GE Hitachi Nuclear Energy

NEDO-33968
Revision 0
September 2022

Non-Proprietary Information

Ontario Power Generation Inc.
Darlington New Nuclear Project
BWRX-300 Preliminary Safety Analysis Report:

Chapter 18
Human Factors Engineering

IMPORTANT NOTICE REGARDING CONTENTS OF THIS REPORT

Please Read Carefully

REVISION SUMMARY

Revision #	Section Modified	Revision Summary
0	All	Initial Release

ACRONYM LIST

Acronym	Explanation
AOF	Allocation of Functions
CBP	Computer-Based Procedures
CNSC	Canadian Nuclear Safety Commission
COO	Concept of Operations
COTS	Commercial-Off-The-Shelf
DCT	Data Connection Table
DNNP	Darlington New Nuclear Project
DSA	Deterministic Safety Analysis
EOP	Emergency Operating Procedure
FRA	Functional Requirements Analysis
GEH	GE-Hitachi Nuclear Energy
HED	Human Engineering Discrepancy
HF	Human Factors
HFE	Human Factors Engineering
HFEITS	Human Factors Engineering Issue Tracking System
HFEPP	Human Factors Engineering Program Plan
HPM	Human Performance Monitoring
HRA	Human Reliability Analysis
HSI	Human-System Interface
I&C	Instrumentation and Control
ISV	Integrated System Validation
MCR	Main Control Room
NUREG	Nuclear Regulatory Report
OE	Operating Experience
OER	Operating Experience Review
PSA	Probabilistic Safety Assessment
PSAR	Preliminary Safety Analysis Report
SAA	Severe Accident Analysis
SCR	Secondary Control Room
SPDS	Safety Parameter Display System
SSC	Structures, Systems, and Components

Acronym	Explanation
T&E	Testing and Evaluation
TA	Task Analysis
TSV	Task Support Verification
UIS	User Interface Specification
V&V	Verification and Validation

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

18.0 HUMAN FACTORS ENGINEERING

Preliminary Safety Analysis Report (PSAR) Chapter 18 presents 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 and analysis informing the design of the plant Structures, Systems, and Components (SSC) 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 PSAR chapter reflects the level of maturity of the HFE Program, plant design, and safety analyses at the time of submission. The pre-operational safety analysis report details further design and analyses development and summarizes HFE Program progression in support of the Licence to Operate submission.

Chapter 18 provides a summary of the BWRX-300 Human-System Interface (HSI) design goals and bases, analyses undertaken to understand the plant-specific HFE requirements related to task performance, the process for detailed HSI design, and activities supporting effective design implementation. The overall design and implementation process is described in detail in NEDC-33982P, "BWRX-300 Darlington New Nuclear Project (DNNP) Human Factor Engineering Program Plan" (Reference 18.1-1). The Human Factors Engineering Program Plan (HFEPP) presents the comprehensive, iterative design approach used for the development of human-centred interfaces and work environment for the plant.

Note that Section 18.1 provides an overview of the HFE Program and outlines its activities or "technical elements". The remainder of the chapter provides the details, including the scope and summary of methods, of the technical elements outlined in Section 18.1.

18.1 Management of the Human Factors Engineering Program

18.1.1 HFE Program Goals

The high-level goal of the BWRX-300 HFE Program is to conduct a proportionate, integrated, and effective set of HFE design activities that considers users and all phases of the plant lifecycle and that result in a design that reduces the risks and consequences related to human interactions with the plant to as low as reasonably achievable. The program was developed and conducted in line with multiple nuclear regulatory requirements, particularly those in Canadian Nuclear Safety Commission (CNSC) REGDOC-1.1.2, "Licence Application Guide: Licence to Construct a Reactor Facility" (Reference 18.1-2), CNSC REGDOC-2.5.1, "General Design Considerations: Human Factors" (Reference 18.1-3) and CNSC REGDOC-2.5.2, "Design of Reactor Facilities: Nuclear Power Plants" (Reference 18.1-4).

The HFEPP defines the program and outlines the way that the specified general human-centred HFE design goals are operationalized and verified during the design process. This is achieved, through the application of the HFE analyses, integrated design and safety analysis support, and provision of tools, technical requirements, and guidance to designers. The HFE Program ensures that the plant-level design goals are achieved, including:

1. Design of HSIs reduces the likelihood of error and provides for timely, clear error detection.
2. Tasks can be accomplished within time and performance criteria.
3. Allocation of Function (AOF) and proposed job design (staff complement and job roles) are such that a suitable level of human vigilance is ensured and acceptable workload levels that minimize periods of human underload and overload is provided.
4. Presentation of information supports a high degree of situational awareness of the state of the plant and actions required.

5. HSI design supports the capability of personnel to recover from previous decisions and actions that did not achieve intended results.
6. Application of ergonomic principles to working areas and their environments ensure these 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, best-practice guidance, and plant-specific HFE analyses, and through integrated HFE team support to the design. Achievement of the goals is confirmed using the design tools, HFE Testing and Evaluation (T&E) throughout the design development, and HFE Verification and Validation (V&V) of the realized design.

18.1.2 Program Scope

The HFE Program scope applies to HSI components and SSC within or that form part of facilities, systems, equipment, and components throughout the plant. HSIs are defined as any region or point at which a person interacts with a system, equipment, or component. System interface means any digital and electronic Instrumentation and Control (I&C) user interfaces, as well as hardware-based user interfaces and design features on panels, equipment, and individual components. This includes HSIs within or forming part of:

- Control facilities for reactor operations
- Facilities for supporting response to accidents and emergencies
- Control room or stations for radwaste processing
- Control room or stations supporting refuelling and maintenance outage work
- Local control stations
- Equipment- and process line-mounted HSIs
- Auxiliary and support facilities and equipment located external to the main reactor and powerhouse buildings

This includes specification to and oversight of HSIs that form part of SSC 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 also applies across the full scope of users and activities that support plant operation, testing, inspection, and maintenance, including functions such as fuel handling, chemistry, radioactive waste processing, and radiation protection.

The HFE Program described in this plan 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 HSIs, including those at the following locations:

- Main Control Room (MCR)
- Secondary Control Room (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)
- HSIs related to auxiliary and support facilities located outside of the main buildings (e.g., hydrogen tanks or fuel oil supplies)

The HFE Program applies to all plant conditions in the design basis, including normal, outage (refuelling and maintenance outages, including extended refurbishments), abnormal, emergency, and accident conditions. The scope of the HFE Program is extensive; however, the application of HFE support and activities to the scope of each phase and task location is graded (or proportionate), as discussed in Subsection 18.1.4.2 to apply a higher level of emphasis and rigour for important human interactions that are safety-critical or hazardous.

Note that for some phases of the plant lifecycle, particularly Construction and Decommissioning, the HFE activities are focused at a high level. By nature of the single iteration of these plant stages outside of commercial operations, they generally do not involve analysis of recurring operationally related functions and tasks. HFE in design related to these non-commercial operational phases is centred around providing basic guidelines and ensuring design strategies that aid in the achievability of the overall goals of the phase. For example, for decommissioning, HFE design guidelines and requirements for maintainability may equally apply, especially clearance and access for removal of large components and equipment, and consideration of radiological safety through plant structures and equipment layout.

The same general HFE methodologies and tools described in this chapter are also applied to the HSIs related to security. A risk-based approach to HFE design requirements, task support requirements, and testing methodologies is also applied to security considerations. However, due to the sensitive nature of the specific details of security risk ratings, credited human actions, security success criteria, and testing scenarios, the HFE activities for security are found within the Security Annex.

The HFEPP at the time of this PSAR, and in support of the Licence to Construct application, is focused on the design of the plant. After plant turnover to the utility, the utility HFE Program is defined through suitable processes and procedures to address HFE licenced and operating plant activities such as Human Performance Monitoring (HPM), management of change for operational documentation, and design modification activities.

18.1.2.1 Overview of the Human Factors Engineering Program

The HFEPP describes the goals and scope of the HFE Program, along with items such as:

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 organization
5. Process and procedures followed including the process for identifying and managing technical and programmatic issues
6. Documentation developed

7. 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 in the next section.

18.1.2.2 Human Factors Engineering Program Technical Elements

The technical elements for the HFE Program are described briefly below. The full description of these elements, and how they constitute a comprehensive and robust program of HFE integration across the plant design, forms the remainder of this chapter (Sections 18.2 through 18.6).

1. *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. *Functional Requirements Analysis (FRA)* – determination of functions required to achieve plant goals in all plant states (Subsection 18.2.2)
3. *Allocation of Function (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 (TA)* – identification of the tasks required to achieve the allocated functions, and decomposition into task steps to allow the identification and characterization of HSIs, personnel, locations, and support equipment (e.g., communications, lighting, personnel protection) required to perform each task successfully (Subsection 18.2.4)
5. *Staffing Analysis* – determination of the numbers and roles of personal required to support optimal task performance in all plant conditions (Subsection 18.2.5)
6. *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 safety, ensure claimed actions are achievable and identify HSIs requiring the highest level of HFE focus and effort (Subsection 18.2.6)
7. *Human-System Interface (HSI) Design* – identification and management of the set of HFE design requirements from standards, codes, and best-practice guidance, and implementation of those requirements plus results from HFE analyses into the design of HSIs, including integration of HFE team design support; also includes HFE T&E activities (Subsection 18.3.1 through 18.3.6)
8. *Procedures* – process and activities for the development of usable and validated operational documentation, for plant task types (Subsection 18.3.7)
9. *Training and Qualifications* – process and activities for the development of relevant and validated training content, optimized for the plant design, operational documentation, and baseline personnel qualifications and attributes (Subsection 18.3.8)
10. *Human Factors Verification and Validation (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)
11. *Design Implementation* – support and monitoring of the design from “on paper” to a realized constructed plant, including integration with configuration control to ensure no loss of integrity of the HFE Program goals throughout fabrication and construction (Section 18.5)

12. *Human Performance Monitoring (HPM)* – continuous monitoring of user task performance throughout the lifetime of the plant to ensure optimum plant and organizational design and identify early trends and issues that require HFE design improvements (Section 18.6)

    NOTE: This element is only relevant within the future operational plant HFE Program and therefore not currently included in the HFEPP.

The scope and nature of the HFE Program, the HFE organization undertaking the program and the technical elements that comprise it, align with regulatory requirements and international standards and guidance, providing assurance that HFE has been suitably and sufficiently integrated into the plant design.

Table 18.1-1 illustrates the alignment of Chapter 18 and the HFE Program technical elements, with the CNSC expectations for HFE, as per CNSC REGDOC-2.5.1 (Reference 18.1-3) and CSA N290.12-14, “Human factors in design for nuclear power plants” (Reference 18.1-5). The PSAR and HFE Program technical elements inform the subsequent pre-operational safety analysis report and ultimately the overall plant lifecycle of HFE activities.

Although arranged somewhat differently in the PSAR chapter and HFE Program, all required elements are included and addressed. The elements are performed in an iterative manner, with activities and outputs progressively evolving with the design and related safety analyses. These elements inform one another, inform, and are informed by plant design and safety analyses, and are aligned with design and engineering processes and requirements, international best-practice guidance, and regulations.

Table 18.1-1: Mapping of HFE Program Elements with CNSC and CSA Requirements

ELEMENT NO.	PSAR CONTENT	CNSC REGDOC-2.5.1	CSA N290.12-14
--	18.1 Management of the Human Factors Engineering Program	HFEPP, including: Goals, Scope, Background, Criteria for Areas of Consideration Human Factors Input, including: HFE Organization Roles and Responsibilities, Training Needs and Related Groups Methods, including intended tools and technical guides HFE Processes and Procedures Timelines, including logical links to related project activities Documentation Disposition of Human Factors Issues	*HF Planning:* Determine methods, analyses, evaluations, project interfaces, and tools Identify constraints and drivers Graded approach based on risk and complexity Organization and resources Communications Source documents Issue identification and resolution Documentation Scheduling HFE Interfaces with other groups
--	18.2 Human Factors Engineering Analysis		
1	18.2.1 Review of Operating Experience	Operating Experience Review	*HF in Concept Design:* OER
2	18.2.2 Functional Requirements Analysis	Functional Analysis	*HF in Concept Design:* functional analysis
3	18.2.3 Allocation of Function	Allocation of Function	*HF in Concept Design:* functional analysis (definition includes AOF)
4	18.2.4 Task Analysis	Task Analysis, Job Design	*HF in Preliminary Design:* TAs including workload and communications analysis; link analysis
5	18.2.5 Staffing	Staffing & Minimum Shift Complement, Job Design, Shift-Work Systems	*HF Interfaces:* HF in design shall consider the interfaces with staffing; the information common to both HF in design and interfacing disciplines, such as staffing analyses and strategies, should be shared.

ELEMENT NO.	PSAR CONTENT	CNSC REGDOC-2.5.1	CSA N290.12-14
6	18.2.6 Treatment of Important Human Actions	Human reliability, activities with potentially hazardous human interactions	*HF in Concept Design:* identification of scenarios to be analyzed *HF in Preliminary Design:* participation in the assessment of human actions and error consequences; assessment of the feasibility of human actions in the deterministic safety analyses *HF in Detailed Design:* confirmation of the feasibility of human actions important to safety in the probabilistic and deterministic safety analyses; analyses to confirm the ability of the human to perform necessary actions
7	18.3 Design of the Human-System Interface 18.3.1 Design Goals and Design Bases	Design human-machine interface system; design physical working environment	
7	18.3.2 Human-System Interface: Design Inputs		*HF in Concept Design:* a statement of system operational purpose and operational requirements under all anticipated conditions; development or selection of HF in design source documents; identification of SSC requirements to support necessary human actions; HFE assessment of design concepts and options *HF in Preliminary Design:* document high-level HF-related requirements; input to specifications and bid evaluations; requirements derived from HF analysis results
7	18.3.3 Human-System Interface: Detailed Design and Integration		*HF in Detailed Design:* detailed HSI design; design integration of Commercial-Off-The-Shelf (COTS) products

ELEMENT NO.	PSAR CONTENT	CNSC REGDOC-2.5.1	CSA N290.12-14
7	18.3.4 Human-System Interface: Tests and Evaluations		*HF in Preliminary Design:* modeling, mock-ups, or prototyping of user interfaces; evaluations *HF in Detailed Design:* Usability testing
7	18.3.5 Human-System Interface: Design of Main Control Room		Covered within all HF in Design activities
7	18.3.6 Human-System Interface: Design of Secondary Control Room		Covered within all HF in Design activities
8	18.3.7 Procedure Development	Procedure Development	*HF in Detailed Design Stage:* HF analyses output to development of training manuals, operating procedures, and commissioning procedures
9	18.3.8 Training and Qualification Program Development	Training Program Development	*HF in Detailed Design Stage:* HF analyses output to development of training manuals, operating procedures, and commissioning procedures
10	18.4 Human Factors Engineering Verification and Validation	Verification Validation	*HF in Detailed Design Stage:* Verification (carried out before the design is released for construction) Validation (validation activities split between detailed design and implementation)
11	18.5 Design Implementation (post-construction)	Design Implementation	*HF in Design Implementation Stage:* HFE during installation and commissioning
12	18.6 Human Performance Monitoring (at start of testing)	Human Performance Monitoring	N/A (scope of standard is design stages only)

18.1.3 Team and Organization

The HFE team consists of a core and extended team dedicated to integrating HFE requirements and principles into the design. The core HFE team sits within the organization as a separate engineering team, at an equal level to all other discipline teams. The HFE team holds the technical authority over HFE activities and requirements and has the equal authority and issues resolution mechanisms as any other engineering team. The extended HFE team includes members from other disciplines within the engineering organization. This ensures fully integrated and timely consideration of HFE in the daily engineering design decisions and activities.

The core HFE team is comprised of an HFE Technical Lead and two general roles: HF Engineer or HFE Specialist and HFE Operations/Maintenance. The qualifications for these roles may be met by individuals or collectively by the HFE team. The responsibilities and qualifications of these roles are defined in the HFEPP as summarized below:

1. Technical Lead: 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; point-of-contact for schedule development, integration, and management of the program. This role is expected to have the base qualifications of either the HFE Specialist or HFE Operations/Maintenance role, with additional HFE capability across a breadth of HFE competence areas suitable for the full scope of the HFE Program and experience in project management and managing HFE or other technical, cross-cutting programs.
2. HF Engineer/HFE Specialist: Provide specialized 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; identify and participate in the resolution of identified HFE issues and non-compliances. This role requires a bachelor’s degree in HFE, Engineering Psychology, or related science with four years of cumulative experience related to the HFE aspects of HSIs (design, development, and T&E), particularly modern digital process control HSIs, and four years of cumulative experience related to the HFE aspects of workplace design.
3. HFE Operations/Maintenance: Provide knowledge of operations and maintenance activities, including task characteristics, HSI characteristics, environmental characteristics, and technical requirements related to operational activities, and apply those insight in support of activities such as development of HSIs, procedures, and training programs. Participate in the development of scenarios for Human Reliability Analysis (HRA) evaluations, task analyses, HSI T&E, validation, and other evaluations. This role requires a bachelor’s degree in a technical field; experience as a senior authorized reactor operator, or as a qualified maintenance technician; five or more years of plant experience, preferably in Boiling Water Reactors exposure to plant procedure development, personnel training, and operational nuclear plant programs; and two or more years of experience in one or more areas of HFE analysis, design, T&E, and HFE V&V.

The responsibilities of the HFE team are to establish and perform the activities as defined in this PSAR chapter throughout the design lifecycle to ensure that the facilities, systems, equipment, and tools are designed to be compatible with the capabilities, limitations, and needs of the human. The specific duties of the HFE team are to guide, perform, and support the analysis and design activities, ensuring the execution and documentation of all steps in the activities are performed in accordance with the established program and procedures.

The HFE team is responsible for:

1. Development of HFE plans and procedures including management of any identified HFE issues
2. Oversight, participation in, and review of HFE design, safety analyses, development, T&E activities, including identification of in-process HFE issues
3. Recommendations for, and support to implementation of design-based resolutions for issues identified during the implementation of the HFE requirements and analysis results
4. Verification of correct and robust implementation of HFE requirements, analysis results and issue resolution into the design
5. Assurance that HFE activities comply with HFE plans and procedures
6. Managing documentation of HFE activities and issues management
7. Plan and implement HSI design configuration control during design implementation

To ensure suitably qualified and experienced persons are performing the work, HFE Program activity assignments are allocated by the Technical Lead based on the team member's role and their specific experience. For example, not all the team HF Engineers/HFE Specialists are experienced in HFE safety analysis, identifying, and evaluating important human actions. Only those team members with adequate experience and training (if applicable) in a particular HFE activity will be assigned to those activities. To ensure there are no singleton specialisms within the team and associated vulnerability to knowledge loss, more than one team member will be required to be deemed competent for each activity. Team members that do not meet the full qualification of an HFE team role, or who are not deemed suitably qualified for a specific activity, will receive mentoring and technical oversight to support developing the skills required for the role or work assignment.

18.1.3.1 Cross-Discipline Support and Integration

Due to the cross-functional nature of a completely integrated HFE design process, HFE activities interface with many other disciplines. In addition, the other disciplines act as extended parts of the HFE team for some aspects of the HFE Program implementation. 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.

Specifically, work activities that require integration of HFE and other disciplines are entered into the resource-loaded schedule by the HFE Technical Lead with all required resources, including those from other teams. Pre-job briefs are held for each group of activities, or workplan, to clearly define the relevant resource roles and responsibilities for the completion of the work. Further detail on GEH and the BWRX-300 project design processes, including inter-discipline communications and issues resolution, are described in Chapter 17, Sections 17.2 and 17.3.

The descriptions of the following disciplines and groups and their contributions to HFE are representative based on best-practice HFE integration principles. The actual engineering design team disciplines may vary, but the scopes described are covered.

1. Mechanical Engineering and Electrical Engineering
    a. Provide knowledge of the purpose, operating characteristics, and technical specifications of major plant systems
    b. Provide input to HFE analyses, especially function and task analyses

   c. Allocate and implement HFE requirements and recommendations relevant to their scope of design, including management of those requirements provided to suppliers
   d. Participate in developing scenarios for use in TA, validation, and other analyses
2. I&C Engineering
   a. Provide detailed knowledge of the HSI physical design, including control and display hardware selection, design specification, functionality, and installation
   b. Support HFE design of information display design, content, and functionality, particularly connection to the underlying I&C platform
   c. Participate in designing, developing, testing, and evaluating the HSIs
   d. Provide knowledge of data processing associated with displays and controls
   e. Allocate and implement HFE requirements and recommendations relevant to their scope of design, including management of those requirements provided to suppliers
   f. Participate in designing and selecting HSI components, such as controls and displays
   g. Participate in developing scenarios for HRA, validation, and other analyses involving failures of the HSI data processing systems
3. Civil/Structural Engineering
   a. Provide knowledge of the overall structure of the plant, including performance requirements, design constraints, and design characteristics of the following:
      - Containment structures (i.e., Steel-Plate Composite Containment Vessel)
      - Control Rooms (main and secondary)
      - Local control
   b. Provide knowledge of the configuration of plant components
   c. Allocate and implement HFE requirements and recommendations relevant to their scope of design, including management of those requirements provided to suppliers
   d. Provide input to plant analyses, especially function analysis, TA, and development of scenarios for TA and validation
4. Plant Integration Engineering
   a. Prepare the Deterministic Safety Analysis (DSA) establishing the SSC and human actions that are credited for successful event mitigation
   b. Provide knowledge of maintenance, inspection, and surveillance activities based on previous plant design and consideration of evolving new plant design, including:
      i. Development of maintenance and outage strategy and plan documents
      ii. Expected tasks
      iii. Relevant SSC and HSIs
      iv. Task performance requirements
      v. Workspace environment characteristics
      vi. Technical information related to the conduct of these activities

c. Allocate and implement HFE requirements and recommendations relevant to their scope of design, including management of those requirements provided to suppliers

d. Support Plant Architectural and HFE design, development, and evaluation of the control facilities and other HSIs throughout the plant to provide reasonable assurance that each can be inspected and maintained to the specified reliability

e. Provide input regarding maintainability and inspectability during the development of procedures and training

f. Participate in the development of scenarios for HSI evaluations including task analyses, HSI design tests and evaluations, and validation

5. Risk and Reliability Engineering

   a. Perform Probabilistic Safety Assessment (PSA) and HRA to quantify the human contribution to risk and inform HFE analyses

   b. Provide knowledge of plant component and system reliability and availability and assessment methodologies to the HSI development activities

   c. Participate in the development of scenarios for HSI evaluations, especially validation

   d. Provide input to the design of HSIs to provide reasonable assurance it meets reliability goals during operation and maintenance and maintains the specified availability

6. Simulation Assisted Engineering

   a. Develop the simulators for HFE T&E and V&V activities

18.1.4 Process and Procedures

18.1.4.1 Coordination and Documentation of Activities

The HFE Program is planned and conducted in accordance and alignment with overarching design and quality program processes and procedures, within accredited quality management systems as described in Chapter 17. The work is performed in an integrated manner with HFE as an equal design discipline, whose cross-cutting requirements and support are embedded within all other design disciplines, with activities, inputs, outputs, and dependencies coordinated through a detailed schedule and associated schedule management processes. The schedule includes activities and deliverables for all disciplines and orders them with logical connections to ensure they are completed in the required sequence.

To help ensure cross-discipline communication and coordination, activities include scheduled periodic formal design reviews conducted by representatives of each discipline. Additionally, deliverables are completed in accordance with a deliverable standard, which specifies the required content from all related disciplines, dictates the format for consistency and quality and specifies the required discipline reviewers for each document. This includes other disciplines reviewing and incorporating outputs from HFE documentation and the HFE team reviewing and incorporating outputs from other disciplines, as appropriate and according to the plan.

The documentation for the HFE Program uses a standard design process that includes documenting internal design records to capture inputs and outputs, as well as providing the basis for formal deliverables. The information in the design records is incorporated into the design by HFE and other disciplines as appropriate and in accordance with the BWRX-300 project work breakdown structure. A full description of the management and integration of HFE activities within the project is described in the HFEPP.

In this way, using the project processes and HFE coordination measures described in the HFEPP, the design activities related to HFE are conducted and documented such that design basis, input maturity and rationale for design and analysis scope is provided for HFE design decisions and analysis results. HFE requirements and recommendations are addressed by the requirements management process (Subsection 18.1.4.3), 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 as described in Subsection 18.1.5.

18.1.4.2 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 HSIs used to perform human actions important to safety, or tasks that are novel, complex, or inherently hazardous. 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
- Asset Protection
- Generation Capability

Although Asset Protection and Generation Capability are typically discounted as relating to safety, the HFE Program recognizes 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 recognized to have a direct effect on plant condition, organizational health, and ultimately, nuclear safety culture.

The overall risk level for the human action 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 when considering each HFE technical element. Further detail is provided in Subsection 18.2.3.

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 HSIs receive a full HFE V&V, all HSIs receive some degree of HFE support during the design phase.

18.1.4.3 Requirements Management

HFE requirements management is performed in accordance with a requirements management process that is standardized and controlled across the entire plant design, as described in Chapter 17, Subsection 17.3.1. 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 categorized 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 HSIs. 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. Requirement traceability and HFE support level is proportionately applied based on the assessed risk-based grading (Subsection 18.4.2).

Where HFE inputs are not in agreement with one another or where they conflict with other discipline design requirements, precedence is given as follows:

- Laws and Regulations
- Regulatory Requirements and Guides
- Requirements related to supporting, maintaining, or recovering the plant in a safe state
- Nuclear Standards
- Nuclear Industry Guidance Documents
- Non-Nuclear Codes, Standards, and Guides

Conflicts between HFE and other design requirements are resolved with the HFE team using the HFE issue resolution process described in Subsection 18.1.5. Decisions regarding trade-offs and design optimizations are conducted within the integrated design process in accordance with standard GEH design procedures.

18.1.5 Issue Tracking

Included in the HFE Program is the establishment and maintenance of an on-going HFE Issues Tracking System (HFEITS) for documenting HF issues that may be identified throughout the full scope of HFE activities, and the actions taken to resolve those issues.

The HFEITS is used to capture issues related to design and implementation HFE activities and specific Human Engineering Discrepancies (HEDs) identified through HFE V&V. The tracking of issues include:

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 HSI 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

18.1.6 References

18.1-1 NEDC-33982P, “BWRX-300 Darlington New Nuclear Project (DNNP) Human Factor Engineering Program Plan,” GE-Hitachi Nuclear Energy Americas, LLC.

18.1-2 CNSC Regulatory Document REGDOC-1.1.2, “Licence Application Guide: Licence to Construct a Reactor Facility.”

18.1-3 CNSC Regulatory Document REGDOC-2.5.1, “General Design Considerations: Human Factors.”

18.1-4 CNSC Regulatory Document REGDOC-2.5.2, “Design of Reactor Facilities: Nuclear Power Plants.”

18.1-5 CSA N290.12-14, Human factors in design for nuclear power plants, Canadian Standard Association.

18.2 Human Factors Engineering Analysis

In this section, six of the HFE Program technical elements are described in depth. The remaining elements are described in other sections. These six elements described in this section include:

- Review of Operating Experience (OE)
- Function Requirements Analysis
- AOF
- TA
- Staffing
- Treatment of Important Human Actions

These are addressed in Subsections 18.2.1 through 18.2.6.

Integrated HFE involvement in, and support of the plant safety analyses also informs these elements. As described in Subsection 18.2.6, the HFE safety analyses activities identify, characterize, and substantiate the human actions that are performed to maintain the plant within or bring it back to a safe state, as described in Chapter 15, Safety Analysis.

18.2.1 Review of Operating Experience

The HFE Program includes the early review of OE to identify applicable HFE issues related to process or personnel safety that can be resolved through design improvements. The issues and lessons learned from the OER provide a basis for improving the plant design in a timely way (i.e., at the beginning of the design process). In addition to the early HFE review of existing OE, the project as a whole has a formal OE identification and management process, which includes HFE team participation in both identifying any OE and implementing HFE-allocated OE items in the HFE Program and design.

18.2.1.1 Objectives and Scope

The objective of the OER is to obtain information and lessons learned from experience to support design of BWRX-300 SSC. OE related to the following areas are considered in the development of the plant design:

- Predecessor plant(s) and systems
- Experience in industries with applicable SSC
- Applicable Industry HSI design experience
- Risk-important human actions
- Specifically identified applicable industry issues
- Issues identified by predecessor or similar plant personnel
- Specifically identified positive features that support task performance

18.2.1.2 Methodology

The OER process includes the following:

- Identification of applicable OE sources, leveraging work previously performed for predecessor plant designs

- Specific methods for gathering sources and performing reviews of sources since the predecessor plants and systems OER
- Establishing a systematic framework and performing systematic searches of OE 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
- Analyzing and consolidating raw OE data into OE Item Summaries on the OER Capture Sheet
- Allocation of each OE item to the HFE activity or document in which the OE item is dispositioned
- Recipient OE item review and allocation acceptance
- Documentation of the findings within an OER report

Existing and new OE is reviewed by HFE, and relevant, applicable problems, issues, and positive insights are identified and addressed throughout the design process. The OER information is made available to design engineers to support development of design features that are expected to reduce human error. Likewise, positive features of previous designs are communicated so that they can be retained.

18.2.1.3 Results

The results of the OER are summarized in an OER report. The report provides the OER process description along with the review methods that were used. The results include:

1. Sources of OER information
2. Summaries of OER issues and improvements
3. List of issues from the OER requiring special attention in the design process based on the grading process
4. Information gathered from personnel interviews conducted at predecessor plants

Implementation of the OER results into the design is managed and tracked through the assignment of and reference to a unique OE identification number. Communication and allocation of the results to the appropriate design team and design requirements document is managed by the HFE team.

The HFEPP provides additional details of the OER activity.

18.2.2 Functional Requirements Analysis

18.2.2.1 Objectives and Scope

FRA is performed to define the necessary functions that enable the achievement of the plant safety and commercial goals. These principal design requirements are necessary to meet plant goals and objectives in all normal and postulated accident conditions. They include meeting regulatory and customer requirements that are documented in plant and product level design requirements specifications.

18.2.2.2 Methodology

FRA is conducted as an integral part of the overall engineering design process specified by standard design process documents, and in particular part of the BWRX-300 requirements management process. The requirements management process as described in Chapter 17, Subsection 17.3.1 consists of the following activities, which apply equally to all types of requirements including the functional ones: elicitation, analysis, documentation, allocation (to specific system(s)), tracing, and requirements V&V. This process is a multi-discipline activity jointly undertaken by all design teams, including the HFE team. Note that, because BWRX-300 is an evolutionary plant with some of the same or similar plant- and system-level safety and performance goals, FRA elicitation is not required to the extent it would be for a completely new design. Eliciting functional requirements from existing design is done through importing functions that exist in current plant designs and are expected to apply to BWRX-300.

18.2.2.3 Results

The result of the multi-disciplinary FRA activities is the definition of the full set of functions that support achievement of the plant goals and 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. Through the requirements management process described in Chapter 17, Subsection 17.3.1 the project has also captured system functional performance requirements which includes the full list of plant functions, with reference and traceability back to the source documents where the requirements were elicited.

These functions from the FRA are captured in a report that also includes the results from the AOF (see next section) and assigning HFE Application Levels to tasks (Subsection 18.1.4.2). The results are input into the AOF process as described in the next section. The output from the FRA and AOF process also contains the full list of functions with characterizations of relevance to HFE, particularly those required to perform AOF and feed to the TA and HSI design activities.

18.2.3 Allocation of Function

18.2.3.1 Objective and Scope

AOF establishes a plant control scheme that enhances plant safety and reliability by taking advantage of human and system strengths and avoiding human and system limitations. The overall allocation can also enhance plant performance and safety by specifying overlapping and redundant responsibilities to the human and system.

The AOF strives to provide personnel with groups of logical, coherent, and meaningful tasks within their capabilities, and ensures a design that maintains human vigilance and situational awareness for any functions allocated to the system. The goal of the AOF is to provide acceptable workload levels per job role that minimize 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. Further analysis of workload and requirements for situational awareness are then undertaken through downstream activities such as TA, HFE T&E and HFE V&V.

The AOF also allows the risk-based task grading, which determines the HFE proportionate, graded approach to activities, as described in Subsection 18.1.4.2.

18.2.3.2 Methodology

The AOF process for BWRX-300 is based on the relevant best-practice methodology presented in IAEA-TECDOC-668, “The role of automation and humans in nuclear power plants” (Reference

18.2-1). The methodology identifies functions that should not be assigned 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 USNRC NUREG/CR-2623, “The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review,” (Reference 18.2-2) 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.

The FRA process provides the list of functions input to the AOF, as described in Subsection 18.2.2. The AOF process is composed of two stages: the first stage establishes an initial (hypothesized) allocation; the second stage evaluates the hypothesized AOF to determine its adequacy and validate that it is optimized within the larger integrated task performance and work environment.

The initial AOF is determined following a formal decision flow with key allocation criteria informing each decision point. The decisions are based on expert judgement formed by a panel that includes an HF Engineer/HFE Specialist, an HFE Operations/Maintenance representative, a Plant Integration Engineering representative, and a System Engineer for the respective system. The expert panel accounts for the mandatory criteria when hypothesizing the initial allocation. The panel also makes use of OE to determine how functions were allocated in previous or similar applications and evaluate how they have performed.

The second stage of the AOF process is the AOF evaluation. This stage is performed later in the design and HFE T&E process, following completion of system level and integrated TA. 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, where overload issues are less likely to be revealed. Functions and tasks allocated to humans are considered in combination using scenario development. The scenarios are then evaluated to determine acceptability based on expected concurrent task performance, workload (physical and cognitive), vigilance, and situation awareness.

As part of the AOF activity, functions are decomposed to tasks, and multiple tasks may be necessary to support each function. For example, to fulfil a core protection function, a task to perform a system readiness surveillance test supports the eventual task of safety system initiation. The function tasks require a “task allocation” that uses the same criteria applied at the overall AOF level. The safety analyses also provide input to the AOF, specifying when human actions are required to backup automatic (i.e., system) actions.

In addition to allocation, within the AOF activity, task grading is completed. As described in Subsection 18.1.4.2, a graded approach to HFE is applied to the BWRX-300 project. The human actions resulting from the AOF process described above are graded based on four key risk categories:

1. Nuclear Safety
2. Personnel Safety
3. Asset Protection
4. Generation Capability

The characteristics of the human actions are assessed against criteria in each category that results in an initial High, Medium, or Low numerical risk rating. This gives the overall minimum HFE Application Level for activities within the HFE Program for each human action. The scope and level of detail for each HFE technical element is defined for each of these HFE Application Levels.

When the risk is assessed numerically using the initial ranking criteria, the result is a minimum HFE Application Level. The HF Engineer/HFE Specialist reviews the rating and the associated HFE scope and level of effort for each technical element and takes into consideration other HFE risk factors to determine if the HFE Application Level needs to be increased for that specific technical element. The additional risk factors include:

- Complexity of the action
- Anticipated complexity and constraints of HSI
- Complexity of the system
- Frequency of the task
- Physical environment
- Cognitive environment
- Novelty of the action, system, or HSI technology
- Time sensitivity of the action

The review of an individual HFE technical element for each human action may increase an HFE Application Level but not reduce it. For example, a particular human action may have a low minimum application level based on the broad key risk criteria, but because it is a complex or novel task, it is raised to a higher application level for the TA activity.

18.2.3.3 Results

Output from the first stage of AOF is the initial AOF to human, system, or shared (both human and system). For system or shared allocations, it may be necessary to establish backup actions when redundant functions with like allocations is not possible or reasonable. For these cases, the shared and backup allocation categories are used.

The initial allocation for each system AOF is documented in a workbook which is formally managed as an internal design basis record. The workbook is communicated to all relevant stakeholders (Mechanical and I&C engineers, as well as HFE analysts) to be used as the basis for the design and TA. The initial allocation is revised and refined as necessary as the plant design and safety analyses progresses.

The results from the AOF evaluation are a final refinement of the initial allocation, including design and safety analysis modifications where necessary to support changes to allocation outcome. The final optimal AOF is used for Integrated System Validation (ISV) testing to confirm that performance, workload, and situation awareness are suitable.

The results of the AOF development and refinement activities, and specification of the final AOF are provided in a summary report.

18.2.4 Task Analysis

TA is the identification of task requirements to accomplish the functions and tasks that have been allocated in whole, or in part, to humans. These are designated in the AOF results as Human, Shared, or System with Human Backup.

TA assigns tasks to the job positions specified by the staffing process. TA determines the steps needed to accomplish human actions and documents the task details and required task support HSI controls, indications, and alarms). The TA process also assesses the graded HFE Application Level to determine if a change to is warranted based on task characteristics.

18.2.4.1 Objectives and Scope

The TA plan establishes:

1. Methods for conduct of the TA consistent with accepted HFE practices and principles
2. Scope of the TA including actions performed at the MCR, SCR, and at other control facilities, including those required to support response to accidents and emergencies
3. Range of plant operating conditions, including start-up, normal and abnormal operations, transients, refuelling, lower power, and shutdown conditions, and emergency or accident conditions
4. HSI operations during periods of maintenance, testing, and inspection of plant SSC
5. Links among task descriptions and safety importance, function achievement, human error potential, and impact of task failure
6. Descriptions of the personnel activities required for successful completion of tasks
7. Requirements for alarms, displays, data processing, and control

18.2.4.2 Methodology

The task inputs provided by the AOF and Task Grading process form the starting point for TA. These tasks are divided into levels of effort as defined through the task grading portion of the AOF process, as described in Subsection 18.2.3. All tasks regardless of HFE Application Level receive a TA. However, the level of detail within the TA varies based on HFE Application Level. For example, those at the lowest risk level may be performed by the responsible System Engineer and reviewed by HFE for acceptability.

There are two levels of TA: Basic TA and Detailed TA. Human actions ranked at the lowest HFE Application Level undergo a Basic TA; human actions at the medium and highest HFE Application Levels undergo a Detailed TA. The Detailed TA also includes preliminary workload analysis and assessment of requirements for situational awareness. In addition to the Detailed TA, the highest HFE Application Level requires additional link Analysis and timeline Analysis to be performed to evaluate and inform the layout of HSIs to optimize task performance.

Basic TA consists of:

- Task Selection
- Task Step Sequence Narrative, including:
    - Descriptive narrative of the task
    - Cue that determines the need for the task
    - Action to be taken
    - Prerequisites for the task
    - Time available versus time required to complete

Detailed TA consists of:

- Task Selection

- Task Step Sequence Narrative, as per Basic TA
- Task-Level Support, Job Design, Workload, and Workplace Definition including:
  - Information needed
  - Controls needed
  - Alarms needed
  - Personnel involved
  - Communication needs
  - Location and access considerations
  - Workspace needed
  - Job aids, tools, or equipment needs
  - Environmental considerations and potential hazards
  - Special clothing or personal protective equipment needs
  - Time available versus time required to complete (if needed on a step basis)

The Detailed TA is coordinated with the qualitative human error analysis, which is informed by and used to substantiate the quantitative HRA, as described in Subsection 18.2.6. The TA also identifies critical task steps where incorrect or incomplete actions might lead to undesired or unsafe consequences.

The TA activity also includes Integrated TA. Integrated TA is conducted for those operations that require interaction with multiple systems and a coordinated response that may involve multiple plant personnel. The Integrated TA takes the system-level TAs and the results from the human error analyses (described in Subsection 18.2.6) and performs higher-level whole sequence analyses, including integrated workload analysis and timeline analysis. The Integrated TAs, at a minimum, include each event sequence that contains an HFE Application Level 1 human action and each unique scenario described in the plant safety analyses.

18.2.4.3 Results

The BWRX-300 TA procedure defines set templates for capturing the TA, which are combined with the AOF results workbook, documenting the full set of analysis activities. The activities are iterative and progressive, and the workbook method allows timely and effective update of the TA and distribution of the results. The TA workbook is functionally divided into subsets of information needed to process the output activities from TA, including input to:

- Staffing and qualifications
- HSI development, including I&C Data Connection Tables (DCTs)
- Training development
- Procedure development

The results from the additional link, timeline and preliminary workload analyses in the Detailed TAs are also used to further inform the HSI design requirements, confirm or identify issues with the AOF, and provide a baseline for HSI T&E activities. The Integrated TA results provide an input into group-use and aggregate HSI designs, control facility and plant location and workspace design considerations, development of plant-level procedures, and the scenarios selected for ISV.

The results of all the TA activities, when they are complete, are summarized in a TA summary report.

18.2.5 Staffing

The required and expected number of personnel available to achieve plant functions and goals is an important consideration throughout the design process and in HFE analyses. BWRX-300 staffing assumptions and analysis results are used to frame the future plant operating organization during TA, HRA, and HSI design.

Features of the BWRX-300, such as passive safety systems, increased automation, and simplified HSIs, information systems and content, decrease the assumed initial staffing requirements relative to previous Boiling Water Reactors. For example, TA done as part of the HFE safety analysis work, described in Subsection 18.2.6, may show that the extended time for safety actions may reduce the number of personnel needed for local actions. Safety analyses and identification of human actions may show that some actions that were important in previous boiling water reactor designs have been eliminated in the plant design.

18.2.5.1 Objectives and Scope

Staffing analysis is conducted to determine the minimum staff complement. The minimum staff complement is defined as the minimum number of workers with specific qualifications who are available to the site at all times. The minimum staff must be able to operate and maintain to the plant within its defined safe operating envelope and to successfully respond to all postulated events in the safety analyses, in any plant state.

For staffing assumptions where minimum staff can be varied for different operational states, the most resource-intensive events for each plant mode are analyzed. The Staffing Analysis technical element also determines the maximum staffing in collaborative areas such as control rooms, workshops, and air locks. This informs the needed space, facilities, and other support features.

18.2.5.2 Methodology

The Staffing Analysis for BWRX-300 is conducted in accordance with a plan that was developed to meet the expectations and requirements of CNSC REGDOC-2.2.5, “Minimum Staff Complement” (Reference 18.2-3). The process takes place in three major steps: Expert Panel Staffing Assessment; Staffing Analysis in TA and HSI design; and Staffing Analysis in the HFE V&V Process.

The process starts with an assumed initial staff complement taken from predecessor and similar plants, and representative OE from the operating fleet. Using this information, the initial staffing is optimized, considering the modern design features and new systems of the BWRX-300.

The optimized initial staffing level is subject to an Expert Panel Staffing Assessment that evaluates the minimum staffing to cope with selected credible events. The goal is to perform early and iterative assessments as the design progresses such that the risk of less than adequate staffing is reduced in part with each evaluation. The evaluations are performed as a desktop (talk-through) exercise led by the expert panel. The expert panel is made up of personnel from the HFE team, supported by personnel from Plant Integration Engineering and Risk and Reliability Engineering.

The next steps take place in conjunction with the TA and HSI design process. During TA, task steps are defined, and personnel assignments are made. The TA forms the basis for job design and qualifications for each role. With the TA, timeline analysis is conducted for the most resource-intensive credible events. These events are selected by the expert panel, and the expert panel also performs a review of the timeline analysis and input TA data to evaluate whether the minimum staff complement is adequate.

After this, scenarios for a wider range of events are created and analyzed in the T&E phase of the TA and HSI design process. This allows further evaluation of the minimum staff complement against the most challenging credible events. HSI tests evaluate, using platforms and mock-ups that replicate the interface design, the timing of activities, workload, and other factors such as situation awareness that can lead to changes in the minimum staff complement and job design.

In the final analysis stage, the minimum staff complement is evaluated through the HFE V&V activities. This occurs during early validation in accordance with the multiphase validation approach (Section 18.4), culminating with the ISV. ISV demonstrates the adequacy of the final staffing levels that resulted from the analysis.

18.2.5.3 Results

The staffing analysis results are recorded in a series of reports capturing each Expert Panel Assessment, and a further report capturing the Expert Panel Review of the related staffing analysis activities. In addition to these reports, outputs and reports that are created for the TA and HSI design process and HFE V&V in accordance with those associated technical element descriptions, include results related to or impacting the staffing analysis results.

The confirmed job role and complement determination is also used as an input to training and qualification program development, where base qualifications are established, and the training program is designed (Subsection 18.3.8).

18.2.6 Treatment of Important Human Actions

Consideration and integration of HFE within the safety analyses, and consideration of the results and assumptions of the safety analyses within the other HFE activities both comprise the technical element of Treatment of Important Human Actions. The set of activities supporting this HFE technical element was developed based on requirements for HFE expertise in safety analyses per IAEA SSG-51, “Human Factors Engineering in the Design of Nuclear Power Plants” (Reference 18.2-4), CNSC REGDOC-2.5.1, “General Design Considerations: Human Factors” (Reference 18.2-5), CSA N290.12-14, “Human factors in design for nuclear power plants” (Reference 18.2-6), and international best practice.

18.2.6.1 Objectives and Scope

HFE safety analysis activities, including review of safety analyses outcomes, provides assurance that the full set of human actions that are important to safety are explicitly identified, characterized, and substantiated as achievable within the task performance requirements.

The important human actions are determined using both deterministic and probabilistic means and include identification of the human actions that might cause or contribute to the cause of postulated initiating events. Inclusion in the DSA, PSA, or Severe Accident Analysis (SAA), or other identified contribution to risk determines the risk level in the Nuclear Safety category for determining the initial HFE Application Level to apply to the HFE activities (Subsection 18.1.4.2). Comprehensive, systematic identification and substantiation of human actions claimed within the safety analyses, coupled with the risk-based graded approach described in Subsection 18.1.4.2, ensures that HSIs and tasks associated with important human actions are analyzed and designed with a full detailed and robust HFE effort.

18.2.6.2 Methodology

The safety functions that are performed to maintain the plant within or return it to a safe operating envelope are identified through various means using DSA, PSA, and SAA, as described in Chapter 15, Safety Analysis.

HFE safety analysis activities use the various safety analyses, available system design information, particularly that related to HSIs, and any available and applicable TA results (Subsection 18.2.4) as inputs.

The activities that form part of this technical element include:

1. Perform a Human Operation Hazard Evaluation
2. Review the DSA for explicit and implied human actions, e.g., human actions related to maintenance that ensure safety-class SSC availability, and ensure claimed human actions are achievable through qualitative human error analysis
3. Review the PSA and HRA for:
   a. Ensuring event sequences introduce a Human Performance Limiting Value
   b. Perform qualitative human error analysis to substantiate or refine the human error probabilities used for all human actions claimed in the HRA
   c. Provide HFE qualitative basis and substantiation for any dependency assumptions and analysis
   d. Provide HFE qualitative basis and substantiation for any timeline assumptions and analysis
4. Review the SAA, including Level 2 and Level 3 PSA, to identify explicit and implied human actions, determine task achievability in required timescales, and capture input for procedure development (Subsection 18.3.7) and emergency planning and response (as described in Chapter 19)
5. Compile a database of all important human actions claimed in the safety analyses, including the source of the claim, their key characteristics, related assumptions and any associated HSIs

For each of the above activities, the task performance criteria are defined to enable the HFE analysis to determine the acceptable achievability of each identified human action. Task performance requirements depend on the plant conditions the task is performed in (normal versus abnormal versus emergency or accident conditions), and for events, are defined by the related safety analysis the HFE analysis is underpinning. For example, for precursor human actions, performance requirements are usually "performed correctly" or "performed in accordance with maintenance schedule timelines". For post-initiating event human actions, the requirements are defined by the event conditions. Tasks must be achievable, completed successfully and, where dictated by the related analysis, must be completed within the required time based on the event timeline.

18.2.6.3 Results

The outputs from the activities that form this technical element includes:

1. A Human Operation Hazard Evaluation report that documents the methods used and the evaluation results
2. Design records capturing results of safety analyses reviews

3. Design records capturing HFE qualitative human error analysis and other substantiation of claimed human actions in the various safety analyses
4. A Human Action Claims database containing all important human actions and critical information for each, allowing for adequate and robust consideration in the design
5. A summary report, which summarizes the methods, results, and issues from each of the above outputs

The results are communicated directly to the appropriate design, safety analysis and other HFE team members performing related technical elements, to ensure timely consideration of the full set of human actions important to safety in their respective activities. The outputs from each activity and the Human Action Claims database capture the source of the identified human actions within the safety analysis to allow full traceability from the origin through HFE safety analysis and forward to any design requirements or safety analysis modifications.

In addition to specific HFE safety analysis activities described in this section, the full complement of safety analysis outcomes, including the PSA and HRA, informs and acts as input to the other HFE technical elements, as applicable.

18.2.7 References

18.2-1 IAEA-TECDOC-668, "The role of automation and humans in nuclear power plants," International Atomic Energy Association.

18.2-2 USNRC NUREG/CR-2623, "The Allocation of Functions in Man-Machine Systems: A Perspective and Literature Review," U.S. Nuclear Regulatory Commission.

18.2-3 CNSC Regulatory Document REGDOC-2.2.5, "Minimum Staff Complement."

18.2-4 IAEA Safety Standards Series No. SSG-51, "Human Factors Engineering in the Design of Nuclear Power Plants," International Atomic Energy Association.

18.2-5 CNSC Regulatory Document REGDOC-2.5.1, "General Design Considerations: Human Factors."

18.2-6 CSA N290.12, "Human factors in design for nuclear power plants," CSA Group.

18.3 Design of the Human-System Interface

This section describes the process by which HSI designs are established and evaluated. The HSI design process for BWRX-300 is governed by a process methodology report 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 HSI design process sits within and 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 Chapter 3, particularly Subsection 3.1.7.

18.3.1 Design Goals and Design Bases

The primary goal of the HSI design process is to facilitate safe, efficient, and reliable user task performance during plant normal operational states, abnormal events, and accident conditions. To achieve this goal, HSIs throughout the plant are designed and implemented consistent with HFE core principles and user-centred design practices. The following specific design bases are adopted for the plant:

1. HSI design promotes efficient and reliable operation through application of automated operation capabilities.
2. HSI design uses only proven technology.
3. The workstation and HSI layouts reflect I&C separation restrictions.
4. HSI 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.
5. The principal functions of the Safety Parameter Display System (SPDS) as required by CNSC REGDOC-2.5.2, "Design of Reactor Facilities: Nuclear Power Plants" (Reference 18.3-1) are integrated into the HSI design.

   NOTE: Historically, the SPDS has provided an overview display of important plant parameters during transients and accidents on a separate panel with separate safety categorization due to the safety analysis outcomes for full-scale plants. The SPDS terminology is used in this PSAR for consistency with regulatory documents. However, 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 Subsection 18.3.5). There is no separate panel or system.

6. Accepted HFE principles and methods are used for ensuring HFE is integrated into the design, in alignment with international best practice and meeting the requirements of CNSC REGDOC-2.5.1, (Reference 18.3-2).
7. HFE design requirements are based on international standards and applicable CNSC regulatory requirements, as outlined in the HFEPP.
8. The design basis for accident and emergency control and monitoring facilities meets international standards as well as CNSC REGDOC-2.5.2 (Reference 18.3-1), and CNSC REGDOC-2.10.1, "Nuclear Emergency Preparedness and Response" (Reference 18.3-3).

Task performance criteria developed through the HFE Program analysis activities, in conjunction with those described in Chapter 3, Section 3.1 and Chapter 15, Subsections 15.3.2 and 15.3.3

are used to govern and direct HSI design specifications. These detailed task performance criteria, along with requirements specified in HFE standards and codes, encompass the set of necessary and sufficient design requirements that maintains the implemented plant SSC and HSIs in compliance with accepted HFE principles.

18.3.2 Human-System Interface: Design Inputs

The inputs to the HSI design are derived from several sources. These include specific information relating to the performance of tasks, as well as design requirements and guidance specific to the plant design and a defined full set of plant user characteristics, but not related to task performance. In addition to these documented input sources, the integrated set of HFE Program activities includes HF Engineer/HFE Specialist 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. Finally, HSI design updates are 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.

18.3.2.1 Task-Related Input

A primary input to HSI development is the user task information and control needs established during TA (see Subsection 18.2.4). TA provides the following information that forms the HSI 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
- Information for determining when tasks may be terminated
- System and component alarms
- Information on task performance requirements for group-use and aggregate HSIs
- Information regarding where manual tasks need to be performed (remote or local)

18.3.2.2 Design Requirements and Guidance Input

The second main input to HSI design is the full set of HFE design requirements derived from international codes, standards, regulations, and best-practice guidance, that are applicable to the defined user group characteristics and the types of HSIs 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 provides an extract from the requirements management database, providing a single repository of these common requirements (i.e., applicable to all SSC).

For the design of HSIs, the requirements in the HFE Design Requirements Document 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 layout and create screen artefacts, for example, variations in colour, size, font, and placement. Further inputs are required that ensure consistent and intuitive HSI designs across the plant. The requirements for this part of the HSI design process are defined in the project HSI Style Guide.

For digital software-driven HSIs, the style conventions are further developed into an HSI Element Library, which contains HSI display templates and HSI elements (e.g., symbols, numerical displays, graphs) that the display designer uses to assemble the display content. The HSI

Element Library contains both HSI elements for primary interfaces (those that represent direct interface to the system and plant HSI) as well as secondary interfaces (such as navigation, which do not directly relate to system equipment).

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

18.3.2.3 Human Factors Engineering Concept of Operations

The HSI concept design scope includes development of the HFE Concept of Operations (COO) which defines the physical and cognitive characteristics of the standardized plant full user population. The HFE COO 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. 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).

18.3.2.4 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. The integration of the HFE team with the other disciplines provides the mechanism for designers to request HF Engineer/HFE Specialist support for instances where is not clear, for the HSI 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, they need HF Engineer/HFE Specialist advice on the most suitable alternative design solutions.

18.3.2.5 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 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 HSI design improvement form the inputs to further design development.

18.3.3 Human-System Interface: Detailed Design and Integration

In accordance with the HFEPP and the HSI design methodology, HSI designs are created through the interaction and coordination of the HFE team and discipline engineers. Degree and type of interaction is based on the risk-based HFE Application Level as described in Subsection 18.1.4.2.

18.3.3.1 Objectives and Scope

The objectives of the HSI design process are to:

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

2. Support the principal objectives of the HSI design to provide the indications, 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 HSI design activities through the systematic application of HFE principles and criteria, and with HF Engineer/HFE Specialist support

4. Maximize the plant capacity factor in the HSI design by:
   a. Facilitating planned operations, maintenance, inspection, and testing
   b. Minimizing the occurrence of any undesired power reduction or plant trip caused by erroneous decision-making and actions
   c. Permitting plant commissioning to take place effectively and allowing timely modifications and maintenance of the HSIs

The scope of the HSI design process is to specify requirements for HSIs throughout the plant. For hardware-based HSIs, the HFE team supports other discipline designers in designing and selecting HSIs. In the case of software-based HSIs, developing the optimized displays are HFE team responsibility. As with all other HFE Program activities, the scope and methods used for HSI design are graded based on HFE Application Level (Subsection 18.1.4.2). The HFEPP details the level of effort and scope for HSI design per HFE Application Level.

18.3.3.2 Methodology

The HSI 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 18.3.2).

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

1. Provides design requirement-compliant, application-specific wireframes, and templates for HSI displays, panel layouts, and HSI 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 Design Requirements Document) that apply to the discipline and system, allowing them to design or specify and select compliant SSC or HSIs and to develop compliant system and equipment layouts
3. Depending on HFE Application Level, reviews, tests, and verifies all HSI 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

Depending on the HSI type and the HFE Application Level, the same process is followed but the primary and secondary designers/engineers may vary.

The HFE Program HSI Design technical element includes roll-out of the HFE requirements and support to their implementation for other disciplines. For hardware HSIs, including plant layout and physical environment, direct physical SSC interfaces and HSIs that form part of COTS or bespoke design systems and equipment, the responsible discipline engineer includes the applicable task-based and HFE Design Requirements Document requirements as part of their system and component level design requirements. The applicable HFE requirements are included in “lower” level system and component requirements specifications, including procurement specifications, ensuring consistency of application throughout the plant design. This is 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.

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

The DCT lists the I/O points associated with a HSI element on a display or panel and provides a mapping of instrumented parameters and controlled components to individual HSIs 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 HSI display and panel layouts, including the components and parameters to be included on the HSI 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. The UIS standard deliverable consists of:

- HSI Task Support Inventory
- HSI Task Support Inventory – Key Parameters
- DCT
- HSI display screenshot

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

The HSI design process also includes development of an Alarm Management Design Guide during the concept design stage. The guide provides detailed alarm system and alarm presentation guidance, including outlining the principles for alarm identification, prioritization, filtering, and suppression, in line with human cognitive capacity and required response.

For HSI design, applicable requirements are applied to the developing design, and compliance is documented and maintained by the relevant engineering discipline. Where exception to a requirement is needed, HFE provides design support to the other disciplines to develop and document an HFE-approved justification for an HFE design requirement exception.

The HFE design requirements apply equally to the HSIs of COTS equipment and components. Ability of COTS equipment and component HSIs to meet the HFE design requirements is one of the standard selection criteria. However, it is recognized that not all COTS items require the same level of rigour; standard items that do not include HFE as part of their specification require HFE evaluation for non-compliance with the HFE design requirements. When evaluating COTS products that do not comply with HFE design requirements, special considerations are 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 HSI 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 HSIs
5. Identification of usability or human performance concerns with the proposed application of the COTS product

To accommodate these evaluations, where COTS products are considered, this is determined as early as possible in the design lifecycle, following completion of the HFE COO and other HSI design input documents as soon as the relevant System Engineer specifies that such products will be used.

The individual system and integrated plant-level UISs, hardware-based HSI designs and COTS HSIs, and the plant-level HFE requirements (e.g., those related to workspace layout and working environment), are also integrated into relevant control facility HFE design specifications. The design process for the MCR and SCR are described in Subsections 18.3.5 and 18.3.6; the design for other control facilities, including those for responding to accidents and emergencies follows a similar process, with graded level of effort based on complexity of the HSIs. The facilities for supporting emergency and accident response are in early concept design as described in Chapter 7, Section 7.7 and Chapter 19, Section 19.2.

18.3.3.3 Results

The process and the rationale for the HSI design are documented and managed under GEH Quality Assurance and BWRX-300 specific design plans, as described in Chapter 17. The HSI design process uses the following templates within the TA and HSI Design workbook to create the UIS:

- HSI Task Support Inventory
- HSI Task Support Inventory Key Parameters
- DCT

The specific controls, indications, displays, panels, and HSI elements designed to support the user tasks are documented in the HSI Task Support Inventory table. Data in the table documents that the designer confirmed that the HSI 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.

In addition to the templates, a screenshot of the resulting HSI display is included in the workbook. The HSI design for displays performed by the HFE team also results in the HSI display software file.

To support the standard plant alarm system logic implementation, a detailed alarm presentation specification is produced in line with the Alarm Management Design Guide. The specification includes rationalization and prioritization evaluation results, providing alarm filtering and presentation requirements as input to the I&C team alarm system design activities.

Other outputs include the design documentation (system design specifications, system and component requirements documents, purchase specifications, and drawings and models), as appropriate to the discipline and HSI type being designed. The results of any non-compliance evaluations and design trade-off decisions are recorded in design records and (where appropriate) the HFEITS (Subsection 18.1.5).

18.3.4 Human-System Interface: Tests and Evaluations

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.

18.3.4.1 Objectives and Scope

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 the 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 HSI prototypes and simulation testbeds
- Defining the HFE T&E team and participants
- Establishing HFE T&E methods
- Performing HSI selection and prioritization
- Performing HSI evaluation and user-based testing
- Collecting and analyzing 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 HSI, new systems, high HFE risk grading).

18.3.4.2 Methodology

To maximize the effectiveness of HFE T&E, HSIs are selected based on prioritization criteria. Primarily selection and prioritization of the HSIs are based on the HFE Application Level (Subsection 18.1.4.2). Where HSIs support more than one task, which means they may have more than one associated HFE Application Level, the worst-case (highest risk) level is used.

Beyond this grading, additional HSI are selected for HFE T&E inclusion based on consideration of any HSI 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 HSI.

Some examples of candidate HSI design assumptions include the following:

- Colours and status coding (short time to learning; medium impact if false)
- Hardware HSIs basis ergonomic check (short time to learning; high impact if false)
- Safety HSIs (long time to learning; high impact if false)
- HSIs 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 HSI design. Members of the test team observe the user's actions without intervening, recording what transpires. 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 HSI and actual user behaviour when using it, indicating potential human error traps in the design.

During design development, the performance-based testing may be formative in nature. This type of testing allows for quick low-fidelity prototyping and problem resolution. During formative testing the test administrator and user both participate in the test. The administrator may prompt for information on what and why a user is performing actions to understand the thought process as well as to understand better the prototype or conceptual design limitations.

At appropriate points in the detailed design, testing is done with a summative approach. During summative testing the test administrator does not participate to limit test bias. Several users are tested separately to allow assessment of error variances and statistical comparison of test results.

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. Design features selected for user testing, the test fidelity, user representatives chosen, testbed used, and performance measure(s) and acceptance criteria all depend on the maturity of the design at the stage of the testing.

Considerations for test design include:

1. Availability of plant modeling software and integrated HSI design status
2. Availability and fidelity of a mock-up
3. Availability of control area and equipment 3D modeling
4. Availability of procedures, procedure types, and training material
5. Availability of a sufficiently diverse participant population pool that is representative of the user population to the level required for the testing stage
6. Develop an observation and evaluation plan. The observation plan includes written test plans, scripts for observers and evaluators, standardized training for participants, and the same observers or proctors for all runs of an evaluation (whenever possible).

Once the test plan is complete and the testbed selected or designed, the T&E team develop an observation and evaluation plan. The observation plan includes written test plans, scripts for observers and evaluators, standardized training for participants, and the same observers or proctors for all runs of an evaluation whenever possible.

The test is then conducted in accordance with the plans.

The HFE T&E program uses a variety of methods and tools for analyses, reviews, and evaluations of the HFE T&E performed throughout the design process.

Data collection methods are selected appropriate to the type of test or evaluation being conducted, as detailed in the T&E plan. Techniques appropriate for the evaluation of HSI include:

- Participant questionnaires and interviews
- Direct observation of user behaviours (e.g., task time, task errors, HSI interaction or navigation errors)
- Simulation instructor console data

The following criteria are used to select the data collection methods:

- Safety and risk significance
- Type of design (depending on the type of design, there are some methods that may not apply)
- Type of technology
- Relative time to perform the test or evaluation
- Relative complexity
- Relative cost and value

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 – HFE, other discipline engineering experts, HSI 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 HSI design alternative trade-off decision. If there are several closely ranking alternatives, further HFE review or analysis is undertaken to determine. HFE issues resulting from this evaluation are recorded and tracked using the HFEITS. Those that are not resolved at the time include the necessary information to address them in future project stages.

18.3.4.3 Results

The results from any HFE T&E are documented in design records and on associated test forms design to support the T&E process. Any issues and recommendations resulting from the HFE T&E activities related to design improvement are communicated directly to the applicable HSI designer, used as input to further design development (as per Subsection 18.3.2.5). When the T&E for each design stage is complete, a T&E summary report is prepared that summarizes all T&E activities and their results).

18.3.5 Human-System Interface: Design of the Main Control Room

The current concept of the MCR is described in Chapter 7, Section 7.5. The MCR design features are based upon proven technologies and are demonstrated, through broad scope control room dynamic simulation during HFE T&E and V&V, to satisfy the HSI design goals and design bases. Validation of the implemented MCR design includes 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 HSI design implementation activities include support to the development of dynamic models for evaluating the overall plant response as well as individual control systems, including operator actions. These dynamic models are used to:

- Analyze both steady state and transient behaviours
- Confirm the design of the advanced alarm system concepts
- Confirm the adequacy of control schemes
- Confirm the allocation of control to a system or an operator
- Develop and validate system and plant-level operating procedures

Using part-task simulation, system models are developed, and linked to the HFE-designed the HSI displays. The part-task simulator is used in preliminary plant design and includes design features specific to BWRX-300.

As the design progresses, the part-task simulator proceeds through a series of iterative evaluations resulting in the development of a full-scope simulator. As soon as available, simulators are the preferred testbed for T&E, allowing for progression from static to dynamic testing.

Safety margins used in the DSA account for uncertainty and provide an added margin to ensure that the various limits or criteria important to safety are not challenged. Suitable margin is also added to the HFE analysis of human actions (during TA and human error analysis, per Subsections 18.2.4 and 18.2.6) by ensuring suitable conservatism is included in things like the timeline analysis or the generation of human error probabilities.

Design goals and design bases for the design of HSIs in the MCR and SCR and in other applicable facilities are established in Subsection 18.3.1, based on the HFEPP.

18.3.5.1 Objectives and Scope

The primary goal of HSI design and 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. To achieve this goal, information displays, controls and other interface devices in the control rooms and other plant areas are designed and implemented in a manner consistent with best HFE practices. Further, the following specific design bases are adopted:

1. HSI design promotes efficient and reliable operation through application of automated operation capabilities.
2. HSI design uses only proven technology.
3. Safety-related systems monitoring, and control capability is provided in full compliance with regulations regarding divisional separation, and independence.
4. HSI design is highly reliable and provides functional redundancy such that sufficient displays and controls are available in the MCR, or as a backup, in the SCR and remote locations to conduct a reactor shutdown and to ensure the reactor achieves and maintains safe shutdown conditions, even during postulated accidents.
5. The MCR remains habitable and protected for all events and accidents during which it is required to be used (habitability of the MCR is described in Chapter 6).
6. The principal functions of the SPDS as required by CNSC REGDOC-2.5.2 (Reference 18.3-1) are integrated into the HSI design.
7. Accepted HFE principles and methods are used for integrating HFE into the MCR design. in accordance with international best practice and meeting the requirements of CNSC REGDOC-2.5.1 (Reference 18.3-2).
8. HFE design requirements are based on international standards and applicable CNSC regulatory requirements, as outlined in the HFEPP.
9. The principal functions of the SPDS as required by CNSC REGDOC-2.5.2 (Reference 18.3-1) are integrated into the HSI design.
10. The design basis for accident and emergency control and monitoring facilities meets international standards as well as CNSC REGDOC-2.5.2 (Reference 18.3-1), and CNSC REGDOC-2.10.1 (Reference 18.3-3).

The evaluation of the integrated MCR design provides confirmation that the MCR HSIs and other design features are compliant with the HFE Design Requirements Document and any analysis-based design requirements. Refer to Chapter 7 for description of I&C system content and to Chapter 13 for the Conduct of Operations.

18.3.5.2 Methodology

The MCR concept outlined in Chapter 7 contains a group of workspaces and individual HSIs, which form the foundation for the detailed HSI design. The development of the MCR workspaces and HSI design features is accomplished through:

- Consideration of existing control room OE
- Review of trends in control room designs and existing control room data presentation methods
- Evaluation of modern HSI technologies, including alarm system design, particularly alarm reduction and presentation methods
- Application of relevant compiled requirements from the HFE Design Requirements Document
- Design or specification and selection of individual HSIs
- 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 are specified as part of the TA (Subsection 18.2.4) and qualitative human error analysis (Subsection 18.2.6). These criteria are used to govern and direct all plant control room designs. These detailed task performance criteria, along with requirements specified in HFE standards and codes, 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 HSIs 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 full-scope simulator is evaluated under normal and abnormal reactor operating conditions by participants suitably representative of the defined user population, as described in the HFE T&E process in Subsection 18.3.4. Following the completion of the HFE T&E and V&V on the full-scope simulator, the MCR workspace, and HSI design features are finalized.

18.3.5.3 Results

The results from design MCR design activities are the same as those for the overarching HSI design process as described in Subsection 18.3.3.3. This includes the outputs from the related HFE T&E and V&V activities, and identification and tracking of design-related HFE issues and HEDs.

18.3.6 Human-System Interface: Design of the Secondary Control Room

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 HSIs for the plant systems needed to bring the plant to hot shutdown, with the subsequent capability to attain safe shutdown, if the MCR becomes uninhabitable. The SCR is in early concept at the time of issuing this PSAR. The current concept is described in Chapter 7, Section 7.6. Habitability of the SCR and protection of the route between the MCR and SCR is described in Chapter 6, Section 6.4.

18.3.6.1 Objectives and Scope

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 HSIs for the plant systems needed to bring the plant to hot shutdown, with the subsequent capability to attain safe shutdown, if the MCR becomes uninhabitable. The SCR is in early concept at the time of issuing this PSAR. The current concept is described in Chapter 7, Section 7.6. Habitability of the SCR and protection of the route between the MCR and SCR is described in Chapter 6.

18.3.6.2 Methodology

The methodology for design of the SCR is the same as that for the MCR (Subsection 18.3.5.2) and more generally for HSI design (Subsection 18.3.3.2). As with all HFE Program activities, a proportionate, graded approach is taken to the design of the SCR. Due to the nature and purpose of the SCR and the plant conditions expected when it needs to be used, the human actions are by default important to safety and if incorrectly performed, lead to significant consequences and as such receive the highest HFE Application Level.

18.3.6.3 Results

The results are captured in the same means as for the MCR design (Subsection 18.3.5.3).

18.3.7 Procedure Development

Procedure development for the BWRX-300 is performed by the HFE team in accordance with a plan that details the inputs, method, and scope of procedure development activities.

18.3.7.1 Objectives and Scope

The objective of procedure development is to apply HFE principles and guidance to the development of procedures such that they are technically accurate, comprehensive, explicit, easy to use, and validated. The process for procedure development follows applicable requirements from IAEA-TECDOC-1058, “Good Practices with Respect to the Development and Use of Nuclear Power Plant Procedures” (Reference 18.3-4).

The plant procedures are developed as an integral part of the HSI design development. The procedures are developed either as new or modified from predecessor plants. Existing procedures are modified to reflect the characteristics and functions of the plant task types, modes and conditions, and any applicable OE related to procedure design.

The HFE Program includes activities to verify that all functions and tasks assigned to the plant personnel are included in the procedures. The HFE V&V activities include validation of the procedures using the mock-ups, part-task, and full-scope simulators to confirm their usability and accuracy. Procedure development is iterative and progressive, in line with the developing design and results from progressive HFE analyses.

The scope of procedure development addresses all tasks required to meet functional goals in operations, maintenance, inspection, testing, and accident management of the plant. The scope includes development of:

- Procedures Writer’s Guides
- Plant and System Operations Procedures (start-up, normal (at power operations), and shutdown)

- Maintenance, Inspection, Testing and Surveillance Procedures (including Refuelling and Outage Planning Procedures)
- Alarm Response Procedures
- Abnormal Operating Procedures
- Emergency Procedure Guidelines for Emergency Operating Procedures (EOP) development
- (EOPs)
- Severe Accident Management Guidelines
- Emergency Mitigating Equipment Guidelines

The procedure development process does not include specific requirements for the development or procurement and implementation of a Computer-Based Procedures (CBPs) platform or tool. However, the Procedure Writer's Guide specifies basic HFE requirements for usability of the CBP interface (the same as any other user interface) and the development of the content and format for any CBP inputs follows the same requirements for each procedure type given in the above list.

18.3.7.2 Methodology

The procedures development methodology establishes the process for developing technical procedures that are complete, accurate, consistent, and easy to understand and follow.

For each procedure type, a Procedure Writer's Guide is established. The Procedure Writer's Guide establishes objective criteria so that the procedures developed with it are consistent in organization, style, and content. The Procedure Writer's Guide provides instructions for procedure content and format, writing of steps, and specifying lists of terms used.

Procedures are then written after the associated TAs are finished. TA is an iterative process due to the amount of information that is created at any point in the design process. TA is conducted in a prioritized manner and done on a per task, per system basis. System Design Descriptions are used along with the TA output to give a complete understanding of the system and its operation. These inputs provide understanding of each system, its associated tasks, and its interrelationship to other systems, which allows the development of system level and then integrated operations procedures.

As the TA progresses beyond operations, when the System Engineers have defined test, inspection, and maintenance requirements and the iterative safety analyses have sufficiently matured, procedures are developed for other than normal operations (e.g., test, maintenance, surveillance, alarm response, outages and any other conditions that are not included in the scope of normal plant operations). Procedures that support important human actions for the higher HFE Application Levels are developed by the HFE team based on the detailed TA and qualitative human error analysis. Procedures to support human actions for the lowest HFE Application Level are developed by the responsible System Engineer or the vendor, based on the Basic TA (Subsection 18.2.4).

Initial procedures are tested and evaluated for their usability and efficacy using physical mock-ups, simulation, and plant 3D models early in the design, through the HFE T&E activities. The HSI design and procedures are evaluated together to make a more cohesive model of the future operational plant. This provides contextual feedback for both the HSI design and the procedure, allowing optimization of the design of both simultaneously.

The developed procedures are verified and validated as part of the HFE V&V program (Section 18.4), culminating in ISV. Procedures that support important human actions for the higher HFE Application Levels are validated by individuals that are independent of the design. Individuals that participate in validation of these levels of procedures include representatives of the end users. Final procedure validation is done on the installed physical plant hardware as part of the HFE design implementation once the plant has been built. Procedures to support human actions for the lowest HFE Application Level are validated by the designer.

The final procedure validations are done as specified by the plant pre-operational testing and start-up testing programs. Following ISV, the procedures are used as the basis for pre-operational testing, start-up testing, and operation of the plant. Once a procedure is validated and declared complete, procedure maintenance and control of updates is governed by the engineering change management process ensuring that changes to individual procedures are reflected throughout the full suite of related procedures, and that changes are confirmed as accurate and supported by the design and TA. Validated procedures are provided to operations for training and use.

18.3.7.3 Results

The results of the procedure development process are the final set of procedures and any procedure support documentation developed using the procedure development methodology.

The output documents include the following:

- Procedure Writer's Guides
- Plant and system operations procedures
- Maintenance, Inspection, Testing and Surveillance Procedures (including Refuelling and Outage Planning Procedures)
- Alarm Response Procedures
- Abnormal Operating Procedures
- EPGs
- EOPs
- Severe Accident Management Guidelines
- Emergency Mitigating Equipment Guidelines

18.3.8 Training and Qualification Program Development

Training and qualification program development is coordinated with the other elements of the HFE Program, for example by using HFE TAs to conduct a systematic analysis of job and task requirements. The program of analysis and training material development is conducted by the Training team, in accordance with a plan that provides the methods and framework for ensuring the program meets its requirements and technical basis. The HFE team provide inputs to the training analysis activities and provide support to the Training team in conducting the training program development activities.

18.3.8.1 Objectives and Scope

The aim of the BWRX-300 training and qualification program development is to systematically incorporate information from the other HFE design tasks to support development of accurate and applicable training content and implementation of effective personnel training. The training program development process is intended to produce a program that:

- Identifies all performance requirements of a job or duty area relating to licenced activities
- Defines and documents the training based on a TA that provides the information to establish the knowledge, skills, and abilities to perform each task including identifying the safety-related attributes if any
- Ensures that the training is designed, developed, and implemented to meet the qualification requirements
- Ensures instructors meet and maintain documented qualification requirements, particularly in areas of subject matter expertise and instructional skills
- Ensures that formal evaluation methods are used to confirm and document workers qualifications
- Implements a change management control system that systematically identifies changes to tasks and task lists for revisions of training
- Ensures continuing training is provided as deemed necessary through training needs analysis
- Evaluates training regularly and incorporate the results of the evaluation into a training improvement process
- Ensures that workers training and qualifications records are established and maintained
- Ensures that workers have a level of training related to nuclear safety corresponding to their position including but not limited to radiation safety, fire safety, onsite emergency training, and conventional health and safety

The training and qualification program development includes the following stages:

- Analysis
- Design
- Development
- Implementation
- Evaluation

The overall scope of the resulting training and qualification program includes the following:

1. All categories of personnel conducting tasks within the plant, including the full range of job roles whose actions may affect plant safety
2. The full range of plant conditions (normal operational, outage, abnormal, accident, and emergency)
3. All activities conducted throughout the plant (e.g., operations, radwaste processing, outage refuelling, online and offline maintenance, testing, and inspection)
4. The full range of plant functions and systems
5. The full range of relevant HSIs

The scope of the training and qualification program development plan does not include the specific requirements for certification of plant personnel specified in CNSC REGDOC-2.2.3, “Personnel Certification, Volume III: Certification of Reactor Facility Workers” (Reference 18.3-5). The requirements for certification are incorporated as part of the overall program; however, they do not need to be derived through the defined development process, since they are already specifically defined. The final training and qualification program specific to the operational goals of the plant and developed from the HFE and design inputs, as described in this section, are augmented by the general and specific training and certification requirements specified in CNSC REGDOC-2.2.3, Volume III (Reference 18.3-5).

18.3.8.2 Methodology

The training and qualification program development follows the fundamentals of the systematic approach to training method. The development process complies with the requirements of CNSC REGDOC-2.2.2, “Personnel Training” (Reference 18.3-6).

The Analysis Stage provides the identification of training needs, tasks, or competencies required for training and the knowledge, skills, and abilities required to perform a specified job position based on assigned tasks. Tasks that support plant functions are identified as part of Detailed and Basic TA, described in Subsection 18.2.4. Tasks are selected for training based on difficulty, importance, and frequency analysis. Depending on the difficulty, importance, and frequency ranking, a decision is made to determine if initial training and periodic retraining is needed. This evaluation of training tasks is the training equivalent to grading human actions (Subsection 18.1.4.2). The results of the TA, including identification of critical steps, inform the difficulty, importance, and frequency analysis and resulting rankings.

Depending on the difficulty, importance, and frequency ranking, a determination is made if initial and periodic retraining is required. Tasks that are selected for training are then analyzed to determine the required knowledge, skills, and attributes. The knowledge, skills, and abilities necessary for each job position, including entry-level education, training, and experience, is established to support training design. Any changes to the iterative HFE or system design inputs to the analysis phase are required to be assessed for impact on the training analysis.

During the Design Stage, learning objectives are developed and a description of the plan for training, including purposed methods and settings, is established. Specifically, the Design Stage includes the following activities:

- Determine the scope, purpose, and timeframe of the training
- Determine the ideal training environment
- Select training methods and instructional strategies in accordance with the environment
- Determine and group the job role knowledge, skill, and attributes addressed by each training module
- Determine the final and partial learning objectives for each training module, including defining performance statements, conditions statements and performance standards
- Prepare the table of contents and scope for each training module; scope includes number and type of documents developed in the next phase
- Prepare master training procedures and formats to ensure consistency across the course materials
- Prepare the training plans for each job position; plans comprise learning objectives, contents, learning activities, training equipment, and a list of materials needed for training, including guidance for their use

The completion of the Design Stage establishes the input that is needed for the Development Stage.

In the Development Stage, detailed lesson plans and instructional materials are created, including any on-the-job training documents, and knowledge and performance assessment tests are established. The materials developed must incorporate the required features specified in the Design Stage. The materials are developed such that they have the following attributes:

- Course material content supports mastery of the subject learning objectives.
- Course materials are structured to provide consistent presentation.
- Course material presentation sequence supports effective learning.
- Course materials support successful presentation in the specified venue(s) the course is to be provided.
- Instructor certifications and training required to present training is specified for each course and supports successful presentation in the required venue. Instructors are trained during this phase.
- Exam question banks and examination structure and content are developed to adequately evaluate, and document trainee mastery of the course and job performance objectives associated with the training.

At the end of the Development Stage, the training package is reviewed, piloted on trainees, and revised if necessary.

In the Implementation Stage, instructors prepare for and deliver the training. Trainees are tested to determine if they have mastered the objectives. The results of trainee tests are examined during the Evaluation Stage. The Evaluation Stage examines the effectiveness of the training as delivered. This appraisal is done through the review of training results, training feedback, and continual monitoring of work performance (Section 18.6).

The training and qualification program, developed as discussed above, provides assurance that plant personnel have the capability and competence needed to perform their roles and responsibilities. Participants used for ISV, as described in Section 18.5, are trained using this program and provide validation of the integrated design.

18.3.8.3 Results

The specific program outputs include documentation defining the overall program goals and course structure, as well as the specific job role qualification and training requirements and developed course materials. In addition to the training program content itself, the results of the training and qualification program development are summarized in a report which documents the process and activities used in development, including any inputs used, issues identified, and recommendations made.

18.3.9 References

18.3-1 CNSC Regulatory Document REGDOC-2.5.2, “Design of Reactor Facilities: Nuclear Power Plants.”

18.3-2 CNSC Regulatory Document REGDOC-2.5.1, “General Design Considerations: Human Factors.”

18.3-3 CNSC Regulatory Document REGDOC-2.10.1, “Nuclear Emergency Preparedness and Response.”

18.3-4 IAEA-TECDOC-1058, “Good Practices with Respect to the Development and Use of Nuclear Power Plant Procedures,” International Atomic Energy Association.

18.3-5 CNSC Regulatory Document REGDOC-2.2.3 “Personnel Certification, Volume III: Certification of Reactor Facility Workers.”

18.3-6 CNSC Regulatory Document REGDOC-2.2.2, “Personnel Training.”

18.4 Human Factors Verification and Validation

HFE V&V is a critical HFE design assurance activity applied to the realized design of the plant HSIs and the working environment where those HSIs are used. The HFE V&V program evaluates the plant design (in parts and as an integrated whole) against HFE design principles and requirements, user task requirements, job design and staff complement, procedural accuracy and usability, and effectiveness of training.

18.4.1 Objectives and Scope

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

1. Task Support Verification (TSV) verifies that the HSIs, as defined and baselined in the HSI inventory and characterization, 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 HSIs 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 HSIs and other features due to competing design constraints, and checking for due consideration of OE items, user stakeholder input and HFE T&E results.

HFE Validation is 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 solve 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 HSIs and finalized 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 generalizable set of conditions to ensure that the integrated HSI 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 are applied to HSIs within scope of the HFE Program. As with the other HFE Program activities, the application of HFE V&V is graded to focus on the HSIs, 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 18.1.4.2 is applied to the HFE V&V activities to determine the appropriate scope, rigour, and level of detail for each activity.

18.4.2 Methodology

The HFE V&V program is conducted in accordance with a structured, systematic plan. The program was developed to meet the requirements and best-practice guidance specified in CNSC REGDOC-2.5.1, “General Design Considerations: Human Factors” (Reference 18.4-1), CNSC REGDOC-2.5.2, " Design of Reactor Facilities: Nuclear Power Plants” (Reference 18.4-2), CSA N290.12-14, “Human factors in design for nuclear power plants” (Reference 18.4-3), IEC 61771, “Nuclear power plants – Main Control Room – Verification and validation of design” (Reference 18.4-4), and IAEA SSG-51, “Human Factors Engineering in the Design of Nuclear Power Plants” (Reference 18.4-5). The program adopts a risk-based graded and multi-staged approach to V&V.

The V&V program plan specifies overall process used for HFE V&V, and the scope, inputs, methods, and outputs to be used for each V&V activity. The overall process is shown in Figure 18.4-1.

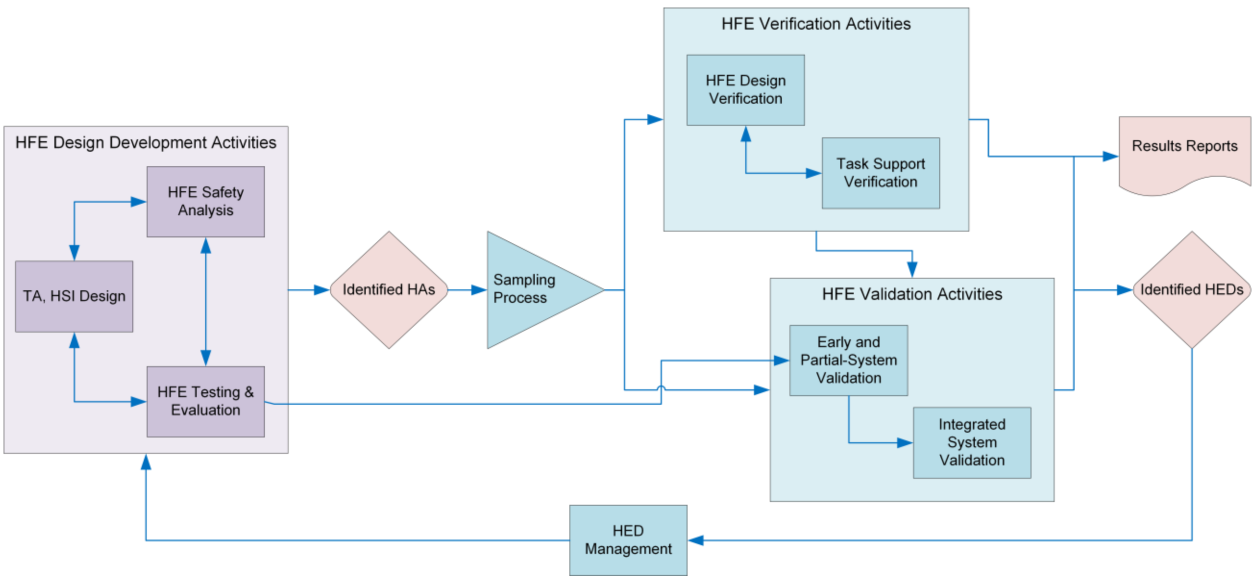

Figure 18.4-1: BWRX-300 HFE V&V Process Overview

The Sampling Process is a support activity that establishes the scope of the HFE V&V activities. In a new plant design, the number of scenarios and HSIs is too large to effectively perform HFE V&V to the same degree on all of them. The purpose of the Sampling Process is to focus on the significant, novel, and complex HSIs 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 Sampling Process selects the inputs that bound the scope of the HFE V&V activities. The verification activities target a selection of HSIs (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 maximize sample relevance and significance while ensuring that the sample is sufficiently broad and diverse, so that the HFE V&V results are generalizable to the overall population of HSIs and scenarios.

TSV compares the HSI elements (alarm, control, information and equivalent) identified during the detailed analysis of a task to the designed HSIs 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 TA (Subsection 18.2.4).

In HFE Design Verification, various aspects of HSI and plant SSC design are compared to the relevant design requirements specified during the design development (Subsections 18.3.1 through 18.3.6). The aspects verified include:

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

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

Early Validations form an essential part of the HFE Validation activities; they are 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 are expected to 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. Simulations and virtual reality models are used to validate the ability of personnel, trained using the training and qualification program material (Subsection 18.3.8), to use the integrated HSIs and finalized procedures such that they support safe plant functionality. ISV is intended to evaluate those integrated aspects that were verified separately through earlier, partial means (i.e., through HFE T&E, TSV, Early Validation). ISV is performed using high-fidelity simulators, task trainers or virtual reality labs (i.e., for scenarios outside of control rooms and control stations). The ISV is the final activity that ensures the integrated design is fulfilling its intended function and demonstrates that claims made in the safety analyses are achievable to the performance requirements specified.

The general method for conducting either early validations or ISV is:

1. Perform preliminary activities
    a. Scenario identification and development
    b. Testbed verification
2. Perform testing
    a. Participant selection
    b. Scenario definition and documentation
    c. Performance measures
    d. Test design
    e. Pilot testing
3. Perform data analysis and document results

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

18.4.3 Results

The results of all the HFE V&V activities are captured in the following indicative documents:

1. HFE Verification Results Report
2. HFE Early and Partial Validation Result Report(s)
3. HFE ISV Test Specification
4. HFE ISV Summary Report

Another output of the HFE V&V activities is identified HEDs, which are captured in the HFEITS and managed through the process described in Subsection 18.1.5.

18.4.4 References

18.4-1 CNSC Regulatory Document REGDOC-2.5.1, “General Design Considerations: Human Factors.”

18.4-2 CNSC Regulatory Document REGDOC-2.5.2, “Design of Reactor Facilities: Nuclear Power Plants.”

18.4-3 CSA N290.12, "Human factors in design for nuclear power plants," CSA Group.

18.4-4 IEC 61771, “Nuclear power plants – Main control room – Verification and Validation of Design,” International Electrotechnical Commission.

18.4-5 IAEA Safety Standards Series No. SSG-51, “Human Factors Engineering in the Design of Nuclear Power Plants,” International Atomic Energy Association.

18.5 Design Implementation

Design Implementation addresses the implementation of the HFE design requirements in the final realized design.

18.5.1 Objectives and Scope

The HFE Design Implementation activities have the following objectives:

1. Confirm that the final realized HSIs, plant SSC, procedures, and training conform to the design requirements and design documents resulting from the HFE Program activities
2. Identify any deviations from the design during implementation and assess their impact on the HFE aspects of the design
3. Perform final procedure validation on the physical plant hardware
4. Verify aspects of the design that may not have been evaluated previously in the V&V process, i.e., any HSIs that were absent or modified from the simulator-based ISV, or any plant physical or work environment (e.g., noise, lighting, thermal) characteristics; verification of items not previously identified as needing evaluation uses the same grading process as the original verification during the design stage
5. Verify and document the resolution of all remaining HFE issues and HEDs (Subsection 18.1.5)
6. Verify HFE Application Levels (Subsection 18.1.4.2) are correct based on the final version of documents and data used as input to determine the levels

The scope of the design implementation is the full set of HFE aspects of the plant including design of the HSIs and plant SSC, plant procedures, and finalized training documentation.

18.5.2 Methodology

Unlike the other HFE technical elements, Design Implementation is performed after the design is complete, immediately prior to commencement of commercial operations. Despite the plant being built and undergoing start-up testing and commissioning, the HFE team still performs the Design Implementation activities. The process follows the HFE V&V process. In this case, the Sampling Process includes identifying any changes to the standardized plant design (documented through engineering configuration control process) and assessing impact on HFE aspects of the design. The Sampling Process also identifies aspects of the design that were not able to be previously verified and validated. Additional items not previously identified for V&V but determined to require it are also added to the scope for Design Implementation HFE V&V.

The list of methods used are similar to those described for the HFE Program activities, particularly HFE V&V, Staffing Analysis, Procedure Development, Training and Qualification Program Development, and HFE Issues Tracking.

At this stage, the plant design is in formal engineering configuration control, as described in Chapter 17.

18.5.3 Results

The results of the Design Implementation activities match the outputs for the same activities conducted during the design phase. They are recorded in a summary report. Any remaining HFE issues or HEDs are recorded in the HFEITS for turnover to the plant operating organization, and further mitigation through operating arrangements as required.

18.6 Human Performance Monitoring

The HPM strategy links HFE methods used during the design with methods for monitoring user task performance during operation. The HPM program is fully developed by the licence applicant as part of the future licencing stage.

18.6.1 Objectives and Scope

The purposes of HPM are:

1. To ensure that the high safety standards established by the HFE Program during the design of the plant are maintained even when changes are made to the plant
2. To detect any deterioration of task performance that may be attributable to latent or slow-developing HFE design issues
3. To provide adequate assurance that the safety bases remain valid during the operational phase of the plant

There is no intent for the HSI designer or the applicant to periodically repeat a full set of ISV activities. The strategy is to provide a monitoring plan, building upon the HFE activities during the design that can be carried forward into the operational phase, using industry accepted methods. HPM incorporates the monitoring strategy into the problem identification and corrective action program, which identifies and classifies human errors, provide for evaluation of the root cause, and supports effectiveness verification and documentation of the corrective action.

The scope of the performance monitoring strategy provides reasonable assurance that:

1. The HSI design is effective during:
    a. Normal operations
    b. Maintenance, Inspection, Testing, and Surveillance
    c. Anticipated Operational Occurrences
    d. Design Basis Accidents
    e. Design Extension Conditions
    f. Severe Accidents
2. Human actions, using HSI information, cues and controls can accomplish tasks while maintaining margin for time and performance criteria.
3. Acceptable performance levels established during the HFE ISV are maintained.
4. Changes made to the initial HSIs, user group definition, job design, procedures, and training do not have adverse effects on personnel task performance (e.g., a change interferes with trained skills, or a fatigue management policy is not implemented, contrary to what was assumed in the HFE COO).

18.6.2 Methodology

The HPM program aligns with the overall quality program and condition reporting methods. The program includes:

- Data collection
- Importance screening
- Event analysis to determine causes

- Trend analysis
- Corrective action development

The HPM strategy collects data to trend task performance, particularly seeking issues with design root causes due to non-compliance with or inappropriate application of HFE principles. The HPM program uses existing utility or industry programs (e.g., corrective action, programs, or operator training) for data collection where appropriate. The HPM program is designed to ensure that:

1. Human actions are monitored commensurate with their safety importance.
2. Feedback of information and corrective actions are accomplished in a timely manner.
3. Degradation in performance is detected and corrected before plant safety is compromised.

NOTE: The HFE-based HPM does not seek personnel behaviour-based corrective actions. It is focused solely on issues related to the design of HSIs and organizational arrangements that lead to human error.

The HPM program maintains a database of event causes and corrective actions taken. Such data supports trending of performance anomalies.

The HPM identifies and establishes corrective actions that reduce the potential for incident recurrence. The program systematically identifies the cause of the failure or degraded performance. The corrective actions are derived by:

1. Addressing the significance of the failure through application of PRA/HRA importance measures
2. Classifying the causes and circumstances surrounding the failure or degraded human performance
3. Illuminating the characteristics of the failure (e.g., being task specific or due to design issues)
4. Determining whether the failure is isolated or has generic or common cause implications

18.6.3 Results

The HPM program activities and outputs align with the overall condition reporting requirements. They are expected to include specific incident or trend analysis reports, a recommendations and action tracking database, and periodic summary reports.