GE Hitachi Nuclear Energy

NEDO-34190
Revision A
January 2025

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

BWRX-300 UK Generic Design Assessment (GDA) Chapter 18 – Human Factors Engineering

US Protective Marking: Non-Proprietary Information
UK Protective Marking: Not Protectively Marked

NEDO-34190 Revision A

INFORMATION NOTICE

This document does not contain proprietary information and carries the notations “US Protective Marking: Non-Proprietary Information” and “UK Protective Marking: Not Protectively Marked.”

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

The design, engineering, and other information contained in this document is furnished for the purpose of obtaining the applicable Nuclear Regulatory Authority review and determination of acceptability for use for the BWRX-300 design and licensing basis information contained herein. The only undertakings of GEH with respect to information in this document are contained in the contracts between GEH and its customers or participating utilities, and nothing contained in this document shall be construed as changing those contracts. The use of this information by anyone for any purpose other than that for which it is intended is not authorized; and with respect to any unauthorized use, no representation or warranty is provided, nor any assumption of liability is to be inferred as to the completeness, accuracy, or usefulness of the information contained in this document. Furnishing this document does not convey any license, express or implied, to use any patented invention or any proprietary information of GEH, its customers or other third parties disclosed herein or any right to publish the document without prior written permission of GEH, its customers or other third parties.

UK SENSITIVE NUCLEAR INFORMATION AND US EXPORT CONTROL INFORMATION

This document does not contain any UK Sensitive Nuclear Information (SNI) subject to protection from public disclosure as described in the Nuclear Industries Security Regulations (NISR) 2003, does not contain UK Export Controlled Information (ECI), and does not contain US Export Controlled Information (ECI) subject to the export control laws and regulations of the United States, including 10 CFR Part 810.

EXECUTIVE SUMMARY

The BWRX-300 Generic Design Assessment (GDA) Preliminary Safety Report (PSR) Chapter 18 describes the Human Factors Engineering (HFE) program for the BWRX-300 to demonstrate the adequacy of integration of HFE requirements and analysis results into the plant design.

The overall goal of the BWRX-300 HFE Program is to reduce the risks and consequences related to human interactions with the plant throughout all phases of the lifecycle. The program of HFE activities and analysis informing the design of the plant Structures, Systems, and Components (SSCs) is based on clear definition of the full plant set of users and a clearly defined scope of application across the full plant design, operational modes, and lifecycle stages, with focus on important human actions. The HFE content for this PSR chapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission.

Interfaces between Chapter 18 and other chapters are described in the Introduction. Claims and arguments relevant to GDA Step 2 objectives and scope are summarised in Appendix A, along with an As Low As Reasonably Practicable (ALARP) position. Appendix B provides a Forward Action Plan (FAP).

ACRONYMS AND ABBREVIATIONS

Acronym	Explanation
3D	Three-Dimensional
AC	Alternating Current
ALARP	As Low As Reasonably Practicable
AoF	Allocation of Function
BWR	Boiling Water Reactor
CAE	Claims, Arguments and Evidence
CB	Control Building
COO	Concept of Operations
COTS	Commercial-Off-The-Shelf
DCT	Data Connection Table
DRD	Design Requirements Document
DSA	Deterministic Safety Analysis
EME	Emergency Mitigating Equipment
ESF	Engineered Safety Feature
FAP	Forward Action Plan
FLEX	Diverse and Flexible Coping Strategies
FRA	Functional Requirements Analysis
GDA	Generic Design Assessment
GEH	GE Hitachi Nuclear Energy
GVDS	Group View Display System
HED	Human Engineering Discrepancy
HF	Human Factors
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HFEPP	Human Factors Engineering Program Plan
HMI	Human Machine Interface
HRA	Human Reliability Analysis
HSI	Human System Interface
HVAC	Heating, Ventilation, and Air Conditioning
IAEA	International Atomic Energy Agency
I&C	Instrumentation and Control
I/O	Input/Output
ICS	Isolation Condenser System
INPO	Institute of Nuclear Power Operations
ISO	International Organization for Standardization

Acronym	Explanation
ISV	Integrated Systems Validation
LCS	Local Control Station
LfE	Learning from Experience
MCR	Main Control Room
NRC	Nuclear Regulatory Commission
NUREG	Nuclear Regulatory Report
NSL	Nuclear Site License
OCC	Outage Control Centre
OER	Operating Experience Review
OPEX	Operating Experience
OSC	Operation Support Centre
PSA	Probabilistic Safety Analysis
PSAR	Preliminary Safety Analysis Report
PSR	Preliminary Safety Report
RAB	Reactor Auxiliary Bay
RGP	Relevant Good Practice
RWB	Radwaste Building
SAA	Severe Accident Analysis
SCDS	Safety Case Development Strategy
SCR	Secondary Control Room
SME	Subject Matter Expert
SMR	Small Modular Reactor
SPDS	Safety Parameter Display System
SSCs	Structures, Systems, and Components
TB	Turbine Building
T&E	Testing and Evaluation
TSC	Technical Support Centre
TSV	Task Support Verification
UIS	User Interface Specification
U.S.	United States
UK	United Kingdom
V&V	Verification and Validation
WANO	World Association of Nuclear Operators

DEFINITIONS

Term	Definition
Alarm	An audible and/or visible means of indicating to personnel an equipment malfunction, process deviation, or other abnormal condition requiring a timely response.
Automation	The application of technology to functions such as detection and analysis of fault conditions, situation assessment, diagnosis, and response planning. Automation is generally considered to change the manner of human interaction with system control, rather than fully supplant it (i.e. moving the operator into a supervisory capacity).
Design Basis Accident	A frequency category applied to PIEs or event sequences that are expected to occur at a frequency between 1E-02 and 1E-05 per reactor year.
Deterministic Safety Analysis	Safety analysis using, for key parameters, single numerical values (taken to have a probability of 1), leading to a single value for the result. Typically used with either best estimate or conservative values, based on expert judgement and knowledge of the phenomena being modelled.
Fundamental Safety Functions	Control of reactivity, fuel cooling, long-term heat removal, containment of radioactive materials (including shielding against radiation, control of operational discharges and hazardous substances, as well as limitation of accidental releases).
Human Engineering Discrepancy	A departure of the design from HFE design guidance and/or human performance criteria as identified during the execution of HFE Verification and Validation (V&V) activities.
Human Factors Engineering	The application of knowledge about human capabilities and limitations to plant, system, and equipment design. HFE ensures that the plant, system, or equipment design, tasks, and work environment are compatible with the sensory, perceptual, cognitive, and physical attributes of the personnel who operate, maintain, and support it.
Human Factors Issue	A problem or finding that is known to the industry or is identified throughout the life cycle of the HFE aspects of design, development, and evaluation. Issues are items that need to be addressed later and are tracked to ensure they are not overlooked.
Human Factors Engineering Process Requirements	Requirements for how the HFE Program is conducted and the interfaces between HFE and other disciplines.
Human Factors Engineering Verification and Validation	HFE V&V evaluates completed design features including alarms, controls, indications, and their associated hardware. During HFE V&V, design features are compared with regulatory requirements and guidance, HFE requirements, and the requirements generated during analysis of operator tasks and human-in-the-loop performance-based tests. HFE V&V consists of design verification, task support verification, and Integrated Systems Validation (ISV).
Human System Interfaces (HSIs)	The HSIs are the means through which personnel interact with the plant. This includes the alarms, displays, controls, and job performance aids. This includes interfaces for operations, maintenance, test, and inspection interfaces. The term HSI is synonymous with HMI.

Term	Definition
Important Human Actions	An important human action is a human-machine interaction that is credited in the BWRX-300 Deterministic Safety Analysis (DSA), Probabilistic Safety Analysis (PSA) or Severe Accident Analysis (SAA).
Normal Operation	Operation within specified operational limits and conditions. This includes startup, power operation, shutting down, shutdown, maintenance, testing and refuelling.
Operating Experience (OPEX)	Operating experience involves the identification, capture, sharing and use of lessons based on past experience.
Post-Accident Monitoring	A minimum set of monitoring parameters provided in the design to support accident assessment and mitigation.
Postulated Initiating Event	A change in state of plant equipment, caused by hazards such as equipment failures and internal/external events, that impacts the performance of a fundamental safety function and requires mitigation by defence line functions.
Probabilistic Safety Assessment	A comprehensive, structured approach to identifying failure sequences, constituting a conceptual and mathematical tool for deriving numerical estimates of risk.
Serious Injury	An injury that is life threatening and requires immediate attention (on-site or emergency response) to prevent loss of life or permanent disability.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

None.

NEDO-34190 Revision A

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
A	All	Initial Issuance

18. HUMAN FACTORS ENGINEERING

Introduction

The BWRX-300 GDA Preliminary Safety Report (PSR) Chapter 18 describes the Human Factors Engineering (HFE) program for the BWRX-300 to demonstrate the adequacy of integration of HFE requirements and analysis results into the plant design.

The program of HFE activities inform the design of the plant SSCs is based on clear definition of the full plant set of plant users and a clearly defined scope of application across the full plant design, operational modes, and lifecycle stages. The HFE program is graded (or proportionate), with particular emphasis on reducing the risks and consequences associated with important human interactions that are safety-critical or hazardous (see Subsection 18.2.5).

The content of this PSR chapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission and the scope of a GDA Step 2 PSR.

Chapter Structure

The Chapter covers the following elements:

- Management of the Human Factors Engineering Program – Section 18.1 describes the HFE program. This covers the HFE program goals, scope, team, organisation, processes, procedures and HFE issues and assumptions management.
- Human Factors Engineering Analysis – Section 18.2 describes the key cross-cutting HFE analysis activities. This includes Operating Experience (OPEX) Review, Functional Requirements Analysis (FRA), Allocation of Function (AoF), Task Analysis and Treatment of Important Human Actions.
- Design of the Human-Machine Interface – Section 18.3 describes Human Factors (HF) integration into the design of BWRX-300 Human-Machine Interfaces. This covers design goals and basis, inputs, detailed design, and integration and HFE Tests and Evaluation (T&E). Human Machine Interfaces (HMIs) covered include the Main Control Room (MCR), Secondary Control Room (SCR), Emergency Response Facilities, Local Control Stations (LCSs), equipment and line-mounted HMIs. This Section also describes HF integration into the design of the MCR, SCR, emergency response facilities and plant layout and the physical environment (for example lighting, temperature, and noise).
- Verification and Validation of Human Factors Engineering Analysis Results – Section 18.4 describes the staged program of activities to provide assurance of the correct and sufficient implementation of HFE requirements in the design, and the appropriate design to support required tasks.

The HFE content for this PSR chapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission. The following are out of scope for this version of the chapter:

- Staffing and Qualifications, other than the BWRX-300 MCR staffing concept (see Forward Action PSR18-174 in Appendix B which relates to including further information on staffing in future updates to the safety case).

- Development of procedures and training programs, other than how the outputs from the HFE program are used to inform training program development (see Forward Action PSR18-172 and PSR18-173 in Appendix B which relates to including further information on the procedure concept and procedure development processes in future updates to the safety case).
- Design Implementation – This technical element describes the implementation of the HFE design requirements in the final realised design.
- Human Performance Monitoring – This links HF methods used during the design with methods for monitoring the adequacy of the Human Machine Interfaces (HMIs) and other task support during the operational phase.

Interfaces with Other Chapters

Table 18-1 below identifies the PSR Ch. 18 PSR interfacing chapters. This includes main interfaces, which are the topics most closely connected with PSR Ch. 18 at the current stage of the design and safety case, and other interfaces.

Volume Interfaces

PSR Ch. 18 has interfaces with the following PSR Volumes:

- “Volume 1 - Preliminary Environmental Report” (Reference 18-17)
- “Volume 3 - Preliminary Security Report” (Reference 18-18)

18.1 Human Factors Program Management

18.1.1 Human Factors Engineering Program Goals

The overall goal of the BWRX-300 HFE Program is to reduce the risks and consequences related to human interactions with the plant throughout all phases of the lifecycle.

The HFE program is based on international standards, guidance, Relevant Good Practice (RGP) and multiple nuclear regulatory requirements, in particular:

- “International Atomic Energy Agency (IAEA) SSG-61, Format and Content of Safety Analysis Reports for Nuclear Power Plants” (Reference 18-19).
- “IAEA SSG-51, Human Factors Engineering in the Design of Nuclear Power Plants” (Reference 18-20).
- “Nuclear Regulatory Commission (NRC) NUREG-0711, Human Factors Engineering Program Review Model” (Reference 18-21).
- “Institute of Electrical and Electronics Engineers (IEEE) 1023-2004, Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities.” (Reference 18-22).
- “UK Office for Nuclear Regulation (ONR), Safety Assessment Principles for Nuclear Facilities” (Reference 18-23).
- “UK ONR NS-TAST-GD-058, Technical Assessment Guide: Human Factors Integration” (Reference 18-24).
- “Canadian Nuclear Safety Commission (CNSC) REGDOC-2.5.1, General Design Considerations: Human Factors (Reference 18-25) and CNSC REGDOC-2.5.2, Design of Reactor Facilities: Nuclear Power Plants” (Reference 18-26).

The 005N1716, “BWRX-300 Human Factors Engineering Program Plan (HFEPP)” (Reference 18-27) is the overarching HFE program document. It describes how the human centred HFE design goals are considered and verified during the design process. It ensures that the plant-level design goals, which include reducing the risks and consequences related to human interactions with the plant, are achieved, including:

1. Design of HMIs reduces the likelihood of error and provides for timely, clear error detection.
2. Tasks can be accomplished within time and performance criteria.
3. AoF and staffing arrangements ensure acceptable levels of workload and vigilance that minimise periods of human underload and overload.
4. Presentation of information supports a high degree of situational awareness of the plant state and required actions.
5. HMI design supports recovery from previous decisions and actions that did not achieve intended results.
6. Ergonomic principles are applied to working environments to ensure areas are safe and designed to support performance of required tasks.

The above HFE goals are embedded into the design through:

- Specification of requirements derived from codes, standards, and guidance.
- BWRX-300 specific HFE analyses.
- Integrated HFE team support to the design.

Achievement of the goals is confirmed using design tools, HFE T&E throughout the design development, and HFE V&V of the realised design.

18.1.2 Human Factors Engineering Program Scope

The HFE Program scope applies to HMI components and SSCs within, or that form part of facilities, systems, equipment, and components throughout the plant. HMIs are defined as any region or point at which a person interacts with a system, equipment, or component.

Machine interface means any digital and electronic Instrumentation and Control (I&C) user interfaces, hardware-based user interfaces, and design features on panels, equipment, and individual components.

The HFE Program applies to all HMIs, including those at the following locations:

- MCR
- SCR
- Emergency Response and Support Facilities
- Radwaste Building Control Room or Control Stations
- Local Control Station interfaces
- Equipment- and process line-mounted interfaces (e.g., control actuators and gauges)
- HMIs related to auxiliary and support facilities external to the main reactor and powerhouse buildings (e.g., hydrogen tanks or fuel oil supplies).

The scope of the HFE program includes specification to, and oversight of, HMIs that form part of SSCs supplied by external vendors, ensuring that supplied design or selection of standard equipment and components is consistent with the HFE requirements of the HFE Program.

The HFE Program applies across the full scope of users and activities that support plant operation, testing, inspection, and maintenance. This includes fuel handling, chemistry, radioactive waste processing, and radiation protection.

The HFE Program applies to design activities that consider Human Factors (HF) risks that might arise in all phases of the plant lifecycle, including:

- Construction
- Commissioning
- Operation
- Decommissioning

The HFE Program applies to all plant conditions in the design basis. This includes normal, outage (refuelling and maintenance outages, including extended refurbishments), abnormal, emergency, and accident conditions. The application of HFE support and activities to the scope of each phase and task location is graded (or proportionate), to apply a higher level of rigour for important human interactions that are safety-critical or hazardous (See Subsection 18.2.5).

For the Construction and Decommissioning phase of the system lifecycle, the HFE activities are performed at a higher level. The single iteration nature of these plant stages means they often do not involve analysis of ‘recurring’ operationally related tasks as done in commercial operations. HFE in design for these non-commercial operational phases is centred around providing basic guidelines and design strategies to support achievability of the overall goals of the phase. For example, the HFE principles and requirements for the BWRX-300 include aspects which support safe and reliable decommissioning, such as clearance and access for

removal of large equipment and components, and consideration of radiological safety through plant layout (see Subsection 18.3.7).

The same general HFE methodologies and tools described in this chapter are also applied to HF considerations related to security. A risk-based approach to HFE design requirements, task support requirements, and testing methodologies has been applied to security considerations. However, due to the sensitive nature of the specific details of security risk ratings, tasks important to nuclear security, security success criteria, and testing scenarios, the HFE activities for security are found within the document 006N6248, "BWRX-300 Security Assessment," (Reference 18-28). It is recognised that there can be conflicts between requirements, for example, between safety and security. Future work will involve checking that there are no conflicting requirements between human actions and security functional requirements (see Forward Action PSR18-164 in Appendix B).

Environmental Protection is also considered within the scope of the HFE program, for example through HF integration into SSCs and tasks associated with radioactive waste treatment. To ensure that Environmental Protection considerations are comprehensively covered, a Forward Action has been identified to check that the list of SSCs within the HFE program includes SSCs with a high classification environmental protection function. (see Appendix B, Forward Action PSR18-162).

Conventional safety considerations are addressed within the HFE program. For example, the risk-based grading system to grade each of the tasks or human actions identified throughout the plant includes a personnel safety category (see Subsection 18.1.5).

After plant turnover to the utility, the utility HFE Program is defined through suitable processes to address plant activities such as management of change for operational documentation, and design modification activities. Key assumptions from the HFE activities conducted during the design phase will be captured to feed into the definition of licensee arrangements (Subsection 18.1.5 and Forward Action PSR18-163 in Appendix B).

18.1.3 Overview of the Human Factors Engineering Program

The HFEPP (Reference 18-27) describes the goals and scope of the HFE Program. It also describes:

1. Assumptions and constraints in conducting the program.
2. Coordination of the HFE Program with the overall plant design activities, including coordination with the plant safety analysis.
3. Tools and facilities (e.g., mock-ups, computer simulations) used in support of the program.
4. Composition, qualifications, and responsibilities of the HFE organisation.
5. The technical methodologies used (for example, for AoF and task analysis).
5. Process and procedures followed including the process for identifying and managing technical and programmatic issues.
7. Documentation produced as part of the HFE program (for example, the 006N2829, "BWRX-300 Human Factors Engineering Design Requirements Document (DRD)," (Reference 18-29).
8. Summary of how the results of the HFE analysis are incorporated into the design, operational documentation, and safety analyses.

The HFEPP defines each of the technical elements, the specific activities that comprise the full integrated program, as outlined below. The HFEPP also includes technical elements that are currently out of scope for this version of PSR Ch. 18 (staffing and qualifications, training,

procedures, design implementation and human performance monitoring). These technical elements are therefore not included in the description below.

The full description of these elements, and how they constitute a comprehensive and robust program of HFE integration across the plant design and safety analyses, forms the remainder of this chapter (Sections 18.1 through 18.4). *Operating Experience Review (OER)* – identification, review and incorporation of any recommendations and learning (positive and negative) from past events and user feedback related to HFE in design (Subsection 18.2.1):

2. *FRA* – determination of functions required to achieve plant goals in all plant states (Subsection 18.2.2).
3. *AoF* – assigning the identified functions to system (technology) or human, based on respective capabilities and limitations of each (Subsection 18.2.3).
4. *Task Analysis* – identification of the tasks required to achieve the allocated functions, and decomposition into task steps to allow the identification and characterization of HMIs, personnel, locations, and support equipment (e.g., communications, lighting, personnel protection) required to perform each task successfully (Subsection 18.2.4).
5. *Treatment of Important Human Actions* – activities supporting and providing input to the BWRX-300 safety analyses to ensure clear identification of human actions important to nuclear safety, ensure claimed actions are achievable and identify HMIs requiring the highest level of HFE focus and effort (Subsection 18.2.5).
6. *Human-Machine Interface (HMI) Design* – identification and management of the set of HFE design requirements from standards, codes, and guidance, and implementation of those requirements as well as the results from HFE analyses into the design of HMIs, including integration of HFE team design support. This technical element also includes HFE T&E activities and Human Factors Integration (HFI) into control room, plant layout and the physical working environment (e.g. noise, temperature, lighting) (Subsections 18.3.1 to 18.3.7).

   Human Factors V&V – detailed, staged set of activities to provide assurance of the correct and sufficient implementation of HFE requirements in the design, and the appropriate design to support required tasks (Section 18.4).

The scope of the HFE Program and the HFE organisation undertaking the program align with regulatory requirements and international standards and guidance (See Subsection 18.1.1).

18.1.4 Team and Organization

HFE is positioned within the BWRX-300 team organisational structure such that it has the same level of authority and influence as the other engineering design teams.

The GEH HFE team consists of a core and extended team. The core HFE team is comprised of a Technical Lead role and two specialist HFE roles: Human Factors Engineer and HFE Operations / Maintenance. The extended team includes members from other disciplines within the engineering design team.

The overall responsibility of the GEH HFE team is to establish and perform the activities defined in the HFEPP. This includes guidance and oversight of the design activity to ensure the execution of each step in the activity is carried out in accordance with the established HFE program and procedures. Specifically, the HFE team is responsible for:

1. Developing HFE plans and procedures, including treatment of any identified OPEX and unresolved previous plant HFE issues.
2. Providing oversight, participate in, and review design and safety analyses development.

3. Design and layout of the hardwired and software HMIs in the BWRX-300 control rooms and throughout the plant, and control room layout.
4. Identifying recommendations for, and support to, implementation of resolutions for issues identified in the HFE requirements and analysis results.
5. Verification of correct and thorough implementation of HFE requirements, analysis results and issue resolution into the design.
6. Providing assurance that HFE activities comply with GEH management system processes and HFE project plans and methods.
7. Managing informal and formal documentation of HFE activities and issues management.
8. Planning and implementing HMI design configuration control during design implementation.

The GEH HF team consists of the following main roles. Qualifications for each role are described in the HFEPP (Reference 18-27):

1. HFE Technical Leads: Provides technical and program oversight and review; responsible for ensuring that HFE activities, interfaces, and outputs meet HFE requirements and align with HFE Program objectives. The Technical Leads are the point-of-contact for schedule development, integration, and management of the program.
2. HF Engineers: Provide specialised knowledge of human cognitive and physical capabilities and limitations, applicable HFE design and evaluation practices, and HFE principles, guidelines, and standards; develop and perform HFE analyses. The HF Engineer also identifies and participates in the resolution of identified HFE issues and non-compliances.
3. HFE Operations/Maintenance Specialists: Provide knowledge of operations and maintenance activities, including task characteristics, HMI characteristics, environmental characteristics, and technical requirements related to operational activities, and apply those insights in support of activities such as development of HMIs, procedures, and training programs. The HFE Operations/Maintenance role also participates in the development of scenarios for Human Reliability Analysis (HRA) evaluations, task analyses, HMI T&E, validation, and other evaluations.

Supplier HFE Specialists with United Kingdom (UK) context expertise are utilized to support licensing activities. Where suppliers are engaged to perform activities in support of the HFE program, GEH as the HFE Design Authority oversees the work.

Cross-Discipline Support and Integration

The integration of related groups with HFE is formally addressed through an integrated, detailed schedule, as well as through the HFE technical project management role of the HFE Technical Lead. HFE Awareness training is given to BWRX-300 Engineering personnel. This consists of an overview of HFE and how it relates to the different areas of design.

Discipline specific HFE Liaisons act as the champion of HFE requirements for their discipline. This includes working with the HFE team to resolve HFE issues and Human Engineering Discrepancies (HEDs) (see Subsection 18.1.5), reviewing and accepting HFE design requirements and ensuring that the requirements are incorporated into the design. They also perform cross-disciplinary review of HFE documents and participate in design reviews as the HFE representative as needed and appropriate to the HFE Application Level (see Subsection 18.1.5).

HFE fundamentals training provides the HFE Liaisons in the various engineering and safety analysis disciplines (e.g. Instrumentation and Control Engineering, Mechanical Engineering, PSA and HRA) with a more in-depth understanding of the HFE technical elements, processes, and work products. Further details are provided in the HFEPP (Reference 18-27).

18.1.5 Processes and Procedures

Coordination and Documentation of Activities

The HFE Program is planned and conducted in accordance with overarching design and quality program processes and procedures, within accredited quality management systems described in NEDC-34189P, “BWRX-300 PSR Ch. 17: Management for Safety and Quality Assurance,” (Reference 18-11).” To help ensure cross-discipline communication and coordination, periodic formal design reviews are held by representatives of each discipline.

Deliverables are also completed in accordance with a deliverable standard. This standard specifies the required content from all related disciplines, dictates the format for consistency and quality and specifies the reviewers for each document.

The documentation for the HFE Program uses a standard design process that includes documenting internal design records to capture inputs and outputs and providing the basis for formal deliverables. The information in the design records is incorporated into the design by HFE and other disciplines in accordance with the BWRX-300 project work breakdown structure. A Key Systems Decision process is implemented for the BWRX-300 plant design and is described in the 006N3139, “BWRX-300 Design Plan,” (Reference 18-30). This process is used throughout the design process to support decisions critical to the success of the BWRX-300 design and its implementation. Example applications include the definition of design concepts, requirements, and operating principles. The process considers and evaluates alternative courses of action (options) with participation from relevant stakeholders including HFE where appropriate.

HFE requirements and recommendations are addressed by the requirements management process (see ‘Requirements Management’ below), and either incorporated into the design directly or via alternate solutions agreed as acceptable by HFE, or if not implemented, tracked as an HFE issue (see ‘HF Issues and Assumptions Management’ below).

Risk-Based Graded Approach

A graded (or proportionate) approach to HFE is applied to the conduct of activities within the HFE Program, to provide the appropriate focus for analysis and design. The graded approach provides basic HFE attention to human interactions within the system and provides emphasis and more detailed, rigorous HFE effort on aspects of the plant design related to HMIs used to perform human actions important to safety, or tasks that are novel, complex, or hazardous (refer to Subsection 18.2.5 for further discussion of human actions important to safety). The approach uses a risk-based grading system to grade each of the tasks or human actions identified throughout the plant based on four key risk categories:

- Nuclear Safety
- Personnel Safety (covering conventional safety, radiological dose to personnel and other hazards that could affect personnel safety)
- Asset Protection
- Generation Capability

Although Asset Protection and Generation Capability are typically discounted as unrelated to safety, the HFE Program recognises that equipment damage creates requirements for forced outages and corrective maintenance, as well as impacting production goals, all of which has an indirect impact on personnel and nuclear safety. Consideration of aspects of equipment

protection, reliability, and production risks, also ensures that tasks outside of reactor operations have a decreased likelihood of being classified as Low-Risk Level. Loss of power generation and production shortfalls equate to loss of income for the plant which is recognised to have a direct effect on plant condition, organisational health, and ultimately, nuclear safety culture.

The overall risk level for the task is determined by the highest risk level assigned to each of the four categories. The base risk level is then used to assign a minimum HFE Application Level. The minimum HFE Application Level dictates the minimum degree of application for task analysis, HMI Design, procedure development, HFE V&V, and Design Implementation. However, it does not impact the level of OPEX, FRA, and AOF that are carried out (these are the same for all HFE Application levels). Further detail is provided in Subsection 18.1.3 and the HFEPP (Reference 18-27).

In addition to the formal task grading method for determining proportionate effort during design, the scope and level of effort of HFE activities is also proportionate to project lifecycle risk and change management considerations. This is done by applying greater scope, focus and degree of support on HFE activities that occur earlier within the design lifecycle, when changes are more effectively and easily managed. For example, while not all HMIs will receive a full HFE V&V, all HMIs will receive some degree of HFE support during the design phase.

Requirements Management

HFE requirements management is performed in accordance with a requirements management process that is standardised and controlled across the entire plant design, as described in PSR Ch. 17. Requirements management and traceability is developed and maintained to:

- Ensure HFE requirements relevant to each scope of work are clearly identified, allocated, communicated, and understood by all relevant project personnel.
- Outline how the requirements are met.
- Reference evidence that demonstrates compliance has been achieved.
- HFE requirements are categorised and dispositioned as follows:

    A. Process Requirements – Requirements related to how the HFE Program is conducted and the interfaces among HFE and other disciplines. HFE Process Requirements are allocated to the HFEPP and are fulfilled via the construction and implementation of the architecture and processes defined within this document. As such, all HFE Process Requirements are allocated to and end with the HFEPP.

    B. Product Requirements – Requirements for the design of, or provision for, plant workspace and environmental attributes, SSC, and HMIs. Product requirements are either derived from HFE design standards, codes, and guidance, or generated from HFE analyses as required to support successful task performance in the specific context of plant conditions. These requirements are implemented through design requirements specifications or design records communicated to and implemented by the relevant design teams. The HFE support level is proportionately applied based on the assessed risk-based grading (See ‘Risk-Graded Approach’ above).

Where HFE inputs are not in agreement with one another or where they conflict with other discipline design requirements, they are resolved using the process in the HFEPP to address conflicting requirements (Reference 18-27).

HF Issues and Assumptions Management

A HFE Issues Tracking System (HFEITS) is established to document and manage HF issues that may be identified throughout the full scope of HFE activities, including the actions taken to resolve those issues.

The HFEITS is used to capture HF issues related to design and implementation HFE activities and specific issues that will be identified through HFE V&V (HEDs). The tracking of issues includes:

1. Evaluation of each issue/HED to determine significance and whether it warrants correction when evaluated in the context of the integrated plant design.
2. Identification of appropriate solutions to address issues/HEDs, including, as appropriate, changes to HMI design, procedures, staffing/qualifications, or training.
3. Verification that the solutions implemented to address the issue/HED resolve the problem without generating additional issues/HEDs.
4. Documented traceability of the issue/HED resolution process and identification of residual risks associated with it, if necessary.

The HFEPP details the HFEITS development and management including:

1. Responsibilities for HFE team members in identifying HFE issues and HEDs.
2. The process and criteria for including HFE issues and HEDs within the HFEITS, as opposed to resolving non-compliant design through integrated design teamwork in normal workflow.
3. The process for evaluating the priority and adequate resolution of the issue/HED.
4. The means for confirming acceptable resolution of the issue/HED, based on the nature of the issue, its priority, and the plant lifecycle stage where the resolution occurs.

Generic assumptions on aspects such as staffing, training and qualifications and procedures have been captured in the 005N3747, “Human Factors Engineering Concept of Operation for BWRX-300,” (Reference 18-31). Specific assumptions, for example from task analysis are recorded in formal HFE program deliverables. See Forward Action PSR18-163 in Appendix B) on assumptions management (see Appendix B, Forward Action PSR18-163).

18.2 Human Factors Engineering Analysis

This Section describes the following technical elements:

- Operating Experience - Subsection 18.2.1
- Functional Requirements Analysis - Subsection 18.2.2
- Allocation of Function – Subsection 18.2.3
- Task Analysis - Subsection 18.2.4
- Treatment of Important Human Actions (i.e. from the Probabilistic and Deterministic Safety Analysis) – Subsection 18.2.5

Further detail on the identification and substantiation of human actions to maintain the plant within or bring it back to a safe state is provided in PSR Ch. 15.4.

18.2.1 Operating Experience

The BWRX-300 is an evolutionary design. The HFE program includes systematic processes to identify, review, use and apply OPEX to ensure that HF issues (lessons learned and good practice) are incorporated into the design and safety analyses.

An early OPEX Review (OER): 006N0813, “BWRX-300 Operating Experience Review Process and Results,” (Reference 18-32) has been carried out to inform the basic design with regards to alarms, display of plant information and controls, control and automation, information processing and job aids, real-time communications with plant personnel and other organisations, procedures, training, staffing, and job design.

The early OER process included:

- Identifying applicable OPEX sources, including OPEX reviews and databases for predecessor plant designs. Other sources of information include the Institute of Nuclear Power Operations (INPO) and World Association of Nuclear Operators (WANO) database searches, nuclear industry literature review, GEH lessons learned, HMI technology benchmarking reports and Fukushima lessons learned.
- Establishing a systematic framework and performing systematic searches of OPEX sources.
- Obtaining and incorporating personnel feedback from predecessor or similar types of reactors.
- Conducting reviews of human actions from predecessor designs that are similar to human actions included in the plant safety analyses (e.g. the PSA or DSA).
- Analysing and consolidating raw OPEX data into OPEX Item Summaries on the OER Capture Sheet.
- Allocating each OPEX item to the HFE activity or document in which the item is dispositioned.
- Recipient OPEX item review and allocation acceptance.

The Human Factors team identify, share, and utilise OPEX information in design development activities as an integral part of the HFE program. This includes informing the design and analysis of human actions credited within the DSA or PSA.

In addition to the early HFE OER, the project has a formal OPEX identification and management process, which is described in the 007N1411, “BWRX-300 Operating Experience Report,” (Reference 18-33). This process includes HFE team participation in both

identifying any OPEX and implementing HFE-allocated OPEX items in the HFE Program and the design.

Significant industry events such as Fukushima Daiichi have been reviewed and lessons learned incorporated into the design and organisational arrangements. For example, the BWRX-300 systems that support fundamental safety functions and plant monitoring have been designed to operate for a coping period of seven days, without Alternating Current (AC) power. The Isolation Condenser System (ICS) pools and spent fuel pool have enough inventory to provide adequate decay heat removal and fuel cooling for seven days, after which alternate water makeup sources (for example Diverse and Flexible Coping Strategies (FLEX) / Emergency Mitigating Equipment (EME)) are used to refill the pools.

HFE-related items identified through the early OER and ongoing OPEX process are allocated to a document, process, or activity to disposition. OPEX relating to design considerations or improvements is included in the "BWRX-300 HFE Design Requirement Document" (Reference 18-29) and dispositioned through implementation of the design requirements contained therein. HFE OPEX related to function allocation and task analysis is allocated to the "BWRX-300 HFE Concept of Operations" (Reference 18-31). This OPEX feeds into the HFE Analysis workbooks, where it is dispositioned through job design, HMI design, procedures, or training.

Implementation of the OPEX results into the design is managed and tracked through the assignment of and reference to a unique OPEX identification number.

Examples of how OPEX has informed design requirements include:

- OPEX from INPO 06-001, "Operating Experience to apply to Advanced Light Water Reactor Designs," (Reference 18-34): Interfaces required for emergency procedure execution should be part of permanent plant equipment (versus requiring jumpers, wire lifts, etc.).
    - HFE DRD Requirement: For areas where personnel are performing frequent or safety significant operations, maintenance, inspection, and test activities, permanent means of access to equipment requiring recurrent or emergency operation shall be provided when it is beyond the normal standing reach for workers. (Item OE_0113 from the HFE DRD (Reference 18-29)).
- OPEX from IAEA NP-T-3.8, "Maintenance Optimization Programme for Nuclear Power Plants," (Reference 18-35): On-line monitoring and wireless equipment monitoring allows operator rounds to be reduced, along with the associated radiation exposure.
    - HFE Concept of Operations (COO) requirement: The design will include provisions for on-line video and wireless equipment monitoring to allow operator rounds and associated risk of radiation exposure to be reduced. (Item OE_0157 from the HFE COO (Reference 18-31)).

Communication and allocation of the OPEX results to the appropriate design team and design requirements document is managed by the HFE team. For example, OPEX is shared with design engineers if design features are identified to reduce human error.

A future revision of the safety case will describe how OPEX relating to maintenance, inspection and testing tasks is being used to inform the design of SSCs, and maintenance program development, including links with safety analysis (in terms of the identification and analysis of important human actions). This is identified as a Forward Action (See Appendix B Forward Action PSR18-165).

18.2.2 Functional Requirements Analysis

FRA is the process to identify the key functions needed to achieve the plant safety, environmental, operational, and commercial goals. Through the identification of these functions, principal design requirements are identified to achieve the goals in all operating conditions (normal and postulated accident conditions).

FRA is conducted as part of the overall engineering design process and the BWRX-300 requirements management process: 005N9036, “BWRX-300 Requirements Management Plan,” (Reference 18-36). This includes elicitation, analysis, documentation, allocation (to specific system(s)), tracing, and requirements verification and validation. The characteristics of each function are defined through requirements traceability, which indicates the upstream and downstream source and need for the function and its sub-functions, and the safety classification of those functions based on defence lines as described in the 006N5064, “BWRX-300 Safety Strategy,” (Reference 18-37). FRA is a multi-disciplinary activity jointly undertaken by all design teams, including the HFE team.

The result of the multi-disciplinary FRA activities is the definition of the full set of functions that support achievement of the plant goals, which can be traced to the principal design requirements of the BWRX-300.

Plant- and system-level requirements documents list the functional requirements associated with each system. The system functional performance requirements repository contains the full list of plant functions, with reference and traceability back to the source documents from which the requirements were elicited.

The requirements are managed through a requirements management process which is described in Subsection 18.1.5 and PSR Ch. 17.

18.2.3 Allocation of Function

AoF is the process of deciding whether a task or function will be carried out by a human, a system/technology, or a combination of the two.

AoF processes are applied to enhance plant safety and reliability by ensuring optimal allocation of key functions and tasks by taking advantage of human and system strengths and avoiding human and system limitations. As the AoF processes may eliminate human tasks, they are one of the ways in which a hierarchy of controls is applied to reduce the sensitivity of the plant to human error.

The AoF aims to provide personnel with groups of logical, coherent, and meaningful tasks within their capabilities, and ensures a design that maintains human vigilance and situation awareness for any functions allocated to the system. An important goal of the AoF is to provide acceptable workload levels per job role that minimise periods of human underload and overload to the extent possible. This is done through review of the initial allocation as a whole and using expert judgement to determine if the assigned functions per job role are suitable and sufficient.

AoF processes implemented by the HFE team are described in the HFEPP (Reference 18-27) and in 006N4192, “BWRX-300 Allocation of Function Methodology,” (Reference 18-38). The processes are based on recognised international methods and guidance, specifically on IAEA-TECDOC-668, “The Role of Automation and Humans in Nuclear Power Plants,” (Reference 18-39). This provides a framework to determine functions that must be automated, functions which are better automated, and functions which should be given to humans, due to criteria such as:

- Physical demands (forces, posture)
- Cognitive demands (multitasking, stress, situational awareness, and vigilance)

- Combination of physical and cognitive demands (accuracy, response time)
- Environmental conditions (temperature, radiation)

The AoF process also uses criteria from NUREG/CR-2623, “The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review,” (Reference 18-40) that limit or preclude human participation in a function or, conversely, that make human participation mandatory. These combined criteria form the top-level, overriding criteria in the AoF process.

As outlined in Subsection 18.2.2, a key input to the AoF is the outputs of the FRA which identifies the BWRX-300 functions and tasks that support system functional requirements and require human or machine system support to execute (i.e. non-passive). The safety analyses also provide input to the AoF, specifying when human actions are required to backup automatic actions.

The AoF process includes an initial allocation (human, machine, system, shared) by an expert panel using defined criteria. A systematic review of options is carried out considering human and system capabilities and limitations. Inputs to the process include the 005N3558, “BWRX-300 Fault Evaluation and Fault List,” (Reference 18-41), system development workbooks and Subject Matter Expert (SME) knowledge of tasks that are not explicitly stated such as system startup. The initial allocation represents preliminary results that are subject to change as the design progresses.

AoF evaluation then is performed iteratively during the design, evaluation, and testing process. For example, AoF is assessed as part of Task Analysis, Staffing Analysis, HMI Test and Evaluation, and ISV. The AoF evaluation is a structured examination of function and task groupings that is used to assess allocations in a collective manner within an integrated work environment, instead of on a single function basis as this is not representative of functional delivery (e.g. workload may not be revealed analysing function by functions). Functions and tasks allocated to humans are considered in combination in the context of defined scenarios. The scenarios are evaluated to determine acceptability based on expected concurrent task performance, workload (physical and cognitive), vigilance, and situation awareness.

Should any of these evaluations identify issues with performance, workload, or situation awareness, the contributing functions and tasks are re-examined using the AoF process until satisfactory results are concluded.

The outputs of the 006N5325, “Functional Requirements Analysis, Allocation of Function, and Task Grading Results Report for BWRX-300,” (Reference 18-42) enable the identification of functions of relevance to HFE (i.e. non-passive). They are used as an input to the assignment of HFE Application levels to tasks (as described in Subsection 18.1.5), task analysis and HMI design activities (Subsection 18.2.4 and Section 18.3 respectively).

A Forward Action has been identified to update the AoF methodology to include consideration of security and environmental protection functions (See Appendix B, Forward Action PSR18-166). A Forward Work action has also been identified regarding reviewing the allocation of local control functions and the design of the HMI for radioactive waste management (see Appendix B, Forward Action PSR18-176).

18.2.4 Task Analysis

Risk-proportionate task analysis is carried out to analyse tasks allocated to human or shared during the AoF process. The overall objective is to identify requirements to ensure that tasks, including any human actions claimed in the BWRX-300 safety analyses, are feasible and can be reliably performed.

Task Analysis is undertaken in accordance with the methodology summarised in the HFEPP (Reference 18-27) and detailed in the 006N7318, “BWRX-300 Human Factors Engineering Task Analysis and Human-System Interface Design Methodology Report,” (Reference 18-43).

Inputs to the task analysis include system and plant design information, the HFE COO (Reference 18-31), procedures (where available), OPEX (see Subsection 18.2.1) and human actions claimed in the BWRX-300 safety analyses (see Subsection 18.2.5).

The task analysis is performed at a system level to capture the tasks needed to achieve systems functions and at an integrated level in order to evaluate tasks that need to be carried out at a plant level that involves multiple systems (for example plant start up and shutdown).

As described in Subsection 18.1.5, a risk proportionate approach is used to grade tasks. This determines the level of task analysis to be undertaken. Tasks are graded as High, Medium, or Low risk using a risk matrix which considers the following factors: Nuclear Safety, Personnel Safety, Asset Protection and Generation Capability. The Risk Level is assigned by an expert panel chaired by the HFE Technical Lead. The risk level corresponds to a minimum HFE application level.

The HFE Specialist assesses the characteristics of the task (such as novelty, complexity, frequency, time sensitivity, cognitive demands) to determine if the HFE Application Level needs to be increased.

If Human Actions are credited in the DSA for mitigating events, these will be considered a High-Risk Level. Additionally, HAs that the PSA identifies as risk-important through risk thresholds are considered a High-Risk Level. The remainder of the HAs identified by PSA for modelling are considered a Medium-Risk Level. HAs not included in DSA or PSA are considered a Low-Risk Level for the Nuclear Safety category.

All tasks regardless of HFE Application Level are assessed using task analysis. However, the level of detail within the task analysis varies based on HFE Application Level. There are two levels of task analysis: Basic task analysis and Detailed task analysis. Human actions ranked low HFE Application Level undergo a Basic task analysis; human actions ranked medium and high HFE Application Level undergo a Detailed task analysis.

Basic task analysis (HFE Application Level 3) can be performed by a HFE Specialist or System Engineer. It includes identification of the necessary tasks that support functions from the AoF, as well as review of the HMIs, and other task support measures for overall acceptability to support expected task performance. If problems with task support are noted, an HFE issue or HED is created to track the problem to resolution (see Subsection 18.1.5).

The Detailed task analysis is carried out by a HFE Specialist with inputs from other specialists (e.g. System Engineers, Operations and Maintenance Specialists). In addition to the steps involved in the Basic task analysis, Detailed task analysis includes workload analysis and assessment of requirements for situational awareness. The highest HFE Application Level requires additional link analysis, timeline analysis and qualitative human error analysis to be performed to evaluate and inform the layout of HMIs to optimise task performance. The task analysis provides a basis for the human reliability assessment and provides a record of the qualitative analysis that supports the substantiation of human actions.

The BWRX-300 Task Analysis Methodology (Reference 18-43) defines templates for capturing the task analysis, which are combined with the AoF results to document the full set of analysis activities. The activities are iterative, and the method allows timely and effective update of the task analysis and distribution of the results.

The results from the additional link, timeline and preliminary workload analyses in the Detailed task analyses are used to further inform the HMI design requirements, confirm or identify issues with the AoF and will be used to confirm that important HAs in the safety studies are feasible and can be reliably performed (see Subsection 18.2.5), confirm the potential for design induced violations is controlled by considering the layout and design of equipment (see Section 18.3) and provide a baseline for HMI T&E activities.

The initial task grading and outputs are recorded in the FRA, AoF and Task Grading Results Report (Reference 18-42), which will be updated as the design and safety studies progress.

18.2.5 Treatment of Important Human Actions

Overview and Basis of Approach

The subset of these user interactions that relate to nuclear safety are termed “important human actions.” Important human actions are defined as human actions credited in the BWRX-300 DSA, PSA and SAA. Within the nuclear industry these human actions may also be referred to as, and are synonymous with, Human Based Safety Claims (HBSCs) (usually in relation to the DSA) or Human Failure Events (usually in relation to the PSA).

The graded approach models and provides risk proportionate substantiation of human actions in accordance with the following:

- Human actions, if credited in the DSA will be assigned a High-Risk Level.
- Where the PSA identifies human actions as being risk significant based on measures of risk importance, these will also be assigned a High-Risk Level.
- The remainder of the human actions modelled in the PSA will be assigned a Medium-Risk Level in the Nuclear Safety category.
- User interactions not included in the DSA or PSA will be assigned a Low-Risk Level for the Nuclear Safety category. The graded approach ensures that a minimum HFE application level is applied to all Low-Risk Level user interactions (Subsection 18.1.5).

Future work will thus involve identifying and consolidating the human actions following safety analysis developments (see Forward Action PSR18-178 in Appendix B). Future work will also involve checking that there are no conflicting requirements between human actions and security functional requirements (see Forward Action PSR18-164 in Appendix B). In addition to human actions, the HFE methodologies and tools described in this chapter will also be applied to the following significant user interactions:

- Administrative controls - Administrative controls are user interactions required to keep the facility within its safe operating envelope (i.e. the Operational Limits and Conditions derived from the safety case). These are defined in the operating rules for normal operation (also known as Technical Specifications) and are also used when returning a facility back to normal operations. Future work will involve identifying and defining Administrative Controls following updates to the safety case and safety analysis (see Forward Action PSR18-171 in Appendix B).
- Tasks important to nuclear security – see Subsection 18.1.2.
- Tasks relating to Environmental Protection – see Subsection 18.1.2 and PSR18-162 in Appendix B.

18.2.5.1 Human Actions in the Human Factors Engineering Program

As user interactions are a central focus of the HFE Program, the methodologies, tools, and activities described throughout this chapter directly address the human actions:

- The decisions regarding the allocation of functions provide the first step in applying a hierarchy of controls and eliminating potentially risk significant human actions that may not be feasible or performed reliably (refer to Subsection 18.2.3).
- The HFE COO (Reference 18-31) provides the overarching context for the human actions.

- Learning from OPEX relating to predecessor designs is taken into account. This informs the design of similar human actions identified for the BWRX-300 (refer to Subsection 18.2.1).
- The use of task analysis (including link analysis, timeline analysis and preliminary workload analysis) informs the development of the human actions. It also provides evidence to substantiate the human actions and associated human error probabilities (see Subsection 18.2.4).
- The iterative HFE design activities address performance influencing factors that could undermine reliable completion of the human actions. These design activities include the development of requirements, the application of codes and standards and testing and evaluation (refer to Subsection 18.3.2).
- At this stage in the system lifecycle, the subject of violations is addressed by considering the potential for design induced violations. Design induced violations arise where the design and layout of HMIs/equipment does not support the user and results in perceived inefficiencies when performing tasks. Violations may then occur when the users try to perform the tasks in a manner that they consider more efficient.
- Issues that are identified in relation to the design and substantiation of human actions are/will be managed via the HFEITS (refer to Subsection 18.1.5).
- Evidence supporting the substantiation of human actions will be provided by HFE verification and validation, culminating in ISV. This ensures that the design, particularly the aspects affecting human performance, accomplishes its intended goals for usability and reducing the risk of human error as low as reasonably achievable (Section 18.4).

Further discussion of the human actions, how they are identified, and associated human reliability assessment that will be undertaken in support of the DSA and PSA is provided in PSR Ch. 15.4.

18.3 Design of the Human-Machine Interface

Note: HMI is referred to as “HSI” in BWRX-300 HFE program documentation. HMI is used in the safety case chapters in accordance with IAEA SSG-61 (Reference 18-19). The terms HMI and HSI are interchangeable for the purposes of this Chapter.

This Section describes the process by which HMI designs are established and evaluated. The HMI design process for BWRX-300 is governed by HFE Task Analysis and HSI Design Methodology Report (Reference 18-43) that outlines the required design inputs, design procedure to be followed, design outputs, and the process for conducting HFE T&E during design development.

The HMI design process is fully integrated into the overall plant design process specified through standard engineering design process and procedure documents, as well as the relevant project-specific design process plans.

General design principles and processes are described in PSR Ch. 3. The HMI in the MCR, SCR and emergency response facilities is described in PSR Ch. 7.

The design process for the MCR, SCR and emergency response facilities is described in Subsections 18.3.5 and 18.3.6. Local Control Stations and HMIs are discussed in Subsection 18.3.7. The facilities for supporting emergency and accident response are described in PSR Ch. 7 and PSR Ch. 19.

This Section also describes the integration of HF requirements, standards and methods into the plant layout and the physical environment (for example, temperature, lighting, noise). The BWRX-300 plant layout is described in PSR Ch. 9B: Civil Structures.

18.3.1 Human-Machine Interface: Design Goals and Design Bases

The primary goal of the HMI design process is to facilitate safe, efficient, and reliable user task performance during plant normal operational states, abnormal events, and accident conditions (including severe accidents). This ensures that human actions, if credited in the DSA, PSA or SAA can be completed reliably and that error potential is reduced.

To achieve this goal, HMIs throughout the plant are and will be designed and implemented consistent with HFE principles, standards and guidelines, and user-centred design practices. The following specific design bases are adopted for the plant:

1. HMI design promotes efficient and reliable operation through application of automated operation capabilities. AoF maintains human vigilance and provides acceptable workload levels that minimise periods of human underload and overload.
2. Accepted HFE principles, methods and requirements are used for ensuring HFE is integrated into the design, in alignment with RGP, as outlined in the HFEPP (Reference 18-27).
3. HMI design uses only proven technology.
4. The workstation and HMI layouts reflect I&C separation restrictions (see PSR Ch. 7).
5. HMI design is highly reliable and provides functional redundancy such that sufficient displays and controls are available in the MCR and SCR and remote locations to conduct an orderly reactor shutdown and to cooldown the reactor to safe shutdown conditions, even during design basis equipment failures.

6. The principal functions of the Safety Parameter Display System (SPDS) (i.e., an overview display of important plant parameters during transients and accidents) are incorporated into the HMI design. The BWRX-300 SPDS functionality does not require a different safety classification and is an integral part of, and included with the SC3 displays (see PSR Ch. 7). There is no separate panel or system.
7. The design basis for accident and emergency control and monitoring facilities meets international standards.

The BWRX-300 design has a high level of automation. Key HFE design considerations are maintaining situation awareness, cognitive engagement and keeping the operator 'in the loop'. The BWRX-300 design includes features to maintain situation awareness, such as Group-view displays. The Group View Display System (GVDS) is a large-format, mixed array of software-based information. It can provide an overview or high-level summary of the plant status, direct operators to additional information, support team coordination and awareness of each other's activities, and support personnel communication and collaboration. In addition, the BWRX-300 design process addresses situation awareness through:

- Information needs analysis in the form of task-based HMI inventory, alarm identification and rationalisation process, and accident monitoring parameter inventory.
- Detailed HMI design considering aspects such as the HMI inventory, functional grouping including consolidation of safety related parameters, salience management, special labelling of important parameters, alarm prioritisation and suppression functionality, automation interaction design guidelines.
- Phased HFE verification and validation program, including confirmation that the design supports situation awareness.

The operator will be actively engaged with Plant Automation System actions and 'kept in the loop' through design features such as sequential step automation. For example, during power raise the operator is required to provide inputs and verifications during the automated sequences.

18.3.2 Human-Machine Interface: Design Inputs

Task performance criteria developed through the HFE Program analysis activities, in conjunction with the criteria described in PSR Ch. 3 and PSR Ch. 15, are used to develop HMI design specifications. These detailed task performance criteria, along with requirements specified in HFE codes and standards, encompass the set of design requirements necessary to ensure that the implemented plant SSC and HMIs meet accepted HFE principles.

The inputs to the HMI design include:

- Plant user characteristics (Subsection 18.3.2)
- Specific information relating to the performance of tasks (Subsection 18.3.2)
- Design requirements and guidance specific to the plant design (Subsection 18.3.2)

In addition to these documented input sources, the integrated set of HFE Program activities includes HF Engineer support to designers for instances where the correct application of the set requirements is not clear or where design conflicts exist, and suitable alternative design solutions are required (as described in Subsection 18.3.2). Finally, HMI design updates are/will be made based on results from HFE T&E and HFE V&V activities, as described in Subsection 18.3.4 and Section 18.4 respectively.

Human Factors Engineering Concept of Operations

The HFE COO (Reference 18-31) describes the ways in which users interact with the HMIs and with each other to monitor, control, and maintain the plant such that it functions in a safe, secure, and efficient manner. The HFE COO provides the initial set of assumptions regarding the future operational plant, from the user perspective.

The HFE COO defines the physical and cognitive characteristics of the standardised plant full user population. It provides user population anthropometrics for the full range of 5th percentile female to 95th percentile male users, for the worldwide population specified in ISO 7250:3, “Basic human Body Measurements for Technological Design Part 3: Worldwide and Regional Design Ranges for Use in Product Standards,” (Reference 18-44). Other user population characteristics are provided, including population stereotypes (i.e., expectations of interface functionality of the whole user population based on country or nuclear industry norms).

The HFE COO also describes:

- The concept design for the key HMIs throughout the plant (both digital and analogue). This includes the basic HMI technologies, content, equipment, layout, and environment used by plant personnel to monitor, maintain, and control the plant.
- The Alarm Philosophy, in terms of the alarm concept at a high level, and the basic goals for alarm management.

The information and assumptions in the HFE COO provide the basis for task analysis, support the development of HFE design requirements and other HFE program activities such as control facility design.

Task-Related Input

A primary input to HMI development is the user task information and control needs established during task analysis (see Subsection 18.2.4). Task analysis provides the following information that forms the HMI Task Support Inventory:

- Information determining the need to initiate a task
- Control needs to accomplish the task steps
- Information feedback to confirm that task step control actions have been accomplished.
- Information for determining that task steps are accomplishing their intended objectives (e.g. accuracy, time available).
- Information for determining when tasks may be terminated.
- System and component alarms
- Information on task performance requirements for group-use and aggregate HMIs.
- Information regarding where manual tasks need to be performed (remote or local).

Design Requirements and Guidance Input

The second main input to HMI design is the full set of HFE design requirements derived from international codes, standards, regulations, that are applicable to the defined user group characteristics and the types of HMIs used throughout the plant. These requirements are managed through the formal requirements management process for the plant design that allows traceability from source to implementation. The HFE Design Requirements Document (Reference 18-29) provides an extract from the BWRX-300 requirements management database, providing a single repository of these common requirements (and applicable to various SSCs).

For the design of HMIs, the requirements in the HFE DRD (Reference 18-29) do not provide the entire basis for developing display interfaces. For example, within “requirement compliant” screen designs, there are any number of acceptable ways to lay out and create screens or panels, for example, variations in colour, size, font, and placement. Further inputs are required that ensure consistent and intuitive HMI designs across the plant. The requirements for this part of the HMI design process are defined in the 007N2535, “BWRX-300 Human System Interface Style Specification,” (Reference 18-45).

For digital software-driven HMIs, the style conventions are further developed into an HSI Element Library, which contains HMI display templates and HMI elements (e.g., symbols, numerical displays, graphs) that the display designer uses to assemble the display content. The HSI Element Library contains both HMI elements for primary interfaces (those that represent direct interface to the system and plant HMI) as well as secondary interfaces (such as navigation, which do not directly relate to system equipment).

The HSI Style Specification (Reference 18-45) is also used to maintain consistency for hardware-based controls and indicators, where suitable components are selected and, along with HMI panel templates, their specifications are included in the HSI Element Library.

The 007N4670, “BWRX-300 Alarm Management Process Specification,” (Reference 18-46) describes the alarm philosophy, including the principles for alarm identification, prioritisation, filtering, and suppression.

Human Factors Engineering Support

The final input is provided by the HFE team members on an as-required basis. This input is specific to each design challenge or designer technical query and supplements the proactive HFI processes described in Subsection 18.3.2.

The integration of the HFE team with the other disciplines provides the mechanism for designers to request HF Engineer support for instances where is not clear, for the HMI design aspect they are implementing, how the pre-specified requirements are correctly or effectively applied. Designers also request support when they identify conflicting design criteria that limit or prevent implementing the HFE design requirements as specified. In such cases, HF Engineer advice is provided on the most suitable alternative design solutions.

Results from Testing, Evaluation, Verification and Validation

Throughout the design development, HFE T&E is performed (Subsection 18.3.4). Later in detailed design, early HFE V&V activities will start. The results from these HFE T&E and V&V activities may be the identification of an HFE issue with the design or an HED. Recommended resolutions requiring HMI design improvement form the inputs to further design development. HF input to I&C design optioneering and justification of the selected options, HFE T&E and HFE V&V activities are identified as Forward Actions in Appendix B (see PSR18-170, PSR18-179 and PSR18-180 respectively).

18.3.3 Human-Machine Interface: Detailed Design and Integration

In accordance with the HFEPP (Reference 18-27) and the HMI Design Methodology (Reference 18-43) HMI designs are created through the interaction between the HFE team and discipline engineers, as described below.

The objectives of the HMI design process are to:

1. Translate codes and standards, as well as functional and task requirements, into HMI characteristics, displays, software, and hardware that enhance safety and reduce the risk of human error to ALARP through design.

2. Support the principal objectives of the HMI design to provide the information, controls, and status displays necessary for tasks allocated to each user, for all the required plant functions during all plant conditions, and to provide the user with accurate, complete, and timely information regarding the functional status of plant equipment and systems.
3. Ensure design trade-offs are resolved during the HMI design activities through the systematic application of HFE principles and criteria, and with HF Engineer support.
4. Maximise the plant capacity factor in the HMI design by:
    a. Facilitating planned operations, maintenance, inspection, and testing.
    b. Minimising the occurrence of any undesired power reduction or plant trip caused by erroneous decision-making and actions.
    c. Enabling plant commissioning to take place effectively and allowing timely modifications and maintenance of the HMIs.

The scope of the HMI design process is to specify requirements for HMIs throughout the plant. As with all other HFE Program activities, the scope and methods used for HMI design are graded based on HFE Application Level (Subsection 18.1.2). The HFEPP details the level of effort and scope for HMI design per HFE Application Level.

The HMI design products are created through the interaction and coordination of the HFE team and discipline engineers. Degree and type of interaction is based on the HFE Application Level.

The HFE team provides design and task support requirements (Subsection 18.1.4).

Depending on the HFE Application Level and the nature of the HMI, the HFE team:

1. Provides design requirement-compliant templates for HMI displays, panel layouts, and HMI elements, housed within the HSI Element Library.
2. Works with the System Engineer to implement the HFE requirements in the requirements management database (as compiled in the HFE DRD (Reference 18-29) that apply to the discipline and system, allowing them to design or specify and select compliant SSC or HMIs and to develop compliant system and equipment layouts.
3. Depending on HFE Application Level, reviews, tests, and verifies all HMI design work to ensure acceptable requirements are implemented and compliance is documented or performs proportionate design work audits using the design and task support evaluation checklists to ensure acceptable requirements are implemented and compliance is documented.

As described in Subsection 18.2.5, HMIs associated with important human actions receive the highest HFE Application Level.

Detailed Design and Integration: Design of Software Based HMIs

The HMI design process for software-based HMI display designs, which are the responsibility of the HFE team, is to create each system User Interface Specification (UIS), which contains a Data Connection Table (DCT).

The DCT will list the Input/Output (I/O) points associated with an HMI element on a display or panel and provides a mapping of instrumented parameters and controlled components to individual HMIs as follows:

1. Assemble inputs and requirements following the UIS input gathering procedure.

2. Complete the system UIS and the DCT. The UIS provides detailed renderings of the HMI display and panel layouts, including the components and parameters to be included on the HMI displays and panels. A UIS is created for each system, and a UIS is also created for the plant-level displays as a part of control room system design.
3. Integrate the UIS and DCT for each system.

The complete UIS standard deliverable provides the data, templates, and formats necessary for the development of the software and I/O points to drive the user display interfaces. It consists of:

- HMI Task Support Inventory Table
- HMI Task Support Inventory – Key Parameters
- DCT
- HMI display screenshot

The HMI Task Support Inventory table document the specific controls, indications, displays, panels, and HMI elements designed to support the user tasks. Data in the table documents that the designer confirmed that the HMI characteristics are appropriate for the specific use application. The table looks at display and panel locations to confirm that information that needs comparison is located on the same display or panel and that information used in related task actions are located on the same display or panel or are available for concurrent display on adjacent video display units or panels.

The HMI display screenshot is a record of the actual HMI display, contained in a software file, delivered with the UIS to the I&C team for data connection with the logic modules.

The HMI design for displays performed by the HFE team also results in the HMI display software file.

The individual system and integrated plant-level UISs, hardware-based HMI designs and Commercial-Off-The-Shelf (COTS) HMIs (Subsection 18.3.3), and the plant-level HFE requirements (i.e., related to layout and working environment as described in Subsection 18.3.6), are also integrated into relevant control facility designs.

Other outputs from the HMI design process include the design documentation (system design specifications, system and component requirements documents, purchase specifications, and drawings and models), as appropriate to the discipline and HMI type being designed.

The use of software-based HMIs has implications for human actions that may be modelled in the PSA and the quantification of human error probabilities. This is due to the lack of human error quantification methods that are fully validated for modelling human-computer interaction. This point is discussed further in PSR Ch. 15.4.

Detailed Design and Integration: Design of Hardware-based HMIs

For hardware-based HMIs, direct physical SSC interfaces and HMIs, the responsible discipline engineer will include the applicable task-based and HFE DRD requirements as part of their system and component level design requirements. The applicable HFE requirements will be included in lower-level system and component requirements specifications, including procurement specifications, ensuring consistency of application throughout the plant design. This will be managed using the design requirements management tool, the standard content for system design specifications, and the integrated HFE design support activities and issues management process outlined in HFEPP.

Compliance with HFE requirements addressed through the Requirements Management process (see PSR Ch. 17). Where exception to a requirement is needed, HFE provide design

support to develop and document an HFE-approved justification for an HFE design requirement exception.

Detailed Design and Integration: Commercial Off The Shelf Equipment and Components

The HFE design requirements apply to the HMIs of Commercial Off The Shelf (COTS) equipment and components. Ability of COTS equipment and component HMIs to meet the HFE design requirements is one of the standard selection criteria. However, it is recognised that not all COTS items will require the same level of rigor; standard items that do not include HFE as part of their specification will require HFE evaluation for non-compliance with the HFE design requirements. COTS compliance to HFE design requirements is addressed proportionately as described below. When evaluating COTS products that do not comply with HFE design requirements, special considerations will be applied by the HFE team to determine and document acceptability of the discrepancy; these include:

1. Trade-off of benefits of using a proven, standard solution compared to the benefits of a custom solution that more closely meets the HFE design requirements.
2. Analysis of COTS vendor HFE design basis and documentation in relation to HFE codes, standards, and relevant good practice.
3. Evaluation of COTS HMI design applicability to the defined user population, conventions, and stereotypes.
4. Degree of design and task support integration and consistency between the COTS product and the rest of the HMIs.
5. Identification of usability or human performance concerns with the proposed application of the COTS product.

Detailed Design and Integration: Alarms

Alarm system design requirements are embedded in the DRD (Reference 18-29) and Style Specification (Reference 18-45). The specification will include rationalisation and prioritisation evaluation results, providing alarm filtering and presentation requirements as input to the alarm system design activities.

Detailed Design and Integration: Local Control Stations and HMIs

Providing indications and controls in the field supports the assessment of plant conditions, maintenance, inspection, and testing, refuelling and other tasks. LCS interfaces and HMIs (for example equipment and process line-mounted HMIs) are provided where appropriate to support task performance. LCS and other local to plant HMIs may also be required to support for any human actions that may be credited in the DSA, PSA or SAA. Examples of representative LCS and local to plant HMIs include oil processing skids, diesel generator controls, chemistry control systems, fire detection and suppression system panels and security controls.

LCS and local to plant HMIs will utilise technology appropriate for the task and location. The process for HFI into the design of LCS and HMIs is described in Subsection 18.3.2. HFE requirements are provided in the HFE DRD (Reference 18-29), and task specific requirements identified through task analysis.

18.3.4 Human-Machine Interface: Tests and Evaluation

T&E is an integral part of the HFE design process, with the results of evaluation T&E efforts leading to early and effective modification to requirements and design improvements.

The purpose of HFE T&E is to find and address issues early, rather than waiting for HFE V&V activities near the end of the project (Section 18.4). It is the means to test the feasibility of

concepts and early prototypes and to facilitate reaching design decisions. Another difference from HFE V&V is that design and HFE engineers involved during the design stages are not excluded from being test participants.

The scope of the HFE T&E includes:

- Defining the HMI prototypes and simulation testbeds.
- Defining the HFE T&E team and participants.
- Establishing HFE T&E methods.
- Performing HMI selection and prioritisation.
- Performing HMI evaluation and user-based testing.
- Collecting and analysing data.
- Documenting results and communicating them to the relevant stakeholders.

HFE T&E scope ranges in complexity from simple user questionnaire responses and comments to empirical, performance-based techniques to assess how the user responds to the design under increasingly realistic conditions. The level and complexity of HFE T&E is based on design phase, task complexity, integration of the design feature to be assessed, and design and project risk (new HMI, new systems, high HFE risk grading).

To maximise the effectiveness of HFE T&E, HMIs are selected based on prioritization criteria. Primarily selection and Prioritisation of the HMIs are based on the HFE Application Level (Subsection 18.1.5). Where HMIs support more than one task, which means they may have more than one associated HFE Application Level, the highest risk level is used.

Beyond this grading, additional HMI are selected for HFE T&E inclusion based on consideration of any HMI design assumptions that require T&E. Assumptions made during the design phase are identified and refined so that they are specific enough for testing. The design assumptions are weighted to determine test priority (similar to the grading of human actions based on risk). The T&E focuses on the assumptions that have the highest impact if incorrect and the shortest time to learning the HMI.

Some examples of candidate HMI design assumptions include the following:

- Colours and status coding (short time to learning; medium impact if false)
- Hardware HMI ergonomic check (short time to learning; high impact if false)
- Safety Classed HMIs (long time to learning; high impact if false)
- HMIs related to the highest risk-level graded tasks (long time to learning high impact if false)
- New system functionality (long time to learning; high impact if false)

The T&E program is comprised of multiple assessment methods, with the most dominant being performance-based testing. Performance-based testing consists of observing users, given a goal to achieve, interacting with a suitable representation of the HMI design. Post-test analysis focuses on any difficulties encountered by the user, both qualitatively and quantitatively obtained, depending on test stage and testbed fidelity. The results are used to highlight differences between the design team assumptions in developing the HMI and actual user behaviour when using it, indicating potential human error traps in the design.

Each performance-based test cycle begins with the development of a test plan that outlines the purpose, equipment needed, design features being tested, test and data collection methods, performance measures and acceptance criteria, as well as any testing material where appropriate.

Data collection methods are selected appropriate to the type of test or evaluation being conducted, as detailed in the 007N3481, "BWRX-300 Human Factors Engineering Baseline 1 Testing and Evaluation Report," (Reference 18-47). Methods include participant questionnaires and interviews, direct observation of user behaviours and simulator instructor console data.

In addition to performance-based user testing, the HFE T&E team conducts formal trade-off evaluations to determine the relative benefits of potential design alternatives. Trade-off evaluations are conducted by a multi-discipline group of relevant stakeholders including HFE, other discipline engineering experts, HMI designers, and samples of end users. The trade-off evaluation is conducted using a standard trade-off tool, ranking the design alternatives against weighted key HFE criteria. The output of the trade-off tool is used as the basis to make the HMI design alternative trade-off decision. If there are several closely ranking alternatives, further HFE review or analysis is undertaken to determine.

HFE issues from T&E are recorded and tracked using the HFEITS (Subsection 18.1.5). Those that are not resolved at the time include the necessary information to address them in future project stages (for example through HFE verification and validation – see Subsection 18.4). The results from any HFE T&E are documented in design records and on associated test forms designed to support the T&E process. When the T&E for each design stage is complete, a T&E summary report is prepared that summarises all T&E activities and their results.

18.3.5 Design of the Main Control Room

The MCR concept design is described in PSR Ch. 7. The 007N0538, "BWRX-300 Control Room and Related Facilities Requirements Specification," (Reference 18-48) describes the design philosophy, design requirements, and required design features of the MCR, SCR, Technical Support Centre (TSC), Operation Support Centre (OSC) and other control facilities such the Outage Control Centre (OCC).

The primary goal of HFE input to design of the MCR is to facilitate safe, efficient, and reliable user performance during all phases of normal plant operation, abnormal events, and accident conditions. The MCR and the other BWRX-300 control rooms are designed in accordance with international standards and relevant good practices for control room design, integrating results from HFE design requirements and analyses.

The HFE COO (Reference 18-31) describes the nominal MCR staffing concept which includes the following roles: an Operations Supervisor, a Control Room Operator and a Field Technician. This provides a basis for the early HFE analyses and control room design. The initial MCR staffing concept is based on Boiling Water Reactor (BWR) and other relevant OPEX. The MCR staffing concept is initial and will be developed through formal HFE staffing analysis.

The MCR concept design includes three dedicated workstations in the MCR main work area. These include one supervisory workstation, and two redundant control workstations. They serve as the primary work location for plant monitoring and operation responsibilities. Additionally, a Critical Action Panel (Safety Class 1/Safety Class 2) workstation and an emergency communications workstation is available in the MCR main work area to use, when necessary. The MCR main work area has direct access to the shift manager office and a dedicated washroom for MCR personnel.

The development of the MCR workspaces and design features is/will be accomplished through:

- Consideration of existing control room OPEX.
- HFE analyses including task analysis and staffing analysis.

- Review of trends in control room designs and existing control room data presentation methods, such as the use of plant overview panel displays to support situation awareness.
- Evaluation of modern HMI technologies, including alarm system design, particularly alarm reduction and presentation methods.
- Application of relevant requirements from the HFE Design Requirements Document (Reference 18-29).
- Design or specification and selection of individual HMIs.
- Specification of the integrated HFE design requirements for the MCR as a whole.
- Testing of a dynamic MCR prototype (full-scope simulator).

Detailed task performance criteria will be specified as part of the task analysis and qualitative human error analysis (Subsection 18.2.4). These criteria will be used to govern and direct all plant control room designs. These detailed task performance criteria, along with requirements specified in HFE standards and codes (See Appendix C), encompass the set of necessary and sufficient design requirements that maintain the implemented plant control room designs in compliance with accepted HFE principles. This includes ensuring that any HMIs required to provide manual backup control to safety systems are identified and provided in a location and using technology (e.g., hardware-based high-reliability controls and displays) that are available in the postulated task conditions.

The MCR design will be demonstrated, through broad scope control room dynamic simulation during HFE T&E and future V&V, to satisfy the HMI design goals and design bases. Validation of the implemented MCR design will include evaluation of the design features, the user job roles, staff complement, and procedures, performed as part of the HFE V&V process as defined by the test specification and performance measures specified for each validation activity (Section 18.4).

The results from MCR HMI design activities are the same as those for the overarching HMI design process as described in Subsection 18.3.3.

18.3.6 Design of the Secondary Control Room and Emergency Response Facilities

The SCR provides means to safely shut down the plant from outside the MCR in a location that is protected and not impacted by the same scenarios that makes evacuation of the MCR necessary. The SCR provides the HMIs for the plant systems needed for safe shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe shutdown condition. The SCR concept design is described in PSR Ch. 7. Habitability of the SCR and protection of the route between the MCR and SCR is described in PSR Ch. 6.

The BWRX-300 standard design includes emergency response facilities, including an OSC and TSC.

The methodology for design of the SCR HMIs is the same as that for the MCR (Subsection 18.3.6) and more generally for HMI design (Subsection 18.3.3). As with all HFE Program activities, a proportionate, graded approach is taken.

The results for the SCR HMI design will be captured in the same means as for the MCR design (Subsection 18.3.5).

18.3.7 Plant Layout and the Physical Environment

The HFE design inputs described in Subsection 18.3.2 include requirements relating to plant layout and the physical working environment (for example lighting, thermal environment, and noise levels).

The HFE COO (Reference 18-31) defines concepts for plant layout to facilitate the traffic flows, task needs, and communication needs of the plant staff. For example, all areas plant including walkways, stairways, equipment areas and rooms, and external equipment HMIs will accommodate the user group physical characteristics and task-related requirements. This includes component removal envelopes, laydown areas, space for temporary testing, maintenance, or material handling equipment. Wherever possible areas of the plant with higher levels of radiation that need to be accessed regularly on different levels, will have access means (stairways, elevators). This enables transit between levels without having to exit the higher radiation areas.

The HFE DRD (Reference 18-29) specifies requirements for aspects such as access and egress, walkways, and maintenance, inspection, and testing. It also includes requirements for plant layout and the physical environment. Requirements for the physical environment are included in the relevant control facility specifications.

The physical environment is one of the factors considered when determining the HFE application level (described in Subsection 18.1.5). The physical environment and access considerations are also assessed during the task analysis process described in Subsection 18.2.4.

As noted in Subsection 18.3.2, the BWRX-300 design accommodates 95% of the target population by designing interfaces to accommodate the 5th percentile female to 95th percentile male of the international population. Three-Dimensional (3D) manikin models of the 5th percentile female and 95th percentile male defined by the anthropometric measurements in the HFE COO (Reference 18-31) are used to support assessment of aspects such as accessibility of equipment and controls, including those used to perform human actions claimed in the safety analyses.

HFE assessments of access, reach, and visibility are performed as the design develops using the BWRX-300 3D-product models.

The HFE team participates in layout reviews, for example review of the Power Block layout, using two-dimensional drawings and 3D models. The purpose is to identify any HFE issues relating to the placement of specific rooms and equipment and the presence or absence of specific equipment and features. Examples of specific aspects considered include adequate spacing for the performance of tasks, layout of rooms and work areas, means of ingress and egress and physical working environment.

18.4 Human Factors Engineering Verification and Validation

HFE V&V is an important HFE design assurance activity applied to the realised design of the plant HMIs and the working environment where those HMIs are used.

The HFE V&V is the staged program of activities to provide assurance of the correct and sufficient implementation of HFE requirements in the design and the appropriate design to support required tasks. In addition, HFE V&V activities provide the evidence that supports the substantiation of human actions credited within the DSA and PSA (Subsection 18.2.5).

The HFE Verification will be conducted through two activities with the following objectives:

1. Task Support Verification (TSV) verifies that the HMIs, as defined and baselined in the HMI inventory and characterisation, include the necessary features (e.g., controls, information displays, and alarms) required to support tasks and that there are no unnecessary features.
2. HFE Design Verification verifies that the HMIs and plant SSC, are compliant with the applicable HFE design requirements contained in the HFE Design Requirements Document and design-to-analysis requirements input as a result of HFE analysis activities. Verification activities include identifying changes to the design that impact HMIs and other features due to competing design constraints, and checking for due consideration of OPEX items, user stakeholder input and HFE T&E results.

HFE Validation will be conducted through staged activities, as follows:

1. Early and Partial System Validation activities are performed in advance of the full-scope simulator and fully constructed plant and are generally performed only on partial systems. Although they require a sufficient maturity of the design, HFE participants from the V&V team, and end users with enough level of familiarity with the system, they do not require the full integrated system. The purpose of these validation activities is to identify and resolve HFE issues in advance of a fixed design.
2. ISV is the performance-based evaluation of the fully integrated system design. Simulations and virtual reality models are used to validate the ability of personnel, trained using the training and qualification program material, to use the integrated HMIs and finalised procedures in accordance with the task and scenario performance requirements. ISV is intended to evaluate those integrated aspects that were verified and validated singly through earlier, partial means.

HFE Validation ensures that the design, particularly the HFE-specified aspects, accomplishes its intended goals for usability and reducing the risk of human error to as low as reasonably achievable. Validation is an integrated, dynamic, performance-based test activity in which participants are subjected to a set of simulated scenarios that represent a realistic, challenging, and generalisable set of conditions to ensure that the integrated HMI supports safe operation of the plant.

The scope of the HFE V&V activities applies to user interactions with the plant when performing operations, maintenance, testing, and inspection activities. The HFE V&V activities will be applied to HMIs within scope of the HFE Program. As with the other HFE Program activities, the application of HFE V&V will be graded to focus on the HMIs, tasks, and plant conditions that involve important human actions, are complex or novel, or are inherently hazardous. The same risk-based approach described in Subsection 18.1.5 is applied to the HFE V&V activities to determine the appropriate scope, rigor, and level of detail for each activity.

The HFE V&V program meets the requirements and RGP specified in international standards, including IEC 61771, “Nuclear power plants – Main Control Room – Verification and validation of design,” (Reference 18-49), and IAEA SSG-51, “Human Factors Engineering in the Design

of Nuclear Power Plants" (Reference 18-20). The program adopts a risk-based graded and multi-staged approach to V&V. It will be conducted in accordance with a structured, systematic plan. The V&V plan specifies the overall process used for HFE V&V, and the scope, inputs, methods, and outputs to be used for each V&V activity.

In a new plant design, the number of scenarios and HMIs is too large to effectively perform HFE V&V to the same degree on all of them. A sampling process will be used to focus on the significant, novel, and complex HMIs and tasks, ensuring a full breadth of HFE V&V scope but removing any duplication, thus improving the efficacy of the HFE V&V activities.

The verification activities will target a selection of HMIs (e.g., displays, panel layouts, equipment-mounted controls, and indications) and the validation activities target a selection of scenarios. The goal of sampling is to maximise sample relevance and significance while ensuring that the sample is sufficiently broad and diverse, so that the HFE V&V results are generalisable to the overall population of HMIs and scenarios.

TSV compares the HMI elements (alarm, control, information and equivalent) identified during the detailed analysis of a task to the designed HMIs to ensure that all components needed to safely and efficiently complete the tasks present in the final design. The task support inventory and verification criteria are identified during task analysis (Subsection 18.2.4).

In HFE Design Verification, various aspects of HMI and plant SSC design are compared to the relevant design requirements specified during the design development (Subsection 18.3.2). Examples of aspects verified include:

- Static and dynamic HMI features, including HMI-specific and standardised features.
- Interface management features such as navigation and data retrieval.
- Workstations and workspace anthropometrics
- Global workspace features (e.g., layout, workplace environment, lighting, noise)
- Effects of degraded HMI and plant workplace conditions.

During HFE Design Verification, the HFE verifier documents each HMI, or plant SSC element being evaluated (including document and page numbers, screenshots, or photographs as applicable), which subset of HFE Design Requirements Document (Reference 18-29) requirements were applied, and whether the HMI or SSC element passed or failed each requirement.

Early Validations will be performed to identify and solve HFE issues in advance of a fixed design. They require a sufficient maturity of the design, HFE participants from the V&V team, and end users with enough level of familiarity with the system. However, they do not require the full integrated system, including trained users and final procedures, that the ISV requires. Early Validations progress HFE T&E activities and results (Subsection 18.3.4), using higher fidelity testbeds and more cohesive scenario-based sets of tasks. The general method for conducting the Early Validations is the same as that for ISV, without the requirements for a complete integrated system and complex high-fidelity testing environments.

ISV is the performance-based evaluation of the fully integrated system design. ISV evaluates those integrated aspects that were verified separately through earlier, partial means (i.e., through HFE T&E, TSV, Early Validation). The purpose of ISV is to ensure that the integrated design, including the finalised HMIs and procedures is fulfilling its intended function. It also contributes to the substantiation of claims on human action made in the safety analyses. ISV will be performed with trained operators using high-fidelity simulators, task trainers or virtual reality labs (i.e., for scenarios outside of control rooms and control stations).

Any issues or non-compliances identified during the HFE V&V activities will be identified as a HED. HEDs are processed using the HFEITS process as described in Subsection 18.1.5.

The completion of HFE T&E and HFE V&V activities are identified as Forward Actions in Appendix B (PSR18-179 and 180).

18.5 Design Implementation

The content of this PSR chapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission and the scope of a GDA Step 2 PSR. This technical element, which describes the implementation of the HFE design requirements in the final realised design is outside the scope of the GDA Step 2 safety case.

18.6 Human Performance Monitoring

This. The content of this PSR chapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission and the scope of a GDA Step 2 PSR. This technical element, which links HF methods used during the design with methods for monitoring the adequacy of the HMIs and other task support during the operational phase, is outside the scope of the GDA Step 2 PSR.

Table 18-1: Interfacing Chapters

PSR Chapter	Summary of Interface with Chapter 18
Main Interfaces	
"PSR Ch. 3 - Safety objectives and design rules for SSCs" (Reference 18-1)	Safety objectives and design rules for SSCs describes the BWRX-300 general design principles and processes. It summarises measures and assessments to ensure safety including HF. This chapter provides the radiological acceptance principles and criteria. PSR Ch. 18 describes how HF considerations are incorporated into the engineered and administrative safety measures for the BWRX-300.
"PSR Ch. 7 – Instrumentation and Control (I&C)" (Reference 18-2)	Instrumentation and Control (I&C) provides a high-level description of the MCR and SCR layout and use, including the basic tasks to be supported by the HMI. It also describes the instrumentation and control provided in the emergency response facilities. PSR Ch. 18 presents the process for HF integration into the design of the BWRX-300 HMIs, the design of the MCR, SCR and emergency response facilities, including the methods and standards that are applied.
"PSR Ch. 15 – Safety Analysis" (Reference 18-3)	Safety Analysis describes the approaches adopted to take human actions into account in the BWRX-300 deterministic and probabilistic safety analyses, including Human Reliability Analysis (HRA). PSR Ch. 18 describes HF involvement in the safety analyses, including participation in the safety analysis process and use of outputs as part of the HFE program.
Other PSR Chapter Interfaces	
"PSR Ch. 6 – Engineered Safety Features (ESFs)" (Reference 18-4)	ESFs describes the systems that provide habitability of the MCR and SCR. HF integration to the design of the SCR and human actions relating to the SCR are discussed in PSR Ch. 18.
"PSR Ch. 8 - Electrical Power" (Reference 18-5)	Electrical Power describes the design of the electrical systems. PSR Ch. 18 describes the process for Human Factors integration into the design of HMIs and tasks which include those associated with the electrical system.
"PSR Ch. 9A - Auxiliary Systems" (Reference 18-6)	Auxiliary Systems describes the design of the auxiliary systems such as the fuel storage and handling system, Heating, Ventilation, and Air Conditioning (HVAC),and fire protection systems, communications and lighting systems, including HF design considerations. The HFE program scope described in PSR Ch. 18 includes the integration of HF into the task design, equipment, and facilities for the auxiliary systems.

PSR Chapter	Summary of Interface with Chapter 18
"PSR Ch. 9B – Civil Structures" (Reference 18-7)	Civil Structures describes the general design requirements for the Radwaste Building (RWB), Control Building (CB), Turbine Building (TB), Reactor Auxiliary Bay (RAB), Pumphouse/Forebay structures and tunnels, and Fire Pump Enclosure. PSR Ch. 18 describes Human factors integration into the BWRX-300 plant layout including aspects such as accessibility for operations, maintenance, test and inspection, safe means of access and egress and physical environment.
"PSR Ch. 10 - Steam and Power Conversion systems" (Reference 18-8)	Steam and Power Conversion systems includes a description of how the HF requirements and standards described in PSR Ch. 18 are applied to the design.
"PSR Ch. 11 - Management of Radioactive Waste" (Reference 18-9)	Management of Radioactive Waste describes the design of radioactive waste management systems. The HF program scope described in PSR Ch. 18 includes the integration of HF into the task design, equipment, and facilities for radioactive waste management.
"PSR Ch. 13 – Conduct of Operations" (Reference 18-10)	Conduct of Operations describes the BWRX-300 organisational structure, staffing and procedures. PSR Ch. 18 describes the interfaces between the HFE program and operational aspects including the development of staffing arrangements, training, and procedures.
"PSR Ch. 17 – Management for Safety" (Reference 18-11)	Management for Safety describes how the overall management of safety-related activities is assured. It describes the aspects such as configuration control, design processes, issue resolution, performance improvement, and safety culture. The HFE program described in PSR Ch. 18 is planned and conducted in accordance with the design and quality program processes and procedures and accredited quality management systems as described in PSR Ch. 17.
"PSR Ch. 19 – Emergency Preparedness and Response" (Reference 18-12)	Emergency Preparedness and Response covers elements of the BWRX-300 design that will facilitate on-site and off-site emergency arrangements.
"PSR Ch. 21 – Decommissioning and End of Life Aspects" (Reference 18-13)	Decommissioning and End of Life Aspects describes the principles applied to support safe decommissioning, particularly the consideration of OPEX from other decommissioning projects. The HFE program described in PSR Ch. 18 includes the application of HF principles and requirements to support the achievability of the overall goals of the decommissioning phase.
"PSR Ch. 23 - Reactor Chemistry" (Reference 18-14)	Reactor Chemistry outlines the approach taken to manage and control the chemistry in relevant system groups of the BWRX-300. The scope of the HFE program described in PSR Ch. 18 includes tasks associated with reactor chemistry control.
"PSR Ch. 24 - Conventional Safety and Fire Safety" (Reference 18-15)	Conventional Safety and Fire Safety describes the design and arrangements for ensuring conventional and fire safety. The scope of the HF program described in PSR Ch. 18 includes conventional and fire safety considerations.

PSR Chapter	Summary of Interface with Chapter 18
"PSR Ch. 27 – ALARP evaluation" (Reference 18-16)	ALARP evaluation provides the ALARP demonstration for the BWRX-300. PSR Ch. 18 describes how HF contributes to ALARP in relation to the potential for human error.

18.7 References

18-1 NEDC-34165P, “BWRX-300 PSR Ch. 3: Safety Objectives and Design Rules for SSCs,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-2 NEDC-34169P, “BWRX-300 PSR Ch. 7: Instrumentation and Control,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-3 NEDC-34178P, “BWRX-300 PSR Ch. 15: Safety Analysis,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-4 “BWRX-300 PSR Ch. 6: Engineered Safety Features (ESFs),” GE-Hitachi Nuclear Energy, Americas, LLC.

18-5 “BWRX-300 PSR Ch. 8: Electrical Power,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-6 “BWRX-300 PSR Ch. 9A: Auxiliary Systems,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-7 “BWRX-300 PSR Ch. 9B: Civil Structures,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-8 “BWRX-300 PSR Ch. 10: Steam and Power Conversion Systems,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-9 “BWRX-300 PSR Ch. 11: Management of Radioactive Waste,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-10 “BWRX-300 PSR Ch. 13: Conduct of Operations,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-11 NEDC-34189P, “BWRX-300 PSR Ch. 17: Management for Safety and Quality Assurance,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-12 “BWRX-300 PSR Ch. 19: Emergency Preparedness and Response,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-13 “BWRX-300 PSR Ch. 21: Decommissioning and End of Life Aspects,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-14 “BWRX-300 PSR Ch. 23: Reactor Chemistry,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-15 “BWRX-300 PSR Ch. 24: Conventional Safety and Fire Safety Evaluation,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-16 “BWRX-300 PSR Ch. 27: ALARP Evaluation,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-17 “BWRX-300 PSR Volume 1: Preliminary Environmental Report,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-18 “BWRX-300 PSR Volume 3: Preliminary Security Report,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-19 SSG-61, “Format and Content of Safety Analysis reports for Nuclear Power Plants,” IAEA.

18-20 SSG-51, “Human Factors Engineering in the Design of Nuclear Power Plants,” IAEA.

18-21 NUREG-0711, “Human Factors Engineering Program Review Model,” Nuclear Regulatory Commission.

18-22 “1023-2004, Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment, and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities,” Institute of Electrical and Electronics Engineers (IEEE).

18-23 “Safety Assessment Principles for Nuclear Facilities,” UK Office for Nuclear Regulation (ONR).

18-24 NS-TAST-GD-058, “Technical Assessment Guide: Human Factors Integration,” UK ONR.

18-25 REGDOC-2.5.1, “General Design Considerations: Human Factors,” CNSC.

18-26 REGDOC-2.5.2, “Design of Reactor Facilities: Nuclear Power Plants,” CNSC.

18-27 005N1716, “Human Factors Engineering Program Plan,” Rev 2, GE-Hitachi Nuclear Energy, Americas, LLC.

18-28 006N6248, “BWRX-300 Security Assessment,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-29 006N2829, “BWRX-300 Human Factors Engineering Design Requirements Document,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-30 006N3139, “BWRX-300 Design Plan,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-31 005N3747, “Human Factors Engineering Concept of Operation for BWRX-300,” Rev 1, GE-Hitachi Nuclear Energy, Americas, LLC.

18-32 006N0813, “BWRX-300 Operating Experience Review Process and Results,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-33 007N1411, “BWRX-300 Operating Experience Report,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-34 INPO 06-001, “Operating Experience to apply to Advanced Light Water Reactor Designs,” March 2006 and Addendum, September 2007.

18-35 IAEA NP-T-3.8, “Maintenance Optimization Programme for Nuclear Power Plants,” International Atomic Energy Agency, 2018.

18-36 005N9036, “BWRX-300 Requirements Management Plan,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-37 006N5064, “BWRX-300 Safety Strategy,” GE-Hitachi Nuclear Energy, Americas, LLC, 2024.

18-38 006N4192, “BWRX-300 Allocation of Function Methodology,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-39 IAEA-TECDOC-668, “The Role of Automation and Humans in Nuclear Power Plants,” IAEA, 1992.

18-40 NUREG/CR-2623, “The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review,” U.S. Nuclear Regulatory Commission,” 1982.

18-41 005N3558, “BWRX-300 Fault Evaluation and Fault List,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-42 006N5325, “Functional Requirements Analysis, Allocation of Function, and Task Grading Results Report for BWRX-300,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-43 006N7318, “BWRX-300 Human Factors Engineering Task Analysis and Human-System Interface Design Methodology Report,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-44 ISO 7250:3, “Basic human Body Measurements for Technological Design Part 3: Worldwide and Regional Design Ranges for Use in Product Standards,” International Organisation for Standardization (ISO), 2015.

18-45 007N2535, “BWRX-300 Human System Interface Style Specification,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-46 007N4670, “BWRX-300 Alarm Management Process Specification,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-47 007N3481, “BWRX-300 Human Factors Engineering Baseline 1 Testing and Evaluation Report,” GE-Hitachi Nuclear, Americas, LLC, 2023.

18-48 007N0538, “BWRX-300 Control Room and Related Facilities Requirements Specification,” GE-Hitachi Nuclear Energy, Americas, LLC.

18-49 “IEC 61771 - Nuclear Power Plants - Main Control-Room - Verification and Validation of Design,” International Electrotechnical Commission.

18-50 NEDC-34140P, “BWRX-300 Generic Design Assessment (GDA) Safety Case Development Strategy,” GE-Hitachi Nuclear Energy, Americas, LLC.

APPENDIX A CLAIMS, ARGUMENTS AND EVIDENCE

A.1 Claims, Arguments and Evidence

The ONR SAPs 2014 (Reference 18-23) identify ONR's expectation that a safety case should clearly set out the trail from safety claims, through arguments to evidence. The Claims, Arguments and Evidence (CAE) approach can be explained as follows:

1. Claims (assertions) are statements that indicate why a facility is safe,
2. Arguments (reasoning) explain the approaches to satisfying the claims,
3. Evidence (facts) supports and forms the basis (justification) of the arguments.

The GDA CAE structure is defined within the NEDC-34140P, "BWRX-300 Generic Design Assessment (GDA) Safety Case Development Strategy," (Reference 18-50) and is a logical breakdown of an overall claim that:

"The BWRX-300 is capable of being constructed, operated and decommissioned in accordance with the standards of environmental, safety, security and safeguard protection required in the UK."

This overall claim is broken down into Level 1 claims relating to environment, safety, security, and safeguards, which are then broken down again into Level 2 area related sub-claims and then finally into Level 3 (chapter level) sub-claims.

The Level 3 sub-claim that this chapter demonstrates compliance against are identified within the Safety Case Development Strategy (SCDS) (Reference 18-50) is as follows:

2.3.5 Human Factors assessments have been integrated into the design, safety assessments and management arrangements, to meet the relevant safety requirements.

Human Factors also contributes to the demonstration of compliance for other chapter level sub-claims (see Table A-1 below).

This PSR chapter has derived a suite of arguments that summarise how the applicable Level 3 sub-claims are met (see Table A-1 below).

It is not the intention to generate a comprehensive suite of evidence to support the derived arguments, as this is beyond the scope of GDA Step 2. However, where evidence sources are available, examples are provided in the Section of the Chapter referenced in Table A-1.

A.2 Risk Reduction As Low As Reasonably Practicable

It is important to note that nuclear safety risks cannot be demonstrated to have been reduced ALARP within the scope of a 2-Step GDA. In relation to Human Factors, understanding the human contribution to risk and achieving an ALARP position requires information that is not available at GDA Step 2 such as the full suite of tasks to be performed (tasks claimed in the safety studies and other important human actions, for example relating to maintenance and refuelling), as well as details on conduct of operations. It is considered that the most that can be realistically achieved is to provide a reasoned justification that the BWRX-300 Small Modular Reactor (SMR) design aspects will effectively contribute to the development of a future ALARP statement. In this respect, this chapter contributes to the overall future ALARP case by demonstrating that the chapter-specific arguments derived may be supported by existing and future planned evidence for the arguments in Table A-1.

Probabilistic safety aspects of the ALARP argument are addressed within PSR Ch. 15.

Table A-1: Human Factors and Related Claims and Arguments

Chapter 18 Claim	Chapter 18 Argument	Sub-Sections and/or Reports that Evidence the Arguments
2.1 All functions have been derived and substantiated taking into account RGP and OPEX, and processes are in place to maintain these through-life.		
2.1.2 The design of the system has been substantiated to achieve the safety functions in all relevant operating modes.	Task analysis contributes to design substantiation by confirming that tasks are feasible and can be reliably performed.	18.2.4 Task Analysis
	T&E is an integral part of the HFE design process, with the results of evaluation T&E efforts leading to early and effective modification to requirements and design improvements.	18.3.4 Human-Machine Interface: Tests and Evaluation
	The HFE V&V program evaluates the plant design (in parts and as an integrated whole) against safety case requirements, HFE design principles and requirements, user task requirements, job design and staff complement, procedural accuracy and usability, and effectiveness of training. In addition, HFE V&V activities provide the evidence that supports the substantiation of human actions credited within the DSA and PSA.	18.4 Human Factors Verification and Validation
2.1.3 The system design has been undertaken in accordance with relevant design codes and	HMIs throughout the plant are designed and implemented consistent with HFE principles, standards and guidelines and user-centred design practices.	18.3.4 Human-Machine Interface: Tests and Evaluation

Chapter 18 Claim	Chapter 18 Argument	Sub-Sections and/or Reports that Evidence the Arguments
standards (RGP) and design safety principles and taking account of OPEX to support reducing risks ALARP.	The overall layout of the plant, MCR and other BWRX-300 control rooms are designed in accordance with international standards and relevant good practices for control room design, integrating results from HFE design requirements and analyses.	18.3.5, 18.3.6 and 18.3.7 Design of the MCR Design of the SCR and Emergency Response Facilities Plant Layout and the Physical Environment
	The HFE Concept of Operation (COO) defines the physical and cognitive characteristics of the standardised plant full user population. The BWRX-300 is designed to accommodate the full range of 5th percentile female to 95th percentile male users, for the worldwide population specified in ISO 7250:3.	18.3.2 Human-Machine Interface: Design Inputs
2.1.6 The BWRX-300 will be designed, and is intended to be operated, so that it can be decommissioned safely, using current available technologies, and with minimal impact on the environment and people.	The HFE principles and requirements for the BWRX-300 include aspects which support safe and reliable decommissioning, such as clearance and access for removal of large equipment and components, and consideration of radiological safety through plant layout.	18.1.2, 18.3.2, 18.3.7 HFE Program Scope Human-Machine Interface: Design Inputs Plant Layout and the Physical Environment

Chapter 18 Claim	Chapter 18 Argument	Sub-Sections and/or Reports that Evidence the Arguments
2.3 A suitable and sufficient safety analysis has been undertaken which presents a comprehensive fault and hazard analysis that specifies the requirements on the safety measures and informs emergency arrangements (Safety Analysis)		
2.3.5 Human Factors assessments have been appropriately integrated into the design, safety assessments and management arrangements, to meet the relevant safety requirements.	A graded (or proportionate) approach is applied to the conduct of activities within the HFE Program. This provides an appropriate level of analysis to substantiate important human actions.	18.1.4 Team and Organisation
	Allocation of Function processes based on international good practice are applied to enhance plant safety and reliability by ensuring optimal allocation of key functions and tasks by taking advantage of human and system strengths and avoiding human and system limitations. As the AoF processes may eliminate human tasks, they are one of the ways in which a hierarchy of controls is applied to reduce the sensitivity of the plant to human error.	18.2.3 Allocation of Function
	Risk-proportionate task analysis is carried out to analyse tasks allocated to human or shared during the Allocation of Function process. The overall objective is to identify design requirements to ensure that tasks, including any human actions claimed in the BWRX-300 safety analyses, are feasible and can be reliably performed.	18.2.4 Task Analysis

Chapter 18 Claim	Chapter 18 Argument	Sub-Sections and/or Reports that Evidence the Arguments
2.4 Safety risks have been reduced as low as reasonably practicable		
2.4.1 Relevant Good Practice (RGP) has been taken into account across all disciplines.	The HFE program and methodologies within it are based on international standards, guidance, relevant good practice, and multiple nuclear regulatory requirements.	18.1.1 HFE Program Goals
2.4.2 Operating Experience (OPEX) and Learning from Experience (LfE) has been taken into account across all disciplines.	The HFE program includes the identification, review, use and application of Operating Experience to ensure that HF issues (lessons learned and good practice) are incorporated into the design and safety analyses.	18.2.1 Operating Experience

Chapter 18 Claim	Chapter 18 Argument	Sub-Sections and/or Reports that Evidence the Arguments
2.4.3 Optioneering (all reasonably practicable measures have been implemented to reduce risk)	The process for allocation of the functions required to achieve the BWRX-300 safety goals includes a systematic review of options with respect to human and system capabilities and limitations (human, machine, shared).	18.2.3 Allocation of Function
	The HFE T&E team conducts formal trade-off evaluations to determine the relative benefits of potential design alternatives. Trade-off evaluations are conducted by a multi-discipline group of relevant stakeholders including HFE, other discipline engineering experts, HMI designers, and samples of end users. The trade-off evaluation is conducted using a standard trade-off tool, ranking the design alternatives against weighted key HFE criteria. The output of the trade-off tool is used as the basis to make the HMI design alternative trade-off decision.	18.3.4 Human-Machine Interface: Tests and Evaluation
	HFE considerations are integrated into BWRX-300 optioneering processes, such as the Key Systems Decision process is used for the BWRX-300 plant design (Reference 18-30 BWRX-300 Design Plan).	18.1.4 Team and Organisation

APPENDIX B FORWARD ACTION PLAN

The Forward Action Plan (Table B-1) identifies future Human Factors work into the design, safety analysis and the safety case.

Table B-1: Human Factors Engineering Forward Actions

Codes	Finding	Forward Actions	Delivery Phase
PSR18-162	The Environment Agency HF Principle ENDP5 states that 'Human actions should be taken into account in the design of a facility and in operating procedures.' Whilst radioactive waste management is identified as within the scope of the HFE program, the HF grading approach or criteria does not include tasks associated with SSCs that have an environmental protection function.	A list of SSCs with an environmental protection function will be developed by the Environmental Protection topic area/ it is expected that SSCs with an environmental protection function typically also have a nuclear safety function. Future work is needed to check that the list of SSCs within the HFE program includes SSCs with a high classification environmental protection function.	For PCSR/PCER
PSR18-163	The process for capturing, managing (e.g. feed into training program development) and validating assumptions made in the HF analyses is not described in DNNP PSR Ch. 18 or supporting documents. The process for capturing assumptions made in the HF analyses or HF program documents (e.g. relating to training, procedures, task timings, HMI design features). and for validating/ transferring these to a future licensee is not described in DNNP PSR Ch. 18 or supporting references. Assumptions generated through HFE analyses are captured in individual reports.	It should be confirmed that expectations for HF assumptions management can be addressed by project level MSQA processes.	For PCSR/PCER
PSR18-164	Section 4.1.5 of HFE Design Support and Evaluation Report, summarises HFI into security however the link with HBSCs is not explicitly discussed in the DNNP PSR Chapter or any HFI into security aspects.	During the licensing phase, safety HBSCs should be checked against security functional requirements to ensure there are no conflicting requirements for example, SA emergency scenarios may require a flexible response, utilising more personnel from offsite and bringing in	For PCSR/PCER

Codes	Finding	Forward Actions	Delivery Phase
		offsite equipment which may require different security measures.	
PSR18-166	The AoF methodology does not include reference to security and environmental protection functions.	Update the AoF methodology to include security and environmental functions.	For PCSR/PCER
PSR18-167	The HF task grading criteria for personnel safety is not clear -specifically, it is not clear what exceeding 40% legal limits means in practice.	GEH HF to discuss the task grading criteria related to legal limits and possibly remove it from the task grading criteria/method.	For PCSR/PCER
PSR18-169	No Target Audience Description exists; however, it is considered that the majority of the expected contents of a TAD are covered by the Concept of Operations and Design Requirements document (006N2829 BWRX Human Factors Engineering Design Requirements Document).	Future work should review the Concept of Operations against UK Context requirements/standards	For PCSR/PCER
PSR18-170	I&C system design is incomplete.	HF to provide input to design optioneering and justification of the selected options.	For PCSR/PCER
PSR18-171	Administrative controls required to keep the facility within its safe operating envelope (e.g., the Operational Limits and Conditions derived from the safety case) have not yet been defined.	Add more information on Administrative Controls and associated operating rules/technical specifications following updates to the safety case and safety analysis.	For PCSR/PCER
PSR18-172	The procedure concept (i.e. format, computerised, paper based) is not described in the DNNP PSR (however some information on procedures is discussed in PSR Ch. 13). See also related FWA below.	Include information on the procedure concept (format and types of procedures) in the next version of the Safety Case - PCSR	For PCSR/PCER
PSR18-173	Development of procedures and training programs (other than how outputs from the HFE program inform training development) is out of scope for GDA Step 2 but discussed in the DNNP Preliminary Safety Analysis Report (PSAR) and the Standard Product HFEPP.	Include information on the development of procedures and the training program	For PCSR/PCER
PSR18-	Staffing and Qualifications is out of scope for GDA Step 2 but discussed in	Future work and updates to the safety case should describe the process to	For PCSR/PCER

Codes	Finding	Forward Actions	Delivery Phase
174	the DNNP case.	defined and validate staffing requirements and qualifications	
PSR18-176	Control and monitoring of radioactive waste treatment systems will be carried out via local Control Stations rather than a Radioactive Waste Control Room or the MCR. This requires justification in terms of options considered and human reliability considerations.	Provide justification of the decision for the location and HMI requirements for radioactive waste treatment monitoring and control	For PCSR/PCER
PSR18-177	HFI into Safeguards is not discussed in the DNNP PSR Ch. 18 or supporting references. This is out of scope for Step 2 because only a high-level framework for safeguards will be presented during Step 2 and this is largely a Nuclear Site License (NSL) topic.	Define requirements for HFI into the Safeguards topic	During site-specific work
PSR18-179	The output and results of Testing and Evaluation studies are not currently described in the DNNP Safety Case.	Complete Test and Evaluation program and associated summary reports	For PCSR/PCER
PSR18-180	Verification and Validation studies have not yet been completed.	Complete the V&V studies	For PCSR/PCER
PSR18-181	No UK specific Human Factors Integration Plan exists.	The Plant & System Design Document states that a specific project HFEPP could be produced as part of baseline 3. A UK specific HFIP could be produced that includes further information on: • Construction and commissioning • HRA • Decommissioning • V&V technical element • HFI into design development	For PCSR/PCER