analyses, Probability Safety Assessment, as well as existing operating ABWR plant experience. Their verification and validation process is one of the objectives of the commissioning phase.

The operating procedures for the UK ABWR consist of operating rules and operating instructions. The operating rules are derived from the safety case and will define and justify the safe operating envelope. The operating rules that have been identified in GDA are contained in the GTS document [Ref-1]. The operating instructions describe the tasks to be performed by the operators to monitor and control the plant. The operating procedures will encompass all planned evolutions and responses to unplanned events.

The operating documentation describing the actions to be performed (operating instructions) has not yet been developed for UK ABWR. The development of these documents is the responsibility of the future licensee and is therefore outside the scope of GDA. The detailed operating documents should be developed from upstream documents defining and justifying the operating strategy (operating rules).

The general objective of the GTS developed for GDA is to set out the rules that must be observed during normal operation of the nuclear plant in order to keep it within the safe operating envelope, as justified by the safety analyses presented in the safety case. The GTS is described in section 30.4.2 below.

The operating procedures describe the operations to be carried out to achieve a safe and stable state appropriate to each situation.

Examples of types of operating procedures include the following:

System Operating Procedure (SOP): provide instructions for energising, filling, venting, draining, starting up, shutting down, changing modes of operation, returning to service following testing (if not given in the applicable testing procedure), and other instructions appropriate for operation of systems important to safety.

Unit Operating Procedure (UOP): provide instructions for the integrated operations of the plant (e.g., startup, shutdown, power operation and load changing, process monitoring, and fuel handling).

Abnormal Operating Procedure (AOP): specify operator actions for restoring an operating variable to its normal controlled value when it departs from its normal range, or to restore normal operating conditions following a transient. They are event based fault response procedures, with operator actions required to avoid scram. AOPs are used for postulated events that have been analysed and discussed in the design basis analyses, and are limited to a single initiating event followed by successful operation of the safety systems designed to respond to those events. They provide detailed instructions on how to respond to specific plant abnormal conditions, i.e. loss of instrument air, actions on receipt of alarms, etc.

Emergency Operating Procedure (EOP): specify direct actions necessary for the operators to mitigate the consequences of events when operator actions are needed to restore the plant to a safe and stable state. The aim of emergency operation is to restore the plant to safe and stable conditions, while ensuring the fundamental safety functions are achieved.

Alarm Procedure: guide the operator actions for responding to plant alarms.

Administration Procedures are those procedures that:

- describe the administrative controls that apply to specific plant operational activities or to plant operating modes,
- define the required controls for the daily activities of plant personnel.

Examples of such procedures are: MCR access control, operation of plant equipment, procedure change control, plant status and configuration, etc.

Severe Accident Management Guidelines (SAMGs): are symptom based fault response guidelines, for faults resulting in core damage and non-coolable geometry. The Technical Support Centre, under control of the Emergency Control Centre, uses these guidelines with assistance from the MCR and plant teams as required.

Surveillance Test Procedures: cover all surveillance requirements from the GTS [Ref-1].

30.4.2 Generic Technical Specifications

The purposes of the Generic Technical Specifications for GDA [Ref-1] are to identify limits and conditions upon plant operation that are necessary to prevent the possibility of an abnormal situation or event giving rise to an imminent threat to nuclear safety. They provide the required information to assist the future licensee to develop its corresponding site specific Operating Technical Specifications (OTS). The GTS for GDA define the operational limits on parameters and corresponding actions required to ensure that station operations remain inside the limits and requirements of the GDA Safety Case, with a preserved level of margin (i.e. the operating envelope must always sit inside the safety case envelope), and contain the following:

- The operating limits for the parameters and system configurations that must be met to remain within the safe operating envelope that is justified by the safety case. These are the LCOs, which are described further in section 30.7,
- The safety limits and limiting safety system settings,
- The specific operating modes in which each LCO applies,
- The required actions when a parameter limit or system configuration is outside of the safe operating envelope, i.e. an LCO requirement is not met,
- The time limit allowed to return the parameter or system to within the safe operating envelope (described as the Completion Time),
- The surveillance tests that must be performed to verify a parameter or system is within the safe operating envelope, and

- The frequency of the surveillance tests.

The GTS are derived from the assumptions contained in the safety case and define the parameters and configurations of the SSCs required to ensure the safe operation of the plant. The GTS apply to all operating modes and define the SSCs availability and operability requirements, including any necessary auxiliaries, supports and electrical power supplies, to perform their functions and meet the safety objectives.

30.4.3 Maintenance and Inspection

Maintenance is one of operational activities and involves all technical, administrative and management actions during the service life cycle of an item of equipment, in order to maintain it in, or restore it to, a state in which it can carry out the function it is required to perform.

Whereas the operators and MCR are remote from the plant systems and equipment, direct plant interactions are performed by the FOs (to support operations) and maintenance personnel. The goal of the maintenance personnel with respect to plant safety is to support the availability and operability of the SSCs to perform their design functions through the implementation of a preventative maintenance (PM) programme. The ability to access local control panels and plant equipment controls and indications, and effectively operate or maintain, them has been considered throughout the UK ABWR design (plant layout, plant equipment, HMIs, etc.) using the HFE Spec [Ref-6] to implement applicable HF requirements from the list of standards and guidance applicable to relevant aspects of the design.

The Maintenance and Inspection programme should be established prior to the start of commissioning, will be updated to incorporate lessons learned from commissioning and will see continual improvements over the operational life of the plant.

The programme should be developed to maximise the availability and reliability of equipment such that the equipment performance achieves its design function, with the ultimate goal of avoiding in-service equipment failures and ensuring the ability of the plant to operate continuously between refuelling outages. The programme will include activities associated with reliability centred maintenance, preventive maintenance (periodic, predictive, and planned), surveillance and testing and equipment performance and condition monitoring. The programme will be based on a clear understanding of the equipment, both in terms of the probability and consequence of failures. The equipment details will be provided by the equipment manufacturers and the maintenance schedules will be developed through the incorporation of relevant operating experience.

Separate and independent inspection and testing activities will also be completed to align with the requirements of UK legislation. These activities are statutory and time based and extensions to these timings are not usually granted.

The distribution and allocation of maintenance, inspections and testing activities between planned outages and at power operation, requires due consideration of the plant configurations required to

perform those activities. The plant configurations should be specified within the operational documentation and should ensure that the risks associated with these activities are ALARP and bounded by the Safety Case and Technical Specifications. Unit availability will be optimised through the performance of preventive maintenance activities both during power operation and during outages, and should be aligned with the assumptions of the safety analysis that is presented in the Safety Case.

PM involves all actions carried out on an item of equipment to reduce the probability of its operational failure. The aim of preventive maintenance is to ensure that, throughout the service life of the plant, the objectives of safety, availability and cost are achieved, subject to the requirements of ALARP, while complying with applicable rules for the protection of the environment, staff safety, radiation protection and other regulations in force.

All maintenance activities are expected to be concluded by appropriate post-maintenance tests to confirm that the equipment meets the specific performance criteria required by the plant.

When conducting maintenance and testing, plant safety is achieved through the application of the OTS, which detail minimum diverse plant (i.e. system “divisions”) availability/operability and time limits on degraded plant configurations before alternative actions must be taken. The bases for these controls are derived from the safety analyses in the Safety Case. The design of the UK ABWR to support these operational controls is described further in Section 30.5 Plant Status Control.

In order to optimise the PM programme, optimising system availability whilst ensuring no unnecessary intervention is required on functional plant, the UK ABWR maintenance programme will outline the nature, extent and frequency of inspections, tests, overhauls and replacements of components and equipment based on Reliability-Centred Maintenance analysis methods. Such analysis methods take inputs from the safety case and reliability data from operating experience. A robust PM programme maintains or replaces equipment before it fails but not more often than needed, and results in a highly reliable plant with reduced risk to personnel (i.e. radiation exposure, injury, etc.). An example of developing an Equipment Reliability-based PM programme is described in the industry guidance document, INPO AP-913 [Ref-11]. The assumed maintenance philosophy for UK ABWR, developed for the future licensee, is described in the Maintenance Philosophy [Ref-12], and Maintenance Design Philosophy [Ref-13].

The plant layout design optimises the ease with which operators can perform the following:

- Plant isolation,
- Maintenance Activities,
- De-isolation and return to service testing, and
- Condition based monitoring.

Support is assumed to be provided to operations and maintenance through a suitably implemented work management process that covers all areas and functions of the plant, for both online work and during planned outage periods (this may be covered by a separate work management programme specific to outages, for example Outage Management. In addition, generic maintenance sequence is shown in the Approach to Operation Topic Report [Ref-10].). These processes are expected to be developed by the future licensee. However, it is assumed that the process integrates, coordinates and schedules all plant activities and defines the responsibilities and interfaces between the functional organisations. It is also assumed to be designed to minimise operational risk through the prioritised sequencing of tasks, detailed task analysis and risk assessments prior to work execution. An example of best practise in Work Management process is described in the industry guidance document, INPO AP-928 [Ref-14].

30.4.4 Operating Programmes

The operating/work programmes define the processes and procedures that govern the safe operation and maintenance of the plant. These programmes will provide an important input into the ALARP justification for safe plant operation. Relatively few programmes are required during the early years of operation and a schedule for their implementation should be established prior to commissioning and hand-over to operations. These programmes should be based upon the engineering, construction, and commissioning data records.

30.5 Plant Status Control

Operators are responsible for the control and monitoring of the status of the plant and are required to be fully aware of the operational state and availability/operability of SSCs, together with their associated functions, at all times. It is assumed that operations personnel ensure that equipment and systems are in the correct configuration and operating if required, and maintenance personnel ensure that equipment is maintained, available and operable as required, in order to meet the specified safe operating envelope for each plant state.

These envelopes and required plant configurations are established for GDA through the application of the GTS. It is assumed that only suitably qualified and experienced personnel (SQEP) will perform operations and maintenance tasks at the station, and that work will only be performed once it has been authorised by operations.

The design is such that the plant status can be managed and controlled to facilitate configuration changes necessity for periodic maintenance, modifications, and testing activities. Furthermore, various design features ensure that required minimum plant availability/operability is achieved at all times through interlocks and automatic realignment. Specifically, the UK ABWR includes such features as:

- Interlocks that prevent an operator from removing a system or component from service if it violates the requirements for availability in the GTS,
- Interlocks that prevent certain restart sequences if identified plant is not online,
- SSCs that require frequent test and inspection are made easily accessible and safe for performing routine tasks, either locally or remotely, when online. This minimises requirements to take plant out of service, which in turn reduces dose to personnel, risk of latent maintenance errors and risk of incorrect plant configuration,
- Lockout and isolation features throughout the plant that clearly identify SSCs that are not in service,
- Interlocking key systems (e.g. Fortress locking system) linked to operation to prevent leaving plant in an unavailable state,
- Automatic re-alignment on demand of any safety systems that might inadvertently have been left unavailable through being placed in bypass, maintenance or test mode, and
- Alarms for any SSCs required for safety-related operations that have become functionally compromised or unavailable.

The generic approach to plant operation for the UK ABWR is described in the “Topic Report – Approach to Operation of UK ABWR” [Ref-10]. The topic report describes the basic flow of operations in different operating modes and shows the intended steps for managing and controlling the above generic plant situations, based on the reference J-ABWR design.

30.6 UK ABWR Operations Personnel Description

This section provides a high-level description of the assumed or minimum requirements for the personnel who will be responsible for operational activities within the UK ABWR. It is based on the User Group Description that is detailed in the COR [Ref-2]. It should be noted that the following are the basic details related to safe operations within UK ABWR, to the extent they can be determined within GDA. Many of these aspects of the operating organisation can only be developed fully by the future licensee. Hence, is expected that this section will be developed further in the site-specific PCSR.

30.6.1 Operations Personnel Overview

The operations crews at UK ABWR power plants will be responsible for the safe and compliant operation of the plant. This requires a minimum complement of operations personnel to be on site and in post 24 hours a day and seven days a week. The formulation of a nuclear safety baseline (i.e. minimum or baseline organisation required to maintain nuclear safety) is a requirement of the UK regulator, but this can only be done by the future licensee. For the purposes of GDA, the key operations staffing is assumed to be comprised primarily of: Operations Manager, Shift Managers, MCRSs, CROs, FOs, maintenance technicians, and day operations staff.

In addition to operating the reactor unit and balance of plant, these personnel will also:

- Perform maintenance tasks in accordance with nuclear and other maintenance schedules,
- Perform surveillance testing activities as required by the Technical Specifications or similar,
- Respond to unexpected events to prevent or mitigate their consequences and to perform system health checks to confirm their status following recovery from such events,
- Isolate plant and equipment from service and release it for maintenance and testing,
- Accept plant and equipment back into service upon completion of maintenance and testing,
- Process and store new and spent fuel,and
- Conduct refuelling outages, which will include performing planned off-load maintenance.

30.6.2 Operation Complement

The UK ABWR will need to have a minimum complement of:

- One Shift Manager (for the entire station),
- One MCRS (for each reactor unit and each shift) †,

- One CRO (for each reactor unit and each shift) †, and
- A suitable number of FOs (e.g. one reactor, one turbine, one BOP, one Radwaste).

Increased numbers may be required for specific plant status or operational conditions such as during start-up, hot or cold shutdown, or during refuelling.

†Note it is expected that the normal complement will be two CROs and a MCRS per shift per unit.

However, the MCR needs a minimum of only two fully SQEP MCR operators and two FOs during all plant conditions to meet the requirements of this safety case. The MCR operators are assumed to be either the MCRS and a CRO or two CROs if necessary (i.e. due to temporary absence of the MCRS). Due to independent checks and oversight tasks expected to be required of the Supervisor particularly during fault and accident scenarios, at least one person acting in the role of Supervisor or Duly Authorised Person (DAP) (e.g. a delegated "lead" CRO) is required in the MCR at all times.

It is expected that this minimum number of personnel (i.e. two MCR operators plus two FOs) will be able to perform all operator functions in all plant conditions, noting that additional FOs from other units and the Shift Manager are also available to support as appropriate during fault and accident scenarios. This gives the bounding worst-case minimum MCR complement that has been used for all underpinning HF analysis within the UK ABWR safety case.

In addition to the above MCR personnel, if there are two reactor units, they are assumed to share the following support personnel (each shift; numbers of each job role are assumed to be sufficient to perform required tasks) to help achieve the overall operations and maintenance safety goals:

- FOs for covering common plant,
- Maintenance Technicians,
- Maintenance Engineer(s),
- Work Management team,
- Fire Fighting and Safety specialists,
- Administrative support persons,and
- Security specialists and officers.

30.6.3 Roles and Responsibilities

The following are the assumed main responsibilities for each of the job roles within the Operations shift, which are described in greater detail in the COR [Ref-2]. Note that these should be confirmed and further developed in the site-specific PCSR.

Shift Manager

The Shift Manager is responsible for the safe and compliant operation of the power station. The Shift Manager oversees the activities of the entire plant. During accident scenarios, the Shift Manager is assumed to assist the MCRS in supporting and advising the CROs, particularly maintaining the overall incident and site "big picture" and incident management strategy. However, despite this assumption, note that the Shift Manager role within accident scenarios is not required as part of the minimum MCR operations complement within the safety case (see Section 30.6.2).

For site incidents or nuclear emergencies, the Shift Manager is assumed to take control of the incident from whichever MCR is closest at the time of the particular event. As such, all the emergency response facilities will be duplicated in each unit's MCR. If a site incident is declared, the Shift Manager is assumed to be the acting Emergency Controller (EC) until the duty EC is confirmed as in-post and the Emergency Control Centre (ECC) is established.

MCR Supervisor

Each reactor unit will be under the supervision of a MCRS, who is responsible for safe and compliant operation of their respective unit. The MCRS is assumed to report to the Shift Manager and oversees the CROs and FOs.

The MCRS is assumed to act as the lead DAP for their assigned reactor unit and is responsible for the release of nuclear safety related plant or equipment for maintenance. It is assumed that the DAP role with regards to releasing plant may be delegated to a DAP situated within the Maintenance Facility, to help minimise distractions within the MCR.

The MCRS is assumed further responsibility for such things as:

- services and fire protection for their respective unit,
- overseeing access and egress to and from the MCR, and
- transmitting instructions and information between the National Grid and the CRO.

During an emergency or incident, the MCRS is assumed to maintain oversight of their unit and its MCR crew, including FOs. The MCRS is further assumed to independently verify plant conditions and success paths for recovery from incidents (such as independent verification of fault diagnosis, successful actuation of required safety functions and monitoring of critical safety functions).

Control Room Operators

The CROs are responsible for control and monitoring of the main plant items from within the MCR. All MCR operators will be DAPs with the competency and ability to operate all interfaces at any console within the MCR. In the case where the MCRS is temporarily absent, a second CRO is assumed to be assigned to that role whilst the first CRO remains in control of the unit.

In the event of plant faults and design basis events, the CROs are assumed to be responsible for monitoring to confirm that the automated responses have implemented correctly for achieving control of the affected systems or plant equipment. If necessary, the CROs are responsible for taking action to provide backup in the case where automated systems have failed.

Field Operators

The unit will have a suitable number of dedicated FOs. The FOs will take direction from the MCR and perform: plant patrols, routine simple maintenance (procedurally governed), surveillance checks and actions local to plant. Designated FOs will also perform isolations of plant for maintenance.

During an incident or emergency, two FOs are assumed to be designated to assist the respective unit's MCR with any actions local to plant. The remainder of the FOs are assumed to be available to support the Emergency Response Team (ERT) and come under the command of the Shift Manager or EC. In particular the FOs are expected to help with the "first responders" for fire and safety response, personnel who deal with the incident local to plant until relieved by local emergency crews in the event of a fire or first aid incident, or the on-call emergency response crews.

Maintenance Personnel

Although the exact nature of the maintenance organisation within each operating site has yet to be determined, it is assumed that a Maintenance Team will undertake corrective and preventative maintenance of the power plant, as described below. Note that the maintenance discussed in this section does not include any periodic or scheduled testing on SSCs that is required to meet Technical Specifications and that is performed by operating plant from the MCR. Such surveillance testing must be performed by CROs and is included in 3) above.

Maintenance work on the site is assumed to be controlled by a Maintenance Manager who bears ultimate responsibility for ensuring that the plant material condition is maintained to required levels. The Maintenance Manager oversees the entire maintenance function at the site. The Maintenance Manager is supported in this role by Maintenance Team Leads, each of whom leads a team of day and shift maintenance crews.

The Maintenance Team Leads ensure the maintenance work activities are planned, scheduled and undertaken in a suitable manner to optimise plant safety, reliability and availability. Release of plant for maintenance and permissions to start work will be provided in accordance with the nuclear site licence condition compliance arrangements.

The shift maintenance crews are assumed to be primarily responsible for on-line testing out-of-hours and response to emergent and time-critical corrective maintenance, whilst the day crews are assumed to be primarily responsible for less-urgent corrective maintenance and preventative maintenance, inspection and testing. The shift crews are assumed to be supported by a dedicated "Fix-It-Now"

team that focus on addressing urgent emergent maintenance activities particularly those with time limits due to LCOs. This allows the normal maintenance crews to focus on required scheduled and planned work thus minimising the risk of maintenance task backlog.

Work Management Team

Although not part of the Plant Operations or EMIT conducted by both operations and maintenance personnel is expected to be supported by an appropriately structured Work Management Team, comprising technicians and engineers suitably competent in planning and coordinating all the maintenance work and other engineering programmes on site.

In particular, the personnel in the Work Management team (or equivalent) are expected to be experienced in operations and maintenance activities at a UK ABWR, and also be trained in planning, operational decision-making, and nuclear safety risk assessment and risk management. It is essential for them to be able to plan key tasks on site with a broad understanding of the plant function, operations, nuclear safety and LCOs such that any scheduling conflicts are managed effectively whilst the required nuclear safety conditions are maintained at all times.

The existence and responsibilities of such a team has been assumed within UK ABWR design when defining the minimum MCR personnel complement. The role that the Work Management Team (or equivalent) perform is important, extensive and needs suitable focus. It cannot be given to the personnel within the MCR, and such a team is specifically assumed to exist to ensure the workload and administrative burden relating to work management is:

- removed from the MCR operations team such that they are not overloaded and they can focus on their core task of operating and monitoring the plant safely, and
- undertaken by suitably competent personnel who understand the plant and the impact of the decisions they make with regards scheduling of work done on the plant.

The Work Management Team (or equivalent) are expected to be responsible for: receiving any emergent or unplanned maintenance requests; managing the implementation of the planned work schedule; specifying the list and priority of the maintenance tasks for any given work week; preparing the packages of documentation required to conduct the tasks; and coordinating the isolations required to achieve the work safely and effectively.

30.6.4 Physical Capabilities and Attributes

To ensure the environment and equipment are designed to allow the UK ABWR operations staff to perform their required tasks effectively and safely, the considerable variations in shapes, sizes and strengths of users, as well as the task requirements have been considered throughout the GDA HF design activities. Workspaces are designed based on the defining or limiting physical characteristics

(e.g. arm length, shoulder width, height, etc.). This process allows the workspaces in the plant to be designed in such a way that they will be usable by the whole range of potential users. For example, providing access for the tallest and broadest of users whilst ensuring the smallest user can reach and use all necessary controls.

For the purposes of design, the UK ABWR operations staff has been defined as being within the UK 5th percentile female to the 95th percentile male range. Further information on the sources of anthropometric data, how it is used and how compromises with other design requirements are managed can be found in the COR [Ref-2].

30.6.5 Training and Competence

Each job role within the UK ABWR Operations organisation is expected to have a set of basic requirements in terms of qualifications, training and experience for the individual to be considered competent. These role specific requirements and any additional general training that all Plant Operations staff will be expected to have completed are described in more detail in the COR [Ref-2]. However, these aspects of the operating organisation can only be fully developed post GDA phase by the future licensee.

The assumption for all HF analysis that underpins the GDA PCSR is that training and competence is adequate to allow personnel in any job role to carry out the expected actions related to safety knowledgeably and within a timely manner.

30.6.6 Social and Cultural Characteristics

Previous experiences within different social, cultural and industrial backgrounds lead to the creation of mental models that drive an individual's expectations for what is considered normal in regards to behaviours, team dynamics, terminology, etc. These expectations can influence task performance and as such they have been considered during GDA both within the design (e.g. UK expectation for control direction meaning) and within the HF analysis through the use of performance influencing factors in human error analysis.

Information on the specific social, cultural and industrial characteristics and stereotypes considered during the design phase of the UK ABWR is detailed further within the COR [Ref-2].

30.7 Assumptions, Limits and Conditions for Operation

30.7.1 Purpose

One purpose of the generic PCSR is to identify constraints that should be applied by the future licensee of a UK ABWR plant to ensure safety during normal operation, fault and accident conditions. Some of these constraints are maximum or minimum limits on the values of system parameters, such as pressure or temperature, whilst others are conditional, such as prohibiting certain operating modes or certain conditions within modes or requiring a minimum level of availability of required SSC. They are collectively described in other chapters of the GDA PCSR as LCOs. The definition and context of Assumptions, LCOs in GDA is described in PCSR Chapter 4: Safety Management throughout Plant Lifecycle,, section 4.12.

In the operation phase, the assumptions and LCOs made in the safety case are to be utilised to ensure that the plant is maintained within safe operating condition. Assumptions and LCOs are described further below.

30.7.2 Limits and Conditions

During normal operation, the plant is required to be maintained within a safe operating envelope to prevent situations arising that could lead to anticipated operational occurrences or accident conditions, and to help minimise the consequences of such events if they do occur. In addition, if an unexpected deviation from an LCO actually occurs during normal operation, then the plant should be returned to a safe condition as soon as possible and the event should be investigated and any appropriate corrective actions undertaken.

It is assumed that the future licensee will develop OTS based on the GTS [Ref-1], as well as develop appropriate operating instructions and procedures, and will ensure that the plant is operated in accordance with them thereby ensuring that the plant remains within the operating envelope defined by the safety case. The purpose of the GTS is to identify limits and conditions for plant operation necessary to prevent an abnormal situation or event arising and giving rise to a threat to nuclear safety, as described in section 30.4.2. Also, the GTS are derived from the assumptions contained in the safety case made within the relevant other chapters of this PCSR, and their supporting documents, and define the parameters and configurations of the SSCs required to ensure the safe operation of the plant.

30.7.3 Assumptions

The list of assumptions below are the specific to the Operations topic area, as presented within this chapter of the PCSR, that are key to the effective implementation of the operational principles and strategy:

- The level of automation is assumed to be generally the same as for the J-ABWR with the exception of known improvements to further automate some safety system initiation (described in Chapter 27: Human Factors).

- It is assumed that actions of operations and maintenance personnel will be such that they contribute to keeping the plant within its LCOs, and thus support the plant achieving its safety goals. Specifically, it is assumed that operations personnel will ensure that equipment and systems are in the correct configuration and operating if required, and maintenance personnel will ensure that equipment is maintained, available and operable as required.

- It is assumed that the full minimum normal complement of operations and maintenance personnel required to achieve the above assumption will be determined by the future licensee and that they will be on site and in post at all times (i.e. the Nuclear Safety Baseline for personnel will be established, maintained and implemented at all times).

- It is assumed that only SQEP will perform operations and maintenance tasks at the station, and that work will only be performed once it has been authorised by operations.

- The Command and Control philosophy that will be adopted by the future licensee for the UK ABWR is assumed to be similar to that used in existing UK nuclear power plants. This should include roles, responsibilities, training, communications and availability of operational staff in normal operations, and also any changes to those elements that might be needed for effective response to beyond design basis events, emergencies and severe accidents.

- The GTSs are assumed to be developed into OTSs (with some limited differences due to site-specific considerations) which will then be incorporated as required into a suitable hierarchy and organisation of operational procedures to ensure the requirements for plant operations related to nuclear safety are clearly documented.

- It is assumed that daily management of the plant will be supported by a risk-based operational decision-making policy, in which operational decisions concerning all plant conditions that could affect safe plant operation are made based on an in-depth understanding of short- and long-term operational risks, as well as the potential effects of alternative operational options.

- It is assumed that the future licensee will implement, and their operations personnel will use, an effective communications management practice. This should include: techniques to minimise human performance errors in verbal communications; effective, formalised shift handover arrangements; and implementation of a “visible safety case” through effective role descriptions, procedures and training.

- In order to support the achievement of effective communications in plant operational tasks during all plant conditions, portable communications equipment and any equipment not part of the generic design (i.e. specified by the future licensee) are assumed to meet the

same requirements for availability and clarity as the equipment that is a permanent part of the UK ABWR plant.

- It is assumed that an effective maintenance and inspection programme will be implemented that maximises the availability and reliability of equipment such that the equipment performance achieves its design function, whilst taking into account HF considerations such as minimising unnecessary EMIT burden on plant personnel and reducing planned dose uptake. It is further assumed that this programme will be established prior to the start of commissioning, will be updated to incorporate lessons learned from commissioning and will see continual improvements over the operational life of the plant.

- It is assumed that support will be provided to operations and maintenance activities through a suitably implemented work management process and associated resources. These should cover all areas and functions of the plant, for both online work and during planned outage periods; integrates, coordinates and schedules all plant activities and defines the responsibilities and interfaces between the functional organisations; and is designed to minimise operational risk through the prioritised sequencing of tasks, detailed task analysis and risk assessments prior to work execution.

Related Assumptions

The assumptions made in the GDA safety case analysis of the generic UK ABWR that are described in other GDA PCSR chapters (e.g. Chapter 24: Design Basis Analysis) are fully consistent with the set of LCOs in the GTS [Ref-1]. By demonstrating that all of the relevant analysis acceptance criteria are met when applying these assumptions, the analysis confirms that the LCOs for GDA meet their objective of defining an appropriate safe operating envelope.

By managing an actual UK ABWR station in such a way that its operation always remains within the safe operating envelope defined by the site-specific LCOs in the OTS, it follows that its operation will be bounded by all assumptions made in the site-specific Safety Case that generated those LCOs. This ensures that the safety case remains valid for all operating conditions. In general, the site-specific LCOs in the OTS are expected to be similar to the GDA LCOs in the GTS, but there are likely to be some limited differences due to site-specific considerations. These will be justified in the site-specific safety case.

As described in section 30.4.2, assumptions that are identified in various related topic areas within the safety case contribute to development of the GTS within GDA, and eventually form part of the OTS post-GDA. Verification and validation of the procedures that derive from the OTS will be conducted during commissioning and periodical or ongoing review is conducted afterwards. These assumptions are specific to each LCO and GTS and are not repeated in this section.

In addition, any assumptions that underpin the GDA design that have been used to develop operational limits, such as initial setpoint values, should be validated during commissioning. These

assumptions are listed in the relevant PCSR chapters and supporting documents for those design assumptions and are not repeated in this section.

Further, the assumptions regarding the operational concept that form the entire basis of the COR [Ref-2] were used to underpin the HF programme of analysis and support within GDA. Such assumptions are therefore integral to the justification of the GDA design as ALARP in supporting the HBSCs identified through the DBA (Chapter 24: Design Basis Analysis), PSA (Chapter 25: Probabilistic Safety Assessment), SAA (Chapter 26: Beyond Design Basis and Severe Accident Analysis). These assumptions will also be further verified and validated, or changed in post-GDA phases as the actual operational arrangements are developed and the conduct of operations is set in place. These HF operational assumptions are not repeated in this section as they are largely listed within Chapter 27: Human Factors.

30.8 Summary of ALARP Justification

This section presents a high level overview of how the ALARP principle has been applied for the Operations chapter within the GDA and how this contributes to the overall ALARP argument for the UK ABWR.

Generic PCSR Chapter 28: ALARP Evaluation presents the high level approach taken for demonstrating ALARP across all aspects of the design and operation. It presents an overview of how the UK ABWR design has evolved, how the further options that have been considered across all technical areas have resulted in a number of design changes and how these contribute to the overall ALARP case. The approach to undertaking ALARP Assessment during GDA is described in the GDA ALARP Methodology [Ref-15] and Safety Case Development Manual [Ref-16].

The responsibility for developing and implementing operational arrangements (including arrangements for EMIT) rests with the future licensee organisation.

However, within GDA, the demonstration that risks related to UK ABWR operations have been managed to ALARP can be achieved by:

- Adequate and early definition of expected UK Concept of Operations, as far as is possible within the constraints of GDA scope, developed with valid input from a future licensee.
- Suitable and sufficient incorporation of the UK Concept of Operations in any evolutionary design activities, including optioneering studies relevant to usability/maintainability and HF.
- Consistent and comprehensive consideration, across the whole safety case, of the expected features of the future operating organisation.
- Clear definition of the aspects of the design that rely on operators and operational arrangements to enable the plant to remain within a safe envelope during all operating modes, including development of the GDA GTS [Ref-1], and demonstration that those aspects are within the expected capability of the future operating organisation
- Consideration within the design of the conduct of maintenance through development of the Maintenance Philosophy [Ref-12] and the Maintenance Design Philosophy [Ref-13].

Through successful management of the above elements it is possible to demonstrate that relevant aspects of the design are such that they will align with future plant operations and will allow those operations to contribute to the justification that risks from an UK ABWR station have been reduced ALARP.

The above illustrates the links between this chapter and PCSR Chapters 21 and 27 on HMI and HF, respectively. The ALARP statements for those chapters link to, and partly form the basis for, this chapter's ALARP justification.

30.8.1 Risks Related to Operations

The risks related to operations that need to be managed to ALARP within the operations topic area are where human actions related to operating and maintaining the plant:

- fail to keep the plant within its normal safe plant state or keep personnel protected from known/planned radiation hazards,
- inadvertently take the plant into an abnormal or fault scenario or expose personnel to unplanned radiation hazards, and/or
- when in an abnormal or fault scenario, fail to support the return of the plant as required to a safe state or protect personnel from unplanned radiation hazards during the fault.

These are risks that:

- could arise during the operational stage of the plant lifecycle (noting that commissioning and decommissioning are covered in PCSR Chapters 29 and 31, respectively),
- could arise from any activities where human interaction is needed to operate and maintain the plant, in all operating modes defined within the safety case (see PCSR Chapter 5: General Design Aspects), and
- are specifically related to plant monitoring, control, and EMIT activities (not broader site-wide activities in emergencies, which are covered in PCSR Chapter 22: Emergency Preparedness).

Specifically for GDA, the relevant risks within the Operations chapter relate to inability of the UK ABWR design to support optimal performance of operations and failure to identify operational assumptions and requirements clearly, such that the future operating organisation cannot design appropriate operational arrangements.

30.8.2 Relevant Good Practice and Identification of Gaps

Operating arrangements such as procedures, competence management, training, and organisation support systems can enable the risks identified above to be managed to be ALARP, if they are implemented suitably. These arrangements have to be developed to provide more in-depth requirements during the site-specific stage. ONR's assessment of whether to grant a licence will include assessing whether the operating organisation meets those requirements. Therefore, UK Relevant Good Practice (RGP) for operational considerations in design focuses on creating the operating organisation and the associated arrangements. The applicability of such RGP to the design of the basic or generic plant during the GDA stage is limited.

Nevertheless, the requirements for operating the plant are either directly specified by, or the basis for them is laid out by, the plant designer in the generic design stage. Therefore, some of the

requirements within the RGP have implications for activities and actions within the early design of the plant and for the communication of the assumptions and LCOs from the Generic PCSR to the future licensee. This RGP is generally outlined within the ONR SAPs and can be derived from the ONR TAGs (notably NS-TAST-GD-035 'Limits and Conditions For Nuclear Safety (Operating Rules)') regarding definition of limits and conditions for operation for nuclear safety and NS-TAST-GD-058 regarding integration of HF in design. Guidance is also provided in the IAEA Nuclear Safety Guide NS-G-2.2 [Ref-17] particularly on early development of operational rules.

The following bullet points summarise the key aspects of the referenced RGP that relate to consideration of the future operating organisation, and operational assumptions and rules, within the generic design stage. (Note that the use of the words "Technical Specifications" and "Operating Rules" in the text below is used within the RGP; it should be assumed to read "or equivalent" in all cases. Also, note that "operating rules" are the responsibility of the future operating organisation.)

- The designer defines the assumed operating organisation within a Concept of Operations document. The document needs to include such things as: the operational purpose and requirements of the plant system(s); functions to be performed and who by (human or system); the basic command and control philosophy; the preliminary or assumed staffing concept, including number, team structure, roles, responsibilities, competence, and physical and cognitive characteristics; and the basic description of the expected eventual system design, including potential working environments in different plant states. It should be developed wherever possible in consultation with a future licensee organisation.

- The designer identifies clearly and records any further assumptions about operational arrangements (including EMIT work management, etc.) that need to be made when designing features of the plant and when performing all forms of safety analysis to feed into the safety case.

- The designer defines for any future licensees the operating modes which outline all the expected plant states that the design and safety case apply to, such as normal modes of operation or shutdown, abnormal modes, fault scenarios within the design basis, etc. and the LCOs that apply within each mode.

- The designer and safety analysts note any specific actions, either in operations or through EMIT, that are required to maintain the plant in, or return it to a safe state, for each of the operating modes. The operations need to include all plant that has an impact on nuclear safety including not only reactor and balance of plant operations, but fuel handling and storage, and management of radioactive waste. The specific requirements of plant operation to meet the safety case (i.e. the LCOs) are expected to be implemented by the future licensee through Operating Rules (ORs) or administrative controls. These need to be specified to all levels of Defence in Depth. The diagram in ONR's TAG-035 (NS-TAST-GD-035) clearly illustrates this identification requirement; it is shown in Figure 30.8-1 below.

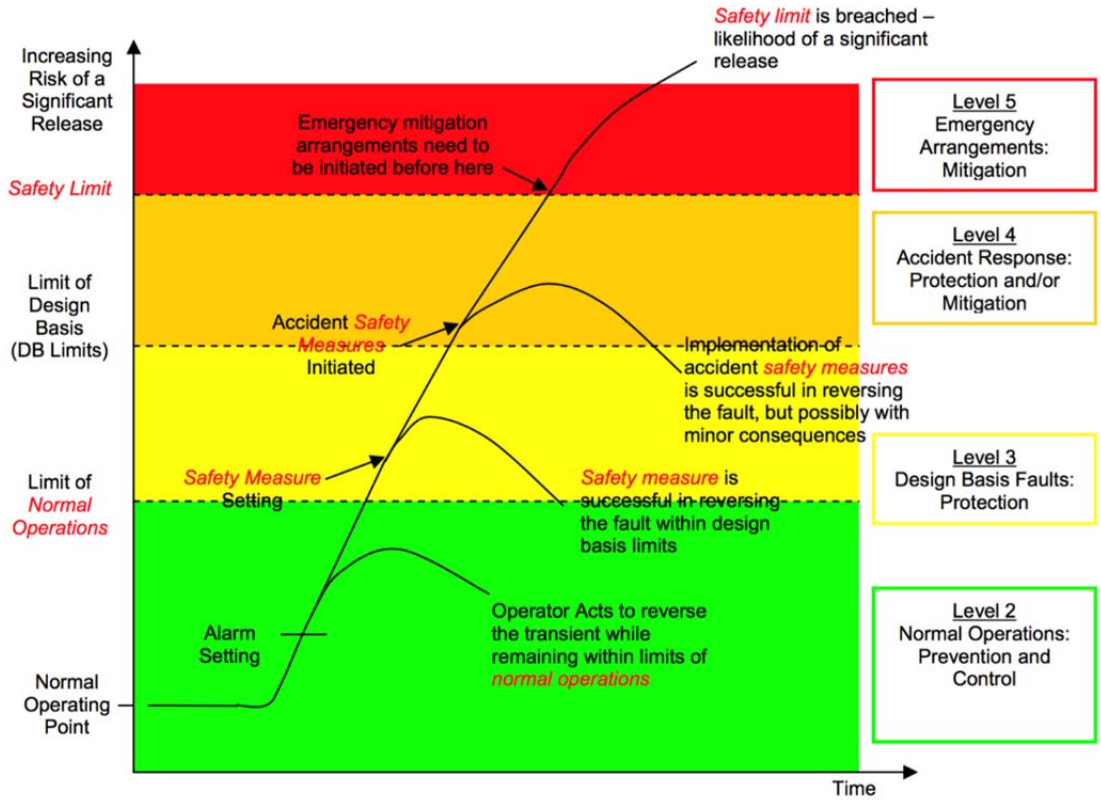


Figure 30.8-1 Definition of Operating Rules for LCOs at all Levels of Defence in Depth (from ONR TAG-035)

- The actions required for keeping the plant in, or returning it to, a safe state must align with the assumed characteristics (i.e. capabilities and limitations) of the operating organisation as defined in the Concept of Operations. The achievability of the actions within the applicable conditions (i.e. plant status, working environment, etc.) must be demonstrated in a manner proportionate to their contribution to risk.

- Any "operating rules" (i.e. either formal Technical Specifications, Operating Rules or their pre-cursors) must be written so they can be used by the operators who need to apply them (and not for example, for the fault analysts, design engineers or even the regulators). To achieve this they must be written with suitable consideration of HF principles that apply to writing instructions or procedures. Some key features required are:

    - They should be simple and based on parameters or information and controls readily available to the operator or maintenance technician,

    - Means of demonstration of compliance needs to be clearly specified and should be achieved through straightforward means (e.g. through direct reading of an indicator and avoiding, where possible, complicated off-line calculations), and

- The number and nature of the rules should be kept to manageable levels using grouping and bounding approaches where practicable.

There is also RGP for consideration of operational arrangements in fuel handling and radwaste handling operations (particularly within IAEA guides), as well as RGP for maintenance specification, planning, management and implementation that comes from INPO (e.g. AP-913 [Ref-11] and AP-928 [Ref-14]). As such, the specifics of the above RGP requirements may vary depending on which aspect of plant operations they are being applied to. However, the general nature of the requirements within the RGP is the same in every case:

- Clearly identify the limits and conditions of the plant and the required actions (operations, EMIT, etc.) for maintaining or returning the plant to a safe state,
- Consider the user capabilities and limitations when identifying actions for maintaining the LCOs, and demonstrate that the actions can be achieved, and
- Ensure the assumptions, Generic Technical Specifications and Operating Rules (or equivalent) are documented in a way that considers “usability” of the documents themselves.

30.8.3 Consideration of Options for Operational Aspects

Options for operational arrangements are not within scope of the GDA PCSR. However, design features and choice of design options in GDA must duly consider the future operating organisation and the impact the options can have on the ability to make ALARP claims in the Operations topic area. This section presents some of the key design options that were chosen to reduce risks in the Operations topic area.

- Improvements to the Allocation of Function (AoF) between human and system, such that automation decisions align with human capabilities as expressed in the UK COR.
- Examples include implementing automation for functions where human capability was challenged, such as Standby Liquid Control system initiation, Residual Heat Removal system (RHR) Suppression Pool cooling mode switching, Fuel Handling Machine operation (full automation option), as well as automation support (i.e. sequential automation) of manually-initiated functions such as certain RHR modes, etc.
- Improvements to the alarm presentation within the MCR, particularly the suppression of certain alarms in certain plant modes or states in order to ensure effective alarm processing by the operators, allowing human performance claims to be achievable.
- Improvements to the plant layout, plant equipment and various key HMIs such that they comply with UK and international modern standards for consideration of human

capabilities and limitations (i.e. physical dimensions for access and clearance, working environment, presentation of information for cognitive processes, etc.).

- HF specialist integration with all of the design teams for every topic area throughout the GDA to provide support to optioneering studies and ALARP work. HF expertise has been provided to multi-disciplinary workshops and to design reviews to ensure that, when considering individual design options and decisions related to ALARP justification, those design decisions have explicitly identified all assumptions about operational arrangements and have balanced HF constraints along with technical ones.

Further detail adequate consideration of HF and operational risks during optioneering and issues resolution is provided in the HF Design and Engineering Report (DER) [Ref-18] and its supporting documents.

30.8.4 Summary of ALARP Position and Justification

In addition to the specific aspects of the design that support the reduction of operational risks to ALARP, Hitachi-GE has met RGP throughout the design activities of GDA. The primary means for this has been through:

- The formal definition of the UK ABWR Concept of Operations, with input from the future licensee, as documented in the COR [Ref-2],
- The implementation of an integrated programme of HF support to the design and safety case, detailed within the HFIP [Ref-3],
- The distillation of relevant HF principles, standards and guidance into the HFE Spec [Ref-6]. The HFE Spec particularly enables widespread consideration of the capabilities and limitations of the operating organisation, ensuring that RGP regarding ORs being designed for the operator is able to be met in future. Further detail on the application of this specification to the UK ABWR design is provided in PCSR Chapter 27: Human Factors,
- The claims made on the operations or maintenance personnel, and the assumptions in design and safety analysis relevant to those claims, have been systematically identified and tracked through the HBSC identification programme plus appropriate procedure [Ref-19] and [Ref-4],
- Proportionate substantiation of those claims is reported in the HBSC Report [Ref-4] and underpinning supporting reports.,and
- All of the above, and any requirements for operational arrangements in future design and safety case stages, will be clearly communicated to the future licensee, for all topic areas, in accordance with “Technology Transfer to Licensee and Operating Regime” [Ref-20].

Through specific activities supporting design development options and by adopting the above good practice systematic processes for UK ABWR, the relevant risks within the Operations topic area have been reduced to ALARP during GDA. In addition, the above demonstrates that future operational arrangements are supported by the generic design and preliminary operational considerations, thus ensuring that the future arrangements can be implemented in such a way that they will also reduce site-specific operations risks to ALARP.

30.9 Conclusions

This chapter outlines the basic concept of operations for the UK ABWR. It provides the links to the operational configurations and limits that arise from the relevant systems chapters, and the means of control and management of the plant by operations personnel to maintain it within its design basis, as covered in PCSR Chapter 21: Human-Machine Interface and Chapter 27: Human Factors. The chapter provides the recommended operation and maintenance strategies, and provides assumptions for operation and maintenance that underpin the UK ABWR GDA assessment.

Although ALARP justification for Operations can only be substantiated by the future site licensee, this chapter presents the current ALARP position, outlining how the consideration of international good practice guidance and UK current practice in basic operating concept has ensured that the relevant risks within the Operations topic area have been reduced to ALARP during GDA. In addition, the chapter demonstrates that future operational arrangements will be supported by the generic design and preliminary operational considerations, ensuring that such future arrangements can be implemented in such a way that they also reduce site-specific operations risks to ALARP.

The future licensee must define their own operations and maintenance arrangements, so some of assumptions for GDA detailed in this chapter may be changed in the site specific stage. However, the future licensee is expected to take account of the basis, recommendations and assumptions detailed in this chapter and its supporting documents to develop the required site specific operational arrangements. This should then ensure that operational considerations at the GDA stage contribute towards ensuring the safe operation of UK ABWR.

30.10 References

[Ref-1] Hitachi-GE Nuclear Energy, Ltd., "Generic Technical Specifications", GA80-1502-0002-00001 (SE-GD-0378), Revision 3, August 2017

[Ref-2] Hitachi-GE Nuclear Energy, Ltd., "Human Factors Concept of Operations Report", GA91-9201-0001-00034 (HFE-GD-0060), Revision E, April 2017

[Ref-3] Hitachi-GE Nuclear Energy, Ltd., "UK ABWR GDA: Human Factors Integration Plan", GA32-1501-0007-00001 (HFE-GD-0058), Revision D, August 2017

[Ref-4] Hitachi-GE Nuclear Energy, Ltd., "UK ABWR GDA: Human-Based Safety Claims Report", GA91-9201-0001-00043 (HFE-GD-0064), Revision E, August 2017

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

[Ref-6] Hitachi-GE Nuclear Energy, Ltd., "UK ABWR GDA: Human Factors Engineering Specification", GA91-9201-0001 -00037 (HFD-GD-0001), Revision D, January 2017

[Ref-7] Institute of Nuclear Power Operators, "Human Performance Tools for Workers", INPO 06-002, April 2006

[Ref-8] Institute of Nuclear Power Operators, "Guideline for Excellence in Procedure and Work Instruction Use and Adherence", INPO 11-003, June 2011

[Ref-9] Hitachi-GE Nuclear Energy, Ltd., "Strategy of Use for HMIs", GA91-9201-0003-01462 (HFE-GD-0360), Revision B, August 2017

[Ref-10] Hitachi-GE Nuclear Energy, Ltd., "Topic Report on Approach to Operation of UK ABWR" , GA91-9201-0001-00266 (XE-GD-0735), Revision A, March 2017

[Ref-11] Institute of Nuclear Power Operators, "Equipment Reliability Process Description", INPO AP-913, September 2016

[Ref-12] Hitachi-GE Nuclear Energy, Ltd., "Maintenance Philosophy", GA91-9201-0003-01498 (XE-GD-0613), Revision B, July 2017

[Ref-13] Hitachi-GE Nuclear Energy, Ltd., "Maintenance Design Philosophy", GA91-9201-0003-01494 (XE-GD-0622), Revision A, January 2017

[Ref-14] Institute of Nuclear Power Operators, "Online Work Management Process Description", INPO AP-928, February 2016

[Ref-15] Hitachi-GE Nuclear Energy, Ltd., "GDA ALARP Methodology", GA10-0511-0004-00001 (XD-GD-0037), Revision 1, November 2015

[Ref-16] Hitachi-GE Nuclear Energy, Ltd., "GDA Safety Case Development Manual", GA10-0511-0006-00001 (XD-GD-0036), Revision 3, June 2017

[Ref-17] International Atomic Energy Agency, “Operational Limits and Conditions and Operating Procedures for Nuclear Power Plants”, IAEA Safety Standards Series No. NS-G-2.2, Vienna, December 2000

[Ref-18] Hitachi-GE Nuclear Energy, Ltd., “UK ABWR GDA: Human Factors Design and Engineering Report”, GA91-9201-0001-00039 (HFE-GD-0065), Revision C, August 2017

[Ref-19] Hitachi-GE Nuclear Energy, Ltd., “Standard Control Procedure for Identification and Registration of Assumptions, Limits and Conditions for Operation”, GA91-0512-0010-00001 (XD-GD-0042), Revision 2, March 2017

[Ref-20] Hitachi-GE Nuclear Energy, Ltd., “Technology Transfer to Licensee and Operating Regime”, GA70-1502-0001-00001 (QGG-GD-0001), Revision 0, August 2016

Appendix A: Document Map