SOUTHERN COMPANY®

UFSAR Table of Contents

UFSAR Formatting Legend

Color	Description
	Original Westinghouse AP1000 DCD Revision 19 content (part of plant-specific DCD)
	Departures from AP1000 DCD Revision 19 content (part of plant-specific DCD)
	Standard FSAR content
	Site-specific FSAR content
	Linked cross-references (chapters, appendices, sections, subsections, tables, figures, and references)

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

TABLE OF CONTENTS (CONTINUED)

LIST OF TABLES

LIST OF FIGURES

Chapter 18 Human Factors Engineering

18.1 Overview

Human factors engineering deals with designing and implementing resources and environments that help people perform tasks more reliably. Traditionally, human factors engineering includes the consideration of:

- Anthropometric or physical fit of humans to either their task-assisting machines or to their surroundings (for example, height, reach, and visual limitations)

- Biomechanical fit of the physical capabilities and limitations of humans relative to the requirements of their tasks (for example, lifting limits and push-pull limits)

- Biophysical fit of the physiological capabilities and limitation of humans to their environment (for example, tolerance to heat or cold, harmful chemicals, and noise)

More recently, the human factors engineering discipline also models human error. Human errors include:

- Errors of execution or “slips”
- Errors of intention or “mistakes” (Reference 1)

Slips are errors in which a person’s intentions are correct, but an incorrect method for executing the action is chosen. Mistakes are errors in which the person forms an incorrect intention but then correctly executes it. Slips tend to be the result of poorly designed physical interfaces (for example, switches on a control board that look or feel alike) or of a poorly designed work environment (for example, temperatures that cause worker exhaustion). Mistakes are cognitive or mental errors. Human factors engineering includes cognitive systems engineering. This discipline focuses on the design of interfaces between humans and machines that support the operator decision-making activities that are required by the task. Cognitive systems engineering is particularly important when designing an interface for operators that control a real-time process, such as a nuclear power plant.

The rapid changes in digital computer and color graphics display technology offer the AP1000 design team an opportunity to improve the real-time decision support for the AP1000 operating staff. The AP1000 has a plant-wide network that provides pre-processed plant data to those members of the plant’s staff who have need of it. The real-time process control interface between the plant’s staff and the plant’s process equipment is the instrumentation and control (I&C) equipment driving graphical display devices in an integrated Human System Interface. Cognitive systems engineering is applied in the design of the human system interface.

The layout and environmental design of the main control room and the remote shutdown room, and the supplementary support areas, such as the technical support center, are sites of application of the traditional disciplines of human factors engineering.

Design input including decisions made in the design of the AP1000 that affect interfaces is provided. This includes input on the operating staff training program and on the development of the plant operating procedures.

Because of the rapid changes that are taking place in the digital computer and graphic display technology employed in a modern human system interface, design certification of the AP1000 focuses upon the process used to design and implement human system interfaces for the AP1000, rather than on the details of the implementation. As a result, this chapter describes the processes used to provide human factors engineering in the design of the AP1000.

This chapter describes the application of the human factors engineering disciplines to the design of the AP1000. [*The basis for the human factors engineering program is the human factors engineering process specified in Reference 2.*]* Figure 18.1-1 illustrates the elements of the human factors engineering program. These elements correspond to the elements specified in References 2, 10, and 11. The organization of this chapter parallels these elements. In addition to the elements of the program review model, this chapter includes a description of the minimum inventory of controls, displays, and alarms present in the main control room and at the remote shutdown workstation. The following provides an annotated outline of the chapter. A number of References are identified which were developed for the AP600 Design Certification. Since the AP1000 operating philosophy and approach are the same for AP600 and AP1000, the References identified below are applicable to AP1000.

Section 18.2, Human Factors Engineering Program Management—presents the AP1000 human factors engineering program plan that is used to develop, execute, oversee, and document the human factors engineering program. This program plan includes the composition of the human factors engineering design team.

Section 18.3, Operating Experience Review—and Reference 3 present the results of a review of applicable operating experience. This operating experience review identifies, analyzes, and addresses human factors engineering-related problems encountered in previous designs.

Section 18.4, Functional Requirements Analysis and Allocation—and Reference 4 present the results of the functional requirements analysis and function allocation process applied to the AP1000. The functional requirements analysis defines the plant's safety functions, decomposes each safety function, compares the safety functions and processes with currently operating Westinghouse pressurized water reactors, and provides the technical basis for those processes that have been modified. The function allocation documents the methodology used to arrive at the AP1000 level of automation for the plant functions, processes, and systems involved in maintaining plant safety, and documents the results and rationale for function allocation decisions.

Section 18.5, Task Analysis—presents the scope and implementation plan for task analysis. The task analysis provides one of the bases for the human system interface design; provides input to procedure development; provides input to staffing, training, and communications requirements of the plant; and ensures that human performance requirements do not exceed human capabilities.

Section 18.6, Staffing—and Reference 5 provide input from the designer for the determination of the staffing level of the operating crew in the AP1000 main control room.

Section 18.7, Integration of Human Reliability Analysis with Human Factors Engineering—and [*Reference 6 present the implementation plan for the integration of human reliability analysis with the human factors engineering program.*]*

Section 18.8, Human System Interface Design—presents the implementation plan for the design of the human system interface.

Section 18.9, Procedure Development—Reference 7 provides input for the development of plant operating procedures, including information on the AP1000 emergency response guidelines and emergency operating procedures.

Section 18.10, Training Program Development—Reference 8 provides input from the designer on the training of the operations personnel who participate as subjects in the human factors verification and validation.

*NRC Staff approval is required prior to implementing a change in this information.

Section 18.11, Human System Interface Verification and Validation Program— [*Reference 9 presents a programmatic level description of the human factors verification and validation.*]*

Section 18.12, Inventory—presents the minimum inventory of controls, displays, and alarms present in the main control room and at the remote shutdown workstation. The design basis and the selection criteria used to identify the minimum inventory are presented.

Section 18.13, Design Implementation—In accordance with Reference 2, this issue is addressed under Section 18.11 as "Issue Resolution Verification" and "Final Plant HFE Verification."

Section 18.14, Human Performance Monitoring—Human performance monitoring applies after the plant is placed in operation.

18.1.1 References

1. Reason, J. T., "Human Error," Cambridge, U.K., Cambridge University Press, 1990.

[2. *NUREG-0711, "Human Factors Engineering Program Review Model," U.S. NRC, July 1994.*]*

3. WCAP-14645, "Human Factors Engineering Operating Experience Review Report for the AP1000 Nuclear Power Plant," Revision 3.

4. WCAP-14644, "AP600/AP1000 Functional Requirements Analysis and Function Allocation," Revision 1.

5. WCAP-14694, "Designer's Input To Determination of the AP600 Main Control Room Staffing Level," Revision 0, July 1996.

[6. *WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan," Revision 2, May 1997.*]*

7. WCAP-14690, "Designer's Input To Procedure Development for the AP600," Revision 1, June 1997.

8. WCAP-14655, "Designer's Input to The Training of The Human Factors Engineering Verification and Validation Personnel," Revision 1, August 1996.

[9. *WCAP-15860, "Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan," Revision 2, October 2003.*]*

10. NUREG-0711, Revision 1, "Human Factors Engineering Program Review Model," May 2002.

11. NUREG-0711, Revision 2, "Human Factors Engineering Program Review Model," U.S. NRC, February 2004.

*NRC Staff approval is required prior to implementing a change in this information.

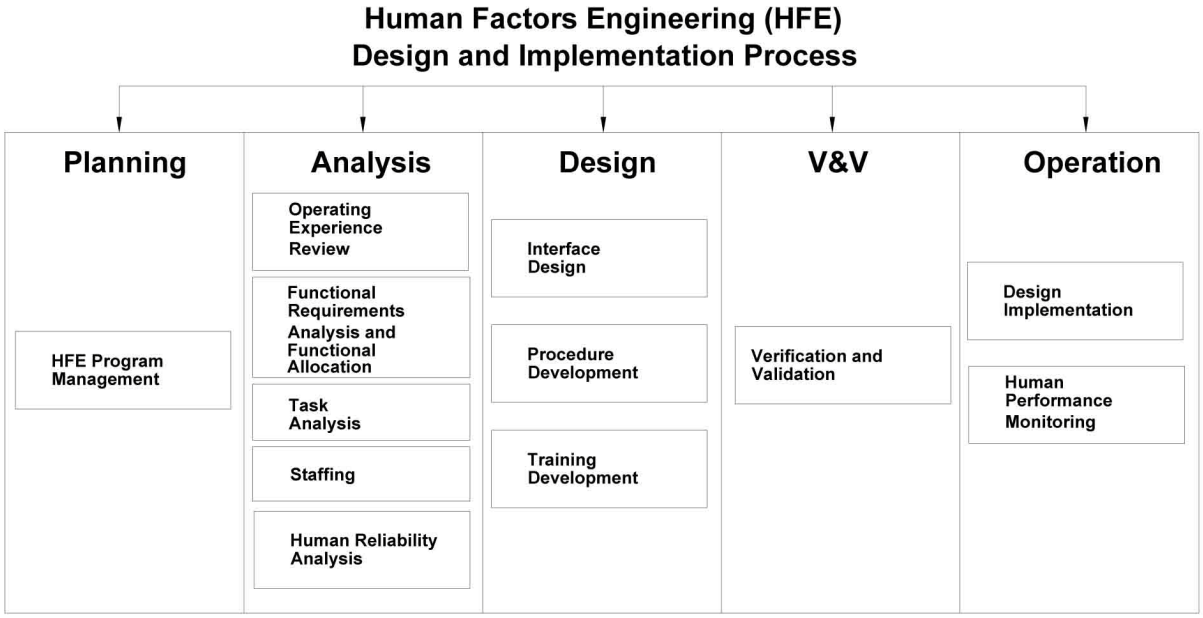


Figure 18.1-1
Human Factors Engineering (HFE)
Design and Implementation Process

18.2 Human Factors Engineering Program Management

The purpose of this section is to describe the goals of the AP1000 human factors engineering program, the technical program to accomplish these goals, the human system interface design team, and management and organizational structure that support the implementation of the technical program.

Human factors engineering is the system engineering of human system interfaces. The program management tools and procedures that govern the design of AP1000 systems apply to the human factors engineering activity. This approach integrates the design of human system interfaces with other plant systems.

18.2.1 Human Factors Engineering Program Goals, Scope, Assumptions, and Constraints

18.2.1.1 Human Factors Engineering Program Goals

The goal of the human factors engineering program is to provide the users of the plant operation and control centers effective means for acquiring and understanding plant data and executing actions to control the plant's processes and equipment.

The objective is to enable personnel tasks to be accomplished within time and performance criteria.

18.2.1.2 Assumptions and Constraints

There are a number of inputs to the human factors engineering design process that specify assumptions or constraints on the human factors engineering program and the human system interfaces design.

Major design inputs include regulatory guidelines, guidance from utilities and utility representative groups, utility requirements documents, and AP1000 plant systems design specifications. The requirements resulting from these design inputs are captured in human system interface specification documents and functional requirements documents.

While assumptions and constraints specified by design inputs are provisionally treated as design requirements, the appropriateness of these requirements is evaluated as part of the human factors engineering design process. Results of human factors engineering activities such as operating experience review, task analyses, mockup activities and verification and validation activities are used to provide feedback on the adequacy of initial human system interface design assumptions and constraints. If results of human factors engineering analyses or evaluations indicate that initial human system interface design assumptions or constraints are inadequate, then the human system interface design requirements are revised utilizing the standard AP1000 design configuration change control process.

Listed below are some of the major inputs to the AP1000 human system interface design and the assumptions and constraints they impose on the AP1000 human system interface design process and human system interfaces design.

Regulatory Requirements

One of the requirements for the AP1000 human factors engineering program is that it complies with applicable regulatory requirements. [*The human factors engineering process is designed to meet the human factors engineering design process requirements specified in NUREG-0711 (Reference 1).*]* This is also in accordance with References 7 and 10.

*NRC Staff approval is required prior to implementing a change in this information.

Utility Requirements

Another source of design input is utility customer requirements. Utility input can take the form of utility requirements documents, and/or input from utility representative groups serving in an advisory capacity.

Examples of utility requirements that impact the human system interface design are:

- **Operating staff assumptions.** A single reactor operator (RO) should be able to control major plant functions performed from the main control room during normal power operations.

- **Assumptions with respect to human system interface resources.** The human system interface design shall include an integrating overview display and mimic in the main control room.

The AP1000 design goals with respect to control room staffing are addressed in Section 18.6 and WCAP-14694 (Reference 3). As noted in WCAP-14694, a number of elements of the AP1000 human factors engineering design process are used to help achieve, verify and validate the control room staffing design goal. These include operating experience review, function analysis and allocation, task analysis, human reliability assessment, human system interface design, procedures, training, and human factors engineering verification and validation.

As described in Section 18.8, one of the human system interface resources is a wall panel information system. The wall panel information system is intended to meet the utility requirement for an integrating overview display and mimic in the main control room. A number of design activities establish the basis and functional requirements for the wall panel information system. Design activities include conducting operating experience reviews in nuclear power plants and related industries to examine the requirements for individual and group situation awareness and how these can best be supported.

Plant System Design Information

The design of the plant systems is an essential input to the human system interface design process. The physical implementation specifications as well as the systems designer's intent with regard to expected systems operation and performance are used as input to the design of the AP1000 human system interfaces. System design data are documented in the individual system specification documents. The input representing the plant's physical structure is represented by the piping and instrumentation drawings, general arrangement drawings, and equipment drawings.

System design specifications include specifications with respect to function allocation between automated systems and human operators. The system design specifications indicate which functions are to be automated, which are to be manual, and which require joint input of person and machine. In addition, the system design specifications indicate the set of instruments and controls that are implemented in the AP1000.

The AP600 function requirements analysis and function allocation document (Reference 4) provides information on the approach to initial function allocation and presents the results for AP600 safety functions. The results include a specification of level of automation and personnel responsibility for AP1000 safety functions, processes, and systems. The results also document the rationale for function allocation decisions for AP1000 safety functions.

The report also describes human factors activities that are conducted as part of the AP1000 human system interface design process to verify the adequacy of function allocation decisions, and establish the ability of operators to perform the role assigned to them. Function-based task analyses are used to verify that the sensors and controls that are provided are sufficient to enable operators to perform

the role assigned to them in system performance. Workload analyses are used to evaluate the adequacy of the integrated roles assigned to operators across systems. Integrated system validation is used to establish the adequacy of the function allocation using man-in-the-loop tests in dynamic simulated plant conditions.

Technology Limits

Recent advances in the technology of digital computing have made it possible and practical to change the performance and role of the human system interface in a process control application such as a nuclear power plant. For the AP1000, a position regarding the limits of the implementation technology to be assumed for the human system interfaces is derived from assessment of existing technology and anticipated advancements. An emphasis is placed on utilization of proven, reliable technology. The decision on the specific technology to be employed is made on a case-by-case basis after available technology alternatives are evaluated.

18.2.1.3 Applicable Facilities

[*Facilities included in the scope of the AP1000 human factors engineering program are the main control room (MCR), the technical support center (TSC), the remote shutdown room, the emergency operations facility (EOF), and local control stations.*]*

The EOF is designed as discussed in Subsection 18.2.6, including specification of a location, in accordance with the AP1000 human factors engineering program. Communication with the emergency operations facility is also as discussed in Subsection 18.2.6. Section 13.3 discusses the responsibility for emergency planning.

The EOF and TSC communications strategies, as well as the EOF and TSC Human Factors attributes, are described in the Emergency Plan. Subsection 9.5.2.2.5 provides additional information related to offsite interfaces.

18.2.1.4 Applicable Human System Interfaces

[*The scope of the human system interfaces encompasses the instrumentation and control systems which perform the monitoring, control, and protection functions associated with all modes of plant normal operation as well as off-normal, emergency, and accident conditions. Both the physical and the cognitive characteristics of those humans involved in the use, control, maintenance, test, inspection, and surveillance of plant systems are accommodated.*]*

18.2.1.5 Applicable Plant Personnel

[*The AP1000 human factors engineering program and the design of the human system interfaces includes the selection, synthesis, and distribution of process data to plant operations personnel as well as other plant personnel. These additional users include management, engineering, maintenance, health physics and chemistry personnel.*]*

18.2.1.6 Technical Basis

[*The human factors engineering program is performed in accordance with accepted industry standards, guidelines, and practices.*]* The references listed at the end of each Chapter 18 section and within any supporting documentation and reports are used to guide the human factors engineering program. [*The human factors engineering process specified in Reference 1 is used.*]* This is also in accordance with References 7 and 10.

*NRC Staff approval is required prior to implementing a change in this information.

18.2.2 Human System Interface Design Team and Organization

The human system interface design team is part of the AP1000 systems engineering function and has similar responsibility, authority, and accountability as the rest of the design disciplines. Figure 18.2-1 depicts the process used by the human system interface design team members. Figure 18.2-2 shows the organization of the human system interface design team and its relationship to the AP1000 design organization.

18.2.2.1 Responsibility

[*The mission of the human system interface design team is to develop the main control room and ancillary control facilities (such as remote shutdown workstation) that support plant personnel in the safe operation and maintenance of the plant. The human system interface design team is responsible for coordinating the human factors aspects associated with designing the structures, systems, and components that make up the main control room and ancillary control facilities.*

The human system interface design team is responsible for:

- *Development of human system interface plans and guidelines*
- *Oversight and review of human system interface design, development, test, and evaluation activities*
- *Initiation, recommendation, and provision of solutions for problems identified in the implementation of the human system interface activities*
- *Assurance that human system interface activities comply with the human system interface plans and guidelines*]*

18.2.2.2 Organizational Placement and Authority

The organization of the human system interface design team and its relation to the AP1000 design organization is depicted in Figure 18.2-2. The structure of the organization may change, but the functional nature of the human system interface design team is retained through the change. The human system interface design team consists of an instrumentation and control system manager, advisors/reviewers team, core human system interface design team, and human system interface technical lead. The technical disciplines described in Subsections 18.2.2.3 and 18.2.2.4 are organized by function within the core human system interface design team. The core human system interface design team and the advisors/reviewers team report to the instrumentation and control system manager. The human system interface technical lead works within the human system interface design function and reports to the instrumentation and control system manager through the manager of the human system interface design function. The instrumentation and control system manager is responsible for the design of the AP1000 instrumentation and control systems which include the human system interfaces. The instrumentation and control system manager reports to the AP1000 project manager.

The manager of the human system interface design function, who performs the function of technical project management for the human factors engineering design process, is responsible for the overall human system interface design and for integration of the human system interface design with the overall plant design. The advisors/reviewers team is responsible for overseeing the general progress of the human system interface design, providing guidance within the core human system interface design team, reviewing and providing comments on documents, specifications, and drawings pertaining to the human system interface design, and providing supplemental expertise in particular areas of design. The responsibility of the core human system interface design team is to produce the

*NRC Staff approval is required prior to implementing a change in this information.

detailed design of the human system interfaces. The human system interface design function is responsible for the functional design of the human system interfaces, main control room and workstation layout (ergonomics), controls, the information system (displays), the wall panel information system, the PMS safety displays, the alarm system, and computerized procedures system design and specification. The responsibilities of the human system interface technical lead include coordinating the technical work of the functional engineering groups, providing the administrative and technical interface between the functional engineering groups and the advisors/ reviewers team, and tracking the identification and resolution of human factors engineering design issues through operating experience review.

18.2.2.3 Composition

[*The human system interface design team consists of a multi-disciplinary technical staff. The team is under the leadership of an individual experienced in the management of the design and operation of process control facilities for complex technologies. The technical disciplines of the design team include:*

- *Technical project management*
- *Systems engineering*
- *Nuclear engineering*
- *Instrumentation and control (I&C) engineering*
- *Architect engineering*
- *Human factors engineering*
- *Plant operations*
- *Computer system engineering*
- *Plant procedure development*
- *Personnel training*
- *Systems safety engineering*
- *Maintainability/inspectability engineering*
- *Reliability/availability engineering*]*

The responsibilities of the individual technical disciplines include:

- Technical Project Management
  - Provide central point of contact for management of the human factors engineering design and implementation process
  - Develop and maintain schedule for human factors engineering design process
- Systems Engineering
  - Provide knowledge of the purpose, technical specifications, and operating characteristics of plant systems
  - Provide input to human factors engineering task analyses
  - Participate in development of procedures and scenarios for task analyses, and integrated system validation
- Nuclear Engineering
  - Provide knowledge of the processes involved in reactivity control and power generation

*NRC Staff approval is required prior to implementing a change in this information.

  - Provide input to human factors engineering task analyses
  - Participate in development of scenarios for task analyses, and integrated system validation

- Instrumentation and Control (I&C) Engineering
  - Provide knowledge of control and display hardware design, selection, functionality, and installation
  - Provide input to software quality assurance programs
  - Participate in the design, development, test, and evaluation of the human system interfaces

- Architect Engineering
  - Provide knowledge of plant component layout and the overall structure of the plant including design characteristics and performance requirements for the containment building, control room, remote shutdown room, and local control stations
  - Provide input to human factors engineering task analyses
  - Participate in development of scenarios for task analyses, and integrated system validation

- Human Factors Engineering
  - Provide knowledge of human performance capabilities and limitations, human factors design and evaluation practices, and human factors principles, guidelines, and standards
  - Develop and perform human factors analyses and participate in resolution of human factors problems

- Plant Operations
  - Provide knowledge of operational activities relevant to characterizing tasks and environment and development of human system interface components, procedures, and training programs
  - Participate in development of scenarios for task analyses, and integrated system validation

- Computer System Engineering
  - Provide knowledge of data processing required for human system interface displays and controls
  - Participate in design and selection of computer-based equipment
  - Participate in development of scenarios for task analyses, and integrated system validation, particularly those involving failures of the human system interface data processing systems

- Plant Procedure Development
  - Provide knowledge of operational tasks and procedure formats
  - Provide input for development of emergency operating procedures, computer-based procedures, and training systems
  - Participate in development of scenarios for task analyses, and integrated system validation
- Personnel Training
  - Develop content and format of personnel training programs
  - Participate in development of scenarios for task analyses, and integrated system validation
- Systems Safety Engineering
  - Identify safety concerns
  - Perform system safety hazard analysis such as thermal atmospheric analysis, toxicology analysis, and radiological analysis
- Maintainability/Inspectability Engineering
  - Provide knowledge of maintenance, inspection, and surveillance activities
  - Provide input in the areas of maintainability and inspectability
  - Support design, development, and evaluation of control room and other human system interface components
  - Participate in development of scenarios for task analyses, and integrated system validation
- Reliability/Availability Engineering
  - Provide knowledge of plant system and component reliability and availability and assessment methodologies
  - Provide input to design of human system interface equipment
  - Participate in development of scenarios for task analyses, and integrated system validation

18.2.2.4 Team Staffing Qualifications

In choosing the human system interface design team members, greater emphasis is placed on the individual's relevant experience to the specific discipline than on formal education. Alternative personal credentials may be selectively substituted for the education and experience requirements specified below. The professional experience of the human system interface design team as a collective whole satisfies the experience qualifications. The human system interface design team members have the following backgrounds:

- Technical Project Management
  - Bachelor’s degree
  - Five years experience in nuclear power plant design or operations and three years of management experience
- Systems Engineering
  - Bachelor of Science degree
  - Four years of cumulative experience of the following areas of systems engineering: design, development, integration, operation, and test and evaluation
- Nuclear Engineering
  - Bachelor of Science degree
  - Four years of experience in the following areas of nuclear engineering: design, development, test, or operations
- Instrumentation and Control (I&C) Engineering
  - Bachelor of Science degree
  - Four years of experience in hardware and software design aspects of process control systems; familiarity with software quality assurance and control
  - Experience in at least one of the following areas of instrumentation and control engineering: development, power plant operations, test evaluations
- Architect Engineering
  - Bachelor of Science degree
  - Four years experience in design of power plant structures and building services
- Human Factors Engineering
  - Bachelor’s degree in Human Factors Engineering, Engineering Psychology, or related science
  - Four years experience in the following areas of human factors engineering: human factors aspects of human system interfaces (design, development, and test and evaluation of human system interfaces for process control applications) and four years experience in human factors aspects of workplace design (design, development, and test and evaluation of workplaces)
- Plant Operations
  - Current or prior senior reactor operator (SRO) license/senior reactor operator instructor certification
  - Two years experience in PWR nuclear power plant operations

- Computer System Engineering
  - Bachelor's degree in Electrical Engineering or Computer Science or graduate degree in other engineering discipline
  - Four years experience in design of computer systems and real-time system applications; familiarity with software quality assurance and control
- Plant Procedure Development
  - Bachelor's degree
  - Four years experience in developing nuclear power plant operating procedures
- Personnel Training
  - Bachelor's degree
  - Four years experience in the development of personnel training programs for power plants and experience in the application of systematic training development methods
- Systems Safety Engineering
  - Bachelor of Science degree or Bachelor's degree in Science
  - Experience in system safety engineering, such as thermal atmospheric analysis, toxicology, radiological analysis and applicable OSHA limits
- Maintainability/Inspectability Engineering
  - Bachelor of Science degree or Bachelor's degree in Science
  - Four years of cumulative experience in at least two of the following areas of power plant maintainability and inspectability engineering activity: design, development, integration, test and evaluation, and analysis/resolution of maintenance problems.
- Reliability/Availability Engineering
  - Bachelor's degree
  - Four years of cumulative experience in at least two of the following areas of power plant reliability engineering activity: design, development, integration, and test and evaluation. Knowledge of computer-based, human system interfaces.

18.2.3 Human Factors Engineering Processes and Procedures

Activities performed relating to human factors engineering are performed in accordance with documented procedures under the quality assurance program for the AP1000. These procedures provide for control of processes as described below.

18.2.3.1 General Process and Procedures

The instrumentation and control system function is responsible for development of the AP1000 instrumentation and control (I&C), including human system interfaces, and coordinating and

integrating AP1000 instrumentation and control and human system interfaces with other AP1000 plant design activities. The overall operation of the project instrumentation and control systems function is defined. The function includes human system interface design of control rooms and control boards, instrumentation and control design, and control room/equipment design. The function includes definition of an engineering plan, review of inputs, production of system documentation, verification of work, procurement and manufacturing follow-up, and acceptance testing. An iterative feature is built into the process.

Documents produced as part of the instrumentation and control and human system interface design process include:

- Operating experience review documents
- Task analysis documents
- Functional requirements documents
- Human system interface design guidelines documents
- Design specification documents
- Instrumentation and control architecture diagrams
- Block diagrams
- Room layout diagrams
- Instrumentation lists
- System specification documents

The procedures governing instrumentation and control engineering work specify methods for verification of work. The types of verification include:

- Design verification by design reviews
- Design verification by independent review/alternative calculations
- Design verification by testing

System Specification Documents

System specification documents identify specific system design requirements and show how the design satisfies the requirements. They provide a vehicle for documenting the design and they address information interfaces among the various design groups.

System specification documents follow established format and content requirements. The content of a system specification document includes:

- Purpose of the system
- Functional requirements and design criteria for the system
- System design description including system arrangement and performance parameters
- Layout
- Instrumentation and control requirements
- Interfacing system requirements

The section on interfacing system requirements describes the support needed from and provided to other systems.

System specification documents document human factors and human system interaction requirements. This includes specification of task requirements, information requirements, and equipment requirements for operations, surveillance, test, and maintenance activities.

System specification documents provide specification of instrument and control requirements including:

- System input to the I&C channel list
- Reference to control logic diagrams
- Alarm requirements and characteristics
- Requirements and characteristics of plant status indications

A system specification document for the operation and control centers system provides a mechanism for documenting and tracking human system interface requirements and design specifications. The operation and control centers system specification document is the umbrella document for capturing generic human factors requirements. It provides a uniform operational philosophy and a design consistency among human system interface resources, including alarm system, plant information system, wall panel information system, and computerized procedures.

Functional requirements and design specifications for the AP1000 operation and control centers system, including the main control room, the technical support center, the remote shutdown room, and local control stations are provided in the operation and control centers system specification document. Functional requirements documents and design specification documents are generated for each of the individual human system interface resources (including alarm system, plant information system, wall panel information system, computerized procedures, controls). Functional requirements documents specify the applicable codes, standards, and design requirements and constraints to be met by the design. These documents are referenced by the operation and control centers system specification document.

Design specification documents provide the design specifications for individual human system interface resources and their integration. Included in these specifications are layout and arrangement drawings, algorithms, and display system descriptions, including display task descriptions, display layouts, and navigation mechanisms.

The operation and control centers system specification document, the functional requirement documents, and design specification documents provide input to the generation of I & C system specification documents such as the system specification document for the data display and processing system.

Design Configuration Change Control Process

Design changes are controlled to assure that proposed changes to design documents under configuration control are appropriately evaluated for impacts and that approved changes are communicated to the responsible design organizations.

The design configuration change control process is used to control and implement changes to the design. It is used when the design to be changed has been previously released in a document for project use and placed under configuration control. A design change proposal is the vehicle used to initiate and document review of proposed design changes. Design change proposals include identification of impacts of the proposed design change from affected functional groups. In some instances, human factors engineering issues are addressed by the initiation of design change proposals. In other instances, they are addressed as a consequence of human factor engineering review of design change proposals originating from other disciplines. Design change proposals are maintained in a database that is used to track the status of each design change proposal from initiation through implementation and closure.

Design Review of Human Factors Engineering Products

Design reviews by a multi-disciplined review team are established as a verification method. Requirements for the design review process, including selection of the review team, preparation of information for review, identification and follow of action items, and documentation of the proceedings, are defined.

Design reviews provide a method of design verification consisting of a systematic overall evaluation of a design that is conducted by an independent design review team. Design reviews are conducted at appropriate stages of design development to provide an objective, independent review of design adequacy, safety, performance, and cost. Design reviews are performed by persons not directly associated with the specific design development, but who, as a group, are knowledgeable in the appropriate technical disciplines.

Original designs, as well as major design changes, are subject to the design review process. For each design review, a design review data package is prepared. It includes checklists, including one specifically addressing human factor engineering questions, which are used by design review committee members to aid their review. For each design issue identified through the use of checklists or otherwise, an action item is initiated.

[*Action items are tracked through the design issues tracking system database as described in subsection 18.2.4. The responsibility of entering design review action items into the design issues tracking system database is assigned to the manager responsible for the system reviewed. The responsible design manager is responsible for tracking and addressing open action items.*]*

18.2.3.2 Process Management Tools

Tools are provided to facilitate communication across design disciplines and organizations to enhance consistency. An AP1000 design database enables parties involved in the engineering design of the plant to access up-to-date plant design data. Procedures define requirements and responsibilities for moving data into the database.

Tools are provided to guide the design review process. These include design review checklists that support evaluation of design adequacy, and a database for tracking action items generated as a result of the design review process. Further details on the process of tracking action items generated by design reviews are provided in Subsections 18.2.3.1 and 18.2.4.

A design configuration change control process is used to control and implement proposed design changes. Design change proposals are maintained in a database that is used to track the status of each design change proposal from initiation through implementation and closure.

A design issues tracking system database is used to document and track design issues that are identified during the plant design process. Further details on the design issues tracking system are provided in Subsection 18.2.4.

18.2.3.3 Integration of Human Factors Engineering and Other Plant Design Activities

The AP1000 design process provides for the integration of human factors engineering activities among the design groups.

The instrumentation and control systems design function is responsible for the development of the AP1000 instrumentation and control systems, including the human system interface. Coordination and integration of the instrumentation and control and human system interface design with other plant design activities is performed by the instrumentation and control systems design function. An iterative design process that includes review and feedback from other engineering and design groups at the design interface is specified. Subsection 18.2.3.1 describes the responsibilities and design process of the instrumentation and control system design function.

System specification documents provide the primary vehicle for transmitting system design data and interface requirements, including human factors engineering and human system interface requirements, to the affected AP1000 design and analysis groups. The system specification

*NRC Staff approval is required prior to implementing a change in this information.

documents include a section on interfacing system requirements that describes the support needed from and provided to other systems in the plant. Interface control is performed at the design interfaces and design changes affecting the interfaces are coordinated. Subsection 18.2.3.1 provides details on system specification documents.

A design configuration change control process provides the process and actions to implement design changes. Subsection 18.2.3.1 provides further details on this process.

Engineering design databases serve as a repository of AP1000 design data for parties involved in engineering design activities of the plant. A technical document control system is used to track the status of AP1000 documents. By using the engineering design databases and the technical document control system, parties have access to up-to-date design data to perform their respective design activities.

Section 18.8 presents the implementation plan for the design of the human system interface. Figure 18.2-3 provides an overview of the AP1000 human factors engineering process, including the design stages of the human system interface. The relationship of other human factors engineering process elements to the human system interface design is shown.

18.2.3.4 Human Factors Engineering Documentation

Procedures address documentation for AP1000, including document preparation, review, retention, access, and configuration control. These procedures apply to all AP1000 activities, including human factors engineering.

Documents refer to any self contained portrayal of the AP1000 design or its basis. These include design criteria, descriptions, specifications, drawings, analysis reports, safety reports and calculations.

A procedure establishes requirements and responsibilities for the preparation, review, and approval of AP1000 design documents. The procedure specifies that documents are to be reviewed by appropriate reviewers, and comments are to be resolved prior to issuance of the document. Appropriate reviewers include responsible engineers or managers impacted by the information in the document.

Changes to released documents are reviewed and approved in accordance with the design configuration change control procedure for the AP1000 program.

Procedures establish content and format requirements for system specification documents. Other procedures addressing documentation requirements include those for design configuration change control, design reviews, design criteria, and control of subcontractor submittals.

Sections 18.3 through 18.12 provide information on the types of documents that are generated as part of the AP1000 human factors engineering program.

18.2.3.5 Human Factors Engineering in Subcontractor Efforts

Human factors engineering and human system interface requirements are passed on to subcontractors through engineering documents including design criteria and system specification documents.

Activities within subcontractor design organizations are performed in accordance with the written procedures of those organizations. [*Effective implementation of each organization's quality assurance program is monitored by their respective internal audit programs, and by supplier audits.*]*

*NRC Staff approval is required prior to implementing a change in this information.

See Section 17.3 for quality assurance requirements associated with subcontractor human factors engineering design efforts.

18.2.4 Human Factors Engineering Issues Tracking

A tracking system is used to address human factors issues that are known to the industry and/or identified throughout the life cycle of the human factors engineering/human system interface design, development, and evaluation. The tracking system enables the documentation and tracking of issues that need to be addressed at some later date.

Tracking of human factors engineering issues is accomplished within the framework of the overall plant design process. In this manner, human factors engineering issues are addressed in the same way as those for other disciplines.

[*The design issues tracking system database is used to track AP1000 design issues to resolution, including human factors engineering issues. This database receives input from the following three sources:*

- *Operating experience review*
- *Design reviews*
- *Design issues associated with the design of the human system interface and the operation and control centers system*]*

For each design issue entered into the database, the actions taken to address the issue and the final resolution of the issue are documented.

The human factors issues in the operating experience review report (Reference 2) that are identified as requiring further consideration by the AP1000 design are entered into the design issues tracking system database.

[*The design review process also provides input to the design issues tracking system database. For each design issue identified through the design review process, an action item is initiated. Action items are entered into the design issues tracking system database. Human factors action items from design reviews are included in the database. For preliminary and intermediate design reviews, some action items may be deferred to a more appropriate, subsequent design review. The responsibility of entering design review action items into the design issues tracking system database is assigned to the manager responsible for the system reviewed.*]*

Human factors engineering design issues directly associated with the AP1000 human system interfaces and the operation and control centers system (such as the main control room, remote shutdown room, and technical support center) are entered into the design issues tracking system database. These are design issues that are identified by the human system interface and operation and control centers system designers as issues that need to be addressed by the human system interface design.

The AP1000 project manager, as shown on Figure 18.2-2, is responsible for the maintenance and documentation of the design issues tracking system. For each issue entered into the design issues tracking system database, a “responsible engineer” field is used to assign an engineer the responsibility for resolution of the issue.

18.2.5 Human Factors Engineering Technical Program and Milestones

[*The human factors engineering program is performed in accordance with the human factors engineering process specified in NUREG-0711 (Reference 1).*]* Figure 18.1-1 shows the elements of

*NRC Staff approval is required prior to implementing a change in this information.

the AP1000 human factors engineering program. [*These elements conform to the elements of the Program Review Model specified in Reference 1, as augmented by Reference 7.*]* This is also in accordance with Reference 10.

Human factors engineering Program Management is addressed in Section 18.2. The remaining elements are addressed in Sections 18.3 through 18.11, 18.13, and 18.14.

These sections address the activities conducted as part of the corresponding human factors engineering element, including the accepted industry standards, guidelines, and practices used as technical guidance, the inputs to the element, and the products, including documents that are generated as output. The facilities, equipment, and tools employed are also addressed in the section corresponding to each element.

Figure 18.2-3 provides an overview of the Westinghouse human factors engineering process. The figure summarizes the major activities of the human factors engineering program, their relative order, and the inputs and outputs for the major activities. The boxes in the diagram indicate major human factors engineering activities. The activities are presented in approximate chronological order, with the outputs of each activity serving as inputs to subsequent activities. The items listed below the activity boxes are the document outputs from that human factors engineering activity. The human factors engineering process includes iterations considering the outcomes of subsequent analysis and design activities, design reviews, and testing. In this approach, design issues are addressed and resolved through the iterative stages of the human factors engineering process. Potential points of iteration are indicated in Figure 18.2-3. Further details on the activities, inputs, and output documents associated with the various elements of the human factors engineering program are provided in the sections corresponding to each human factors engineering element.

Figure 18.2-3 provides a program milestone schedule of human factors engineering tasks showing relationships between human factors engineering elements and activities, products, and reviews. Internal design reviews are performed at various points throughout the design process.

18.2.6 Combined License Information

18.2.6.1 Human Factors Engineering Program

The execution of the NRC approved human factors engineering program as presented by Section 18.2 is addressed in APP-OCS-GBH-001 (Reference 8), and the applicable changes are incorporated into the UFSAR.

The AP1000 Human Factors Engineering Program Plan (Reference 8) fully captures the information certified in Section 18.2. Reference 8 provides execution guidance for the NRC-approved HFE program.

18.2.6.2 Emergency Operations Facility

The design of the emergency operations facility in accordance with the AP1000 human factors engineering program is addressed in Reference 9 (APP-GW-GLR-136).

Reference 9 captures the method by which the AP1000 Human Factors Engineering Program Plan (Reference 8) will be applied to TSCs and EOFs that support an AP1000 plant.

EOF and TSC communications, and EOF and TSC human factors attributes are addressed in Subsection 18.2.1.3.

*NRC Staff approval is required prior to implementing a change in this information.

18.2.7 References

[*1. NUREG-0711, "Human Factors Engineering Program Review Model," U.S. NRC, July 1994.*]*

2. WCAP-14645, "Human Factors Engineering Operating Experience Review Report For The AP1000 Nuclear Power Plant," Revision 3.

3. WCAP-14694, "Designers Input to Determination of the AP600 Main Control Room Staffing Level," Revision 0, July 1996.

4. WCAP-14644, "AP600/AP1000 Functional Requirements Analysis and Allocation," Revision 1.

5. Reason, J. T., "Human Error," Cambridge, U.K., Cambridge University Press, 1990.

6. Not used.

[*7. NUREG-0711, Rev. 1, "Human Factors Engineering Program Review Model," U.S. NRC, May 2002.*]*

8. APP-OCS-GBH-001, "AP1000 Human Factors Engineering Program Plan," Westinghouse Electric Company LLC.

9. APP-GW-GLR-136, "AP1000 Human Factors Program Implementation for the Emergency Operations Facility and Technical Support Center," Westinghouse Electric Company LLC.

10. NUREG-0711, Revision 2, "Human Factors Engineering Program Review Model," U.S. NRC, February 2004.

*NRC Staff approval is required prior to implementing a change in this information.

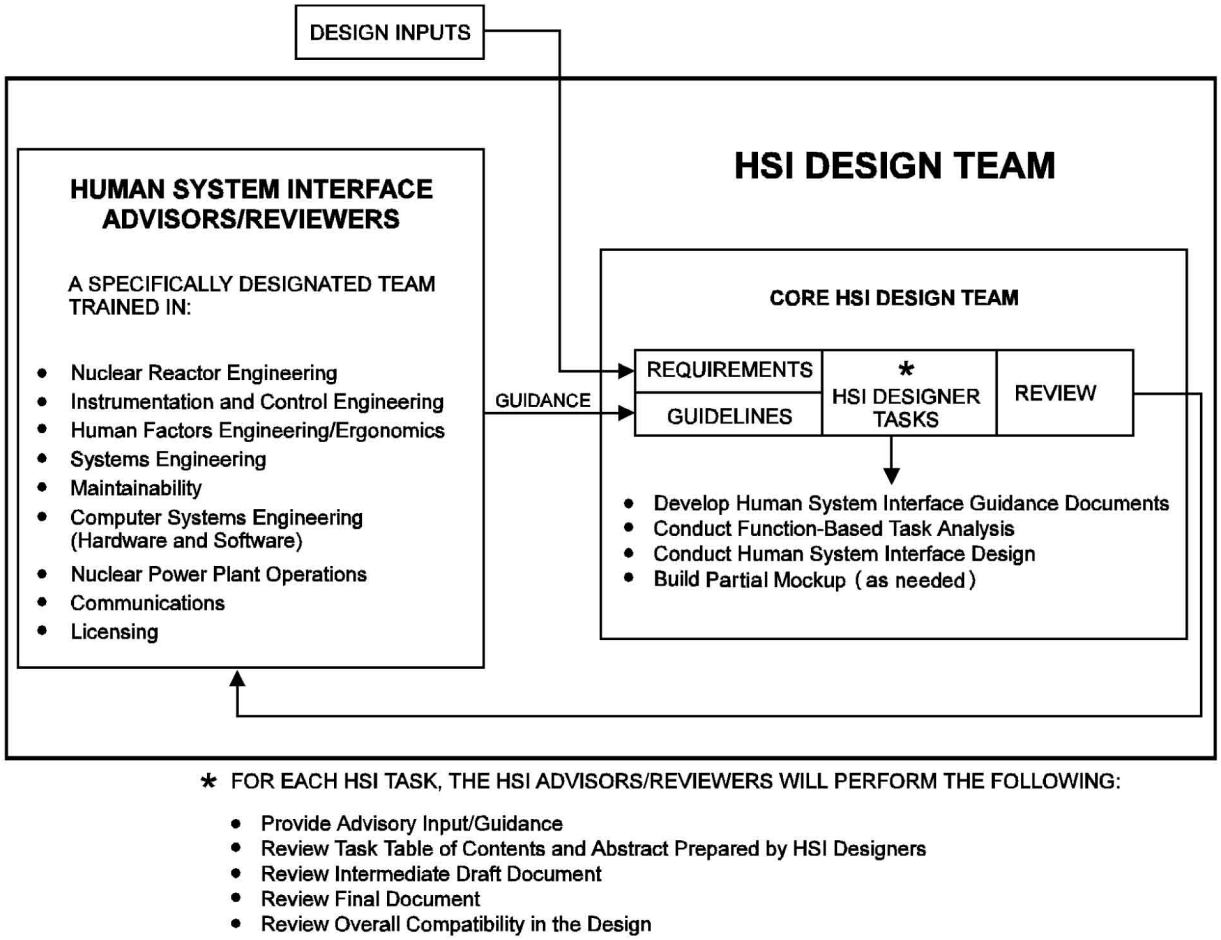


Figure 18.2-1
[*Human System Interface (HSI) Design Team Process*]*

*NRC Staff approval is required prior to implementing a change in this information.

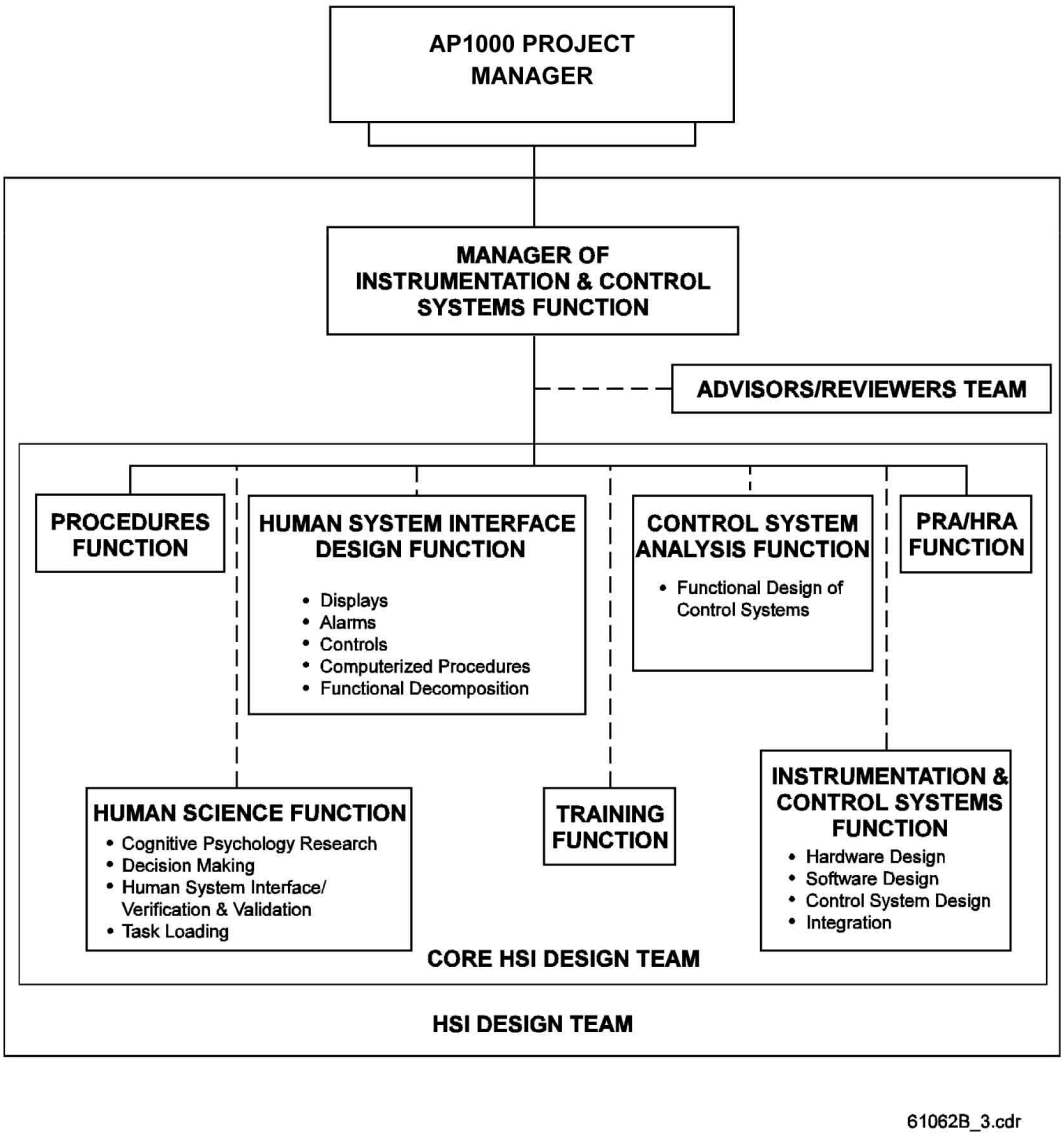


Figure 18.2-2
Human System Interface (HSI) Design Team
Organization and Relationship to AP1000 Organization

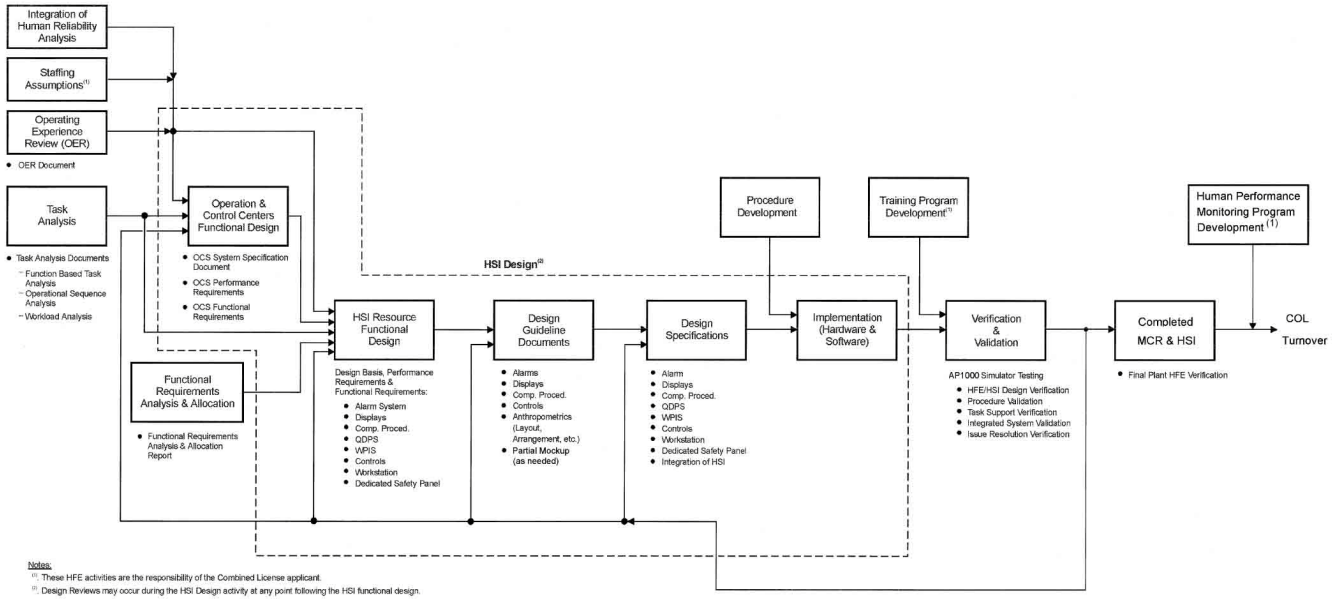


Figure 18.2-3
Overview of the AP1000 Human Factors Engineering Process

18.3 Operating Experience Review

The objective of the operating experience review is to identify and analyze human factors engineering-related problems and issues encountered in previous designs that are similar to the AP1000. Reference 1 documents the results of this review, including descriptions of how the AP1000 design addresses each identified issue.

18.3.1 Combined License Information

Combined License applicant responsibilities identified in Reference 1 are presented in Sections 10.4.12, 16.2, 18.2.6, 18.6.1, and 18.10.1.

18.3.2 References

1. WCAP-14645, "Human Factors Engineering Operating Experience Review Report for the AP1000 Nuclear Power Plant," Revision 3.

18.4 Functional Requirements Analysis and Allocation

Functional requirements and function allocation analyses are performed to establish and document design decisions with respect to level of plant automation.

Functional requirements analysis is defined as the "identification of those functions that must be performed to satisfy plant safety objectives, that is, to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public" (Reference 1).

Function allocation is defined as the "analysis of the requirements for plant control and the assignment of control functions to (1) personnel (e.g., manual control), (2) system elements (e.g., automatic control and passive, self-controlling phenomena), and (3) combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup)" (Reference 1).

Reference 2 documents the methods and results of the functional requirements analysis and function allocation conducted for AP600.

The report provides a description of the AP600 approach to functional requirements analysis and presents the results for AP600 safety functions. The results include a description of AP600 processes, systems, and components involved in maintaining AP600 safety functions. The report also includes a similar analysis for current Westinghouse pressurized water reactor designs to serve as a reference in identifying areas where the AP600 plant differs from previous designs for which operating experience exists. An explicit comparison of the AP600 design with the reference plant design is provided that identifies plant functions, processes, and systems that are new or modified relative to the reference plant design. This includes changes in level of automation.

The report also describes the AP600 approach to initial function allocation and presents the results for AP600 safety functions. A methodology adapted from Reference 3 is used to document the rationale for initial allocation decisions and verify the acceptability of the initial allocation from a human factors perspective. The results include a specification of level of automation and personnel responsibility for AP600 safety functions, processes, and systems. The rationale for the function allocation decisions for AP600 safety functions is documented.

Since AP1000 is like AP600 in its operation and approach to safety functions, Reference 2 is directly applicable to AP1000. It is used as is for functional requirements and function allocation analyses for AP1000.

The report includes a description of human factors activities that are conducted as part of the AP600 HSI design process to verify the adequacy of function allocation decisions and establish the capability of operators to perform the role assigned to them. This is applied to AP1000 and includes:

- How human factors input is provided early in the design process
- How the integrated role of the operator across the systems is confirmed for acceptability
- Mechanisms available for reconsidering, and if necessary, changing AP1000 function allocations in response to operating experience, and the outcomes of ongoing analyses and trade studies

18.4.1 Combined License Information

This section contained no requirement for additional information.

18.4.2 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," U.S. NRC, July 1994.

2. WCAP-14644, "AP600/AP1000 Functional Requirements Analysis and Function Allocation," Revision 1.

3. NUREG/CR-3331, "A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control," 1983.

18.5 AP1000 Task Analysis Implementation Plan

[*Task analysis, according to the Human Factors Engineering Program Review Model (Reference 1), has the following objectives:*

- *Provide one of the bases for the human system interface design decisions*
- *Match human performance requirements with human capabilities*
- *Provide input to procedure development*
- *Provide input to staffing, training, and communications requirements of the plant*]*

This section describes the scope of the AP1000 task analysis activities and the task analysis implementation plan. In addition to References 1 and 16, References 2 through 13 are inputs to this plan.

18.5.1 Task Analysis Scope

[*The scope of the AP1000 task analysis is divided into two complementary activities: function-based task analysis (FBTA) and traditional task analysis, or operational sequence analysis (OSA). The scope of the function-based task analysis is the Level 4 functions*]* identified in Figure 18.5-1. This figure is the functional decomposition (goal-means analysis) for normal power operations in a standard pressurized water reactor. Examples of functions at Level 4 are "Control RCS Coolant Pressure" and "Control Containment Pressure." This set of functions defines the breadth of functions to be analyzed. The function-based task analysis will be expanded in scope to include any additional Level 4 functions identified.

[*The traditional task analysis, or operational sequence analysis, is developed for a representative set of operational and maintenance tasks. The following guidelines are applied to select tasks:*

- *Tasks are selected to represent the full range of operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions.*

- *Tasks are selected that involve operator actions that are identified as either critical human actions or risk-important tasks, based on the criteria in Reference 13.*

- *Tasks are selected to represent the full range of activities in the AP1000 emergency response guidelines.*

- *Tasks are selected that involve maintenance, test, inspection, and surveillance (MTIS) actions. A representative set of maintenance, test, inspection, and surveillance tasks are analyzed for a subset of the "risk-significant" systems/structures/components (SSCs).*

The set of tasks to be analyzed are not identified as a part of design certification. The OSAs listed below are included in the set of tasks to be analyzed: (Each of these satisfies one or more of the selection criteria described above.)

  - *Plant heatup and startup from post-refueling to 100% power*
  - *Reactor trip, turbine trip, and safety injection*
  - *Natural circulation cooldown (startup feedwater with steam generator)*
  - *Loss of reactor or secondary coolant*
  - *Post loss-of-coolant accident cooldown and depressurization*
  - *Loss of RCS inventory during shutdown*
  - *Loss of the normal residual heat removal system (RNS) during shutdown*
  - *Manual automatic depressurization system (ADS) actuation*

*NRC Staff approval is required prior to implementing a change in this information.

– *Manual reactor trip via PMS, via diverse actuation system (DAS)*
– *ADS valve testing during Mode 5*

The human factors engineering program review model (Reference 1) indicates that task analysis should include tasks that are considered to be high-risk and tasks that require critical human actions. Reference 13 defines criteria for critical human actions and risk-important tasks and has identified a list of examples of AP600 tasks that meet these criteria. Reference 13 is applicable to AP1000.]*

Section 16.2 identifies the systems/structures/components included in the Reliability Assurance Program. A subset of these systems/structures/components and a representative set of associated maintenance, tests, inspection and surveillance tasks will be selected by an expert panel. This panel will be comprised of representatives with expertise from relevant groups in the design process, such as systems engineering, reliability engineering, probabilistic risk analysis, human factors engineering, and human system interface design. The set of maintenance, test, inspection and surveillance tasks identified through the expert panel process will be considered to be "risk important" tasks, and will be included in task analysis activities.

18.5.2 Task Analysis Implementation Plan

Figure 18.5-2 shows the proposed sequence of task analyses. Figure 18.5-2 provides information concerning the task analysis and human system interface design elements. [*Task analysis includes both a function-based task analysis and an operational sequence analysis.*]* In Figure 18.5-2, the operational sequence analysis in the task analysis box is designated as OSA-1 since two operational sequence analyses will be implemented.

18.5.2.1 Function-Based Task Analyses

Function-based task analysis is applied to each of the Level 4 functions. There are four components to a function-based task analysis. First, analysis is performed to identify the set of goals relevant to the function. Second, a functional decomposition is performed. This decomposition identifies the processes that, either individually or in combination, have a significant effect on the function. Third, a process analysis is performed by applying a set of questions derived from Rasmussen's model (References 6–9) analysis approach. [*The set of questions used and basis for the methodology is provided in Reference 12.*]* An example of a question from the process analysis is "Are the process data valid?" The results of the process analysis identify the indications, parameters, and controls that the operator uses to make decisions about the respective function. Finally, there is a verification that the indications and controls, identified in the process analysis are included in the AP1000 design.

From the function-based task analyses, the following types of information are obtained:

- A completeness check on the availability of needed indications, parameters, and controls. This includes indications and controls needed for supervisory control of automated systems and manual over-ride.

- Input to the specification and layout of functional displays.

18.5.2.2 OSA-1

The operational sequence analysis completed as part of the task analysis process focuses on specifying the operational requirements for the complete set of tasks selected. For each task, an analysis of the task is conducted that includes the following:

- Plant state data required at each step
- Source of the data (alarm, display, oral communication)

*NRC Staff approval is required prior to implementing a change in this information.

- Action to be taken or decision to be made from the data
- Relevant criterion or reference values
- Information that provides feedback on the action's adequacy
- Other temporal constraints (ordering, tasks that need to be done in parallel)
- Task support requirements needed (required tools)
- Considerations of work environment

The task analyses are developed from the emergency response guidelines and the Probabilistic Risk Assessment event sequences associated with critical or risk-important actions. The following potential limitations on task performance are considered:

- Limits on human performance
- Limits on crew communications

This first operational sequence analysis provides the following types of information:

- Frequency and co-occurrence of plant state parameters and controls
- Display design and organization constraints
- Inventory of alarms, controls, and parameters needed to perform the sequences

As shown in Figure 18.5-2, the function-based task analysis and OSA-1 feed into the human system interface design by providing task performance guidance and constraints. The display and operator workstation design is based on this information.

18.5.2.3 OSA-2

The critical issues for the second operational sequence analysis are:

- Task requirements - This analysis identifies the requirements necessary for the operator to perform the task activities.

- Time to perform tasks - A set of performance time assumptions will be established and used to determine the time required for actions to be completed. These assumptions will provide estimates of task performance times that can be compared to performance time requirements.

- Operator workload analysis - An evaluation of the effect of the human system interface design and the task demands on operator workload will be conducted.

- Operational crew staffing - The workload analysis provides an indication of the adequacy of staffing assumptions. In cases where the operational sequence analysis indicates high operator workload values, or insufficient time available for performance, alternative staffing assumptions or changes to the human system interface design or task allocation to reduce operator workload is evaluated.

This second operational sequence analysis is performed for a representative subset of tasks that include the critical human actions and risk-important tasks and tasks that have human performance concerns (for example, potential for high workload or high error rates).

18.5.2.4 Task Analysis of Maintenance, Test, Inspection and Surveillance Tasks

The maintenance, test, inspection, and surveillance tasks that are identified to be "risk-important" are analyzed using operational sequence task analyses. OSA-1 analyses are conducted on the set of maintenance, test, inspection, and surveillance tasks identified to be "risk-important."

18.5.2.5 Technical Support Center and Emergency Operations Facility

OSA-1 analysis is conducted for the technical support center (TSC) and emergency operations facility (EOF) for the tasks where the data and displays available in the main control room may be utilized to support the TSC and/or EOF functions.

18.5.3 Job Design Factors

Section 18.6 addresses the control room staffing that applies to the AP1000. The staffing level of the main control room, job design considerations, and crew skills are discussed in Subsection 18.6.1.

18.5.4 Combined License Information Item

18.5.4.1 Task Analysis Implementation

The execution and documentation of the task analysis implementation plan presented in Section 18.5 are addressed in APP-GW-GLR-081 (Reference 14), and the applicable changes are incorporated into the UFSAR.

18.5.4.2 Main Control Room Position Scope and Responsibilities

The scope and responsibilities of each main control room position, considering the assumptions and results of the task analysis are addressed in APP-OCS-GJR-003 (Reference 15), and the applicable changes are incorporated into the UFSAR.

18.5.5 References

[*1. NUREG-0711, "Human Factors Engineering Program Review Model," U.S. NRC, July 1994.*]*

2. U.S. NRC Guidance, NUREG/CR-3371, "Task Analysis of Nuclear Power Plant Control Room Crews."

3. IEC-964, "Design for Control Rooms of Nuclear Power Plants."

4. Department of Defense Documents: DI-H-7055, "Critical Task Analysis Report," and MIL-STD-1478, "Task Performance Analysis."

5. NATO Document, "Applications of Human Performance Models to System Design," edited by McMillan, Beevis, Salas, Strub, Sutton, & van Breda, New York: Plenum Press, 1989.

6. Rasmussen, J., "Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering," New York: North-Holland, 1986.

7. Hollnagel, E. and Woods, D. D., "Cognitive Systems Engineering: New Wine in New Bottles," International Journal of Man-Machine Studies, Volume 18, 1983, pages 583-600.

8. Roth, E. and Mumaw, R., "Using Cognitive Task Analysis to Define Human Interface Requirements for First-of-a-Kind Systems," Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting, San Diego, Ca., 1995, pp. 520-524.

*NRC Staff approval is required prior to implementing a change in this information.

9. Vicente, K. J., "Task Analysis, Cognitive Task Analysis, Cognitive Work Analysis: What=s the Difference?" Proceedings of the Human Factors and Ergonomics Society 39th Annual Meeting, San Diego, Ca., 1995, pp. 534-537.

10. Drury, C. G., Paramour, B., Van Cott, H. P., Grey, S. N., and Corlett, E. N., "Task Analysis," Handbook of Human Factors, Salvendy, G. (ed.), New York: John Wiley & Sons, 1987.

11. Woods, D. D., "Application of Safety Parameter Display Evaluation Project to Design of Westinghouse SPDS," Appendix E to "Emergency Response Facilities Design and V & V Process," WCAP-10170, submitted to the U.S. Nuclear Regulatory Commission in support of their review of the Westinghouse Generic Safety Parameter Display System (Non-Proprietary) (Pittsburgh, PA, Westinghouse Electric Corp.), April 1982.

[*12. WCAP-14695, "Description of the Westinghouse Operator Decision Making Model and Function Based Task Analysis Methodology," Revision 0, July 1996.*]*

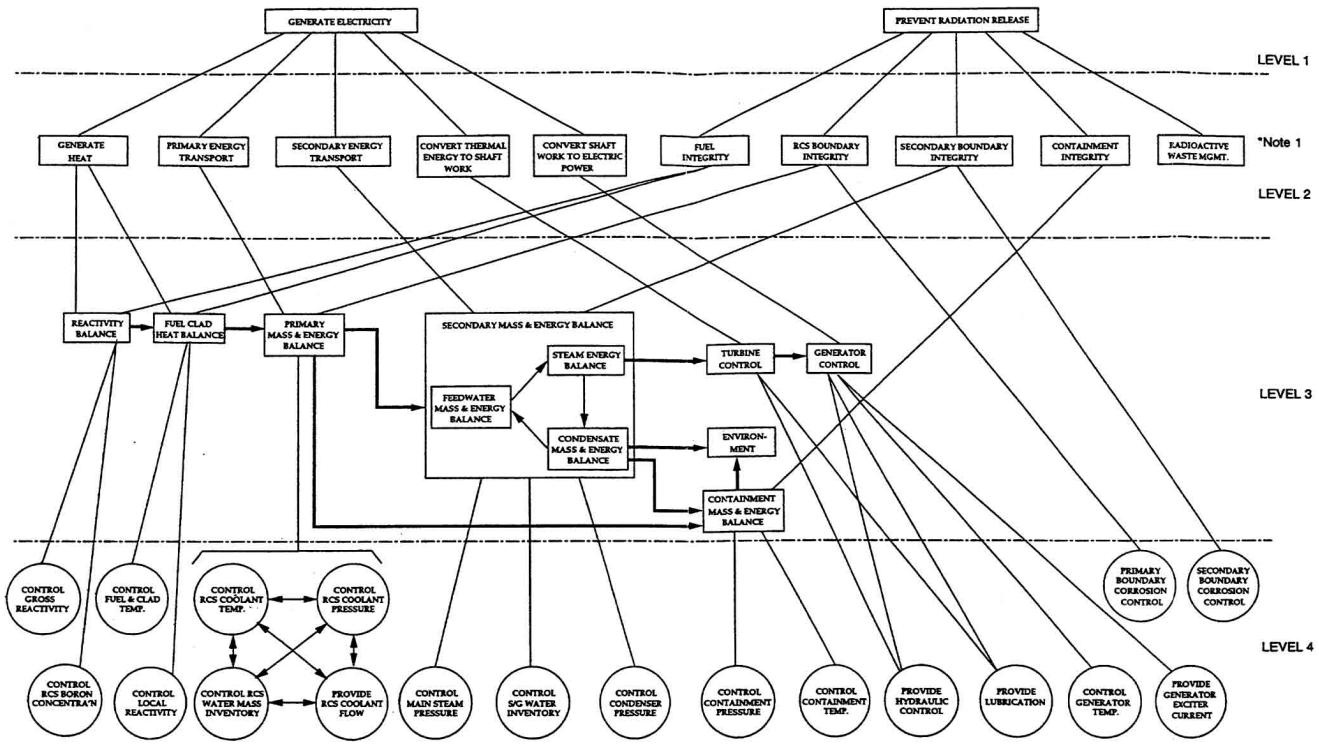
[*13. WCAP-14651, "Integration of Human Reliability Analysis and Human Factors Engineering Design Implementation Plan," Revision 2, May 1997.*]*

14. APP-GW-GLR-081, "Closure of COL Information Item 18.5-1, Task Analysis," Westinghouse Electric Company LLC.

15. APP-OCS-GJR-003, "AP1000 Main Control Room Staff Roles and Responsibilities," Westinghouse Electric Company LLC.

16. NUREG-0711, “Human Factors Engineering Program Review Model,” Revision 2, U.S. NRC, February 2004.

*NRC Staff approval is required prior to implementing a change in this information.



*Note 1: Decomposition and subsequent task analysis of this activity is performed as part of a similar process applied to the radioactive waste control center.

Figure 18.5-1
Top Four Levels of the Normal Power Operation for a Westinghouse PWR

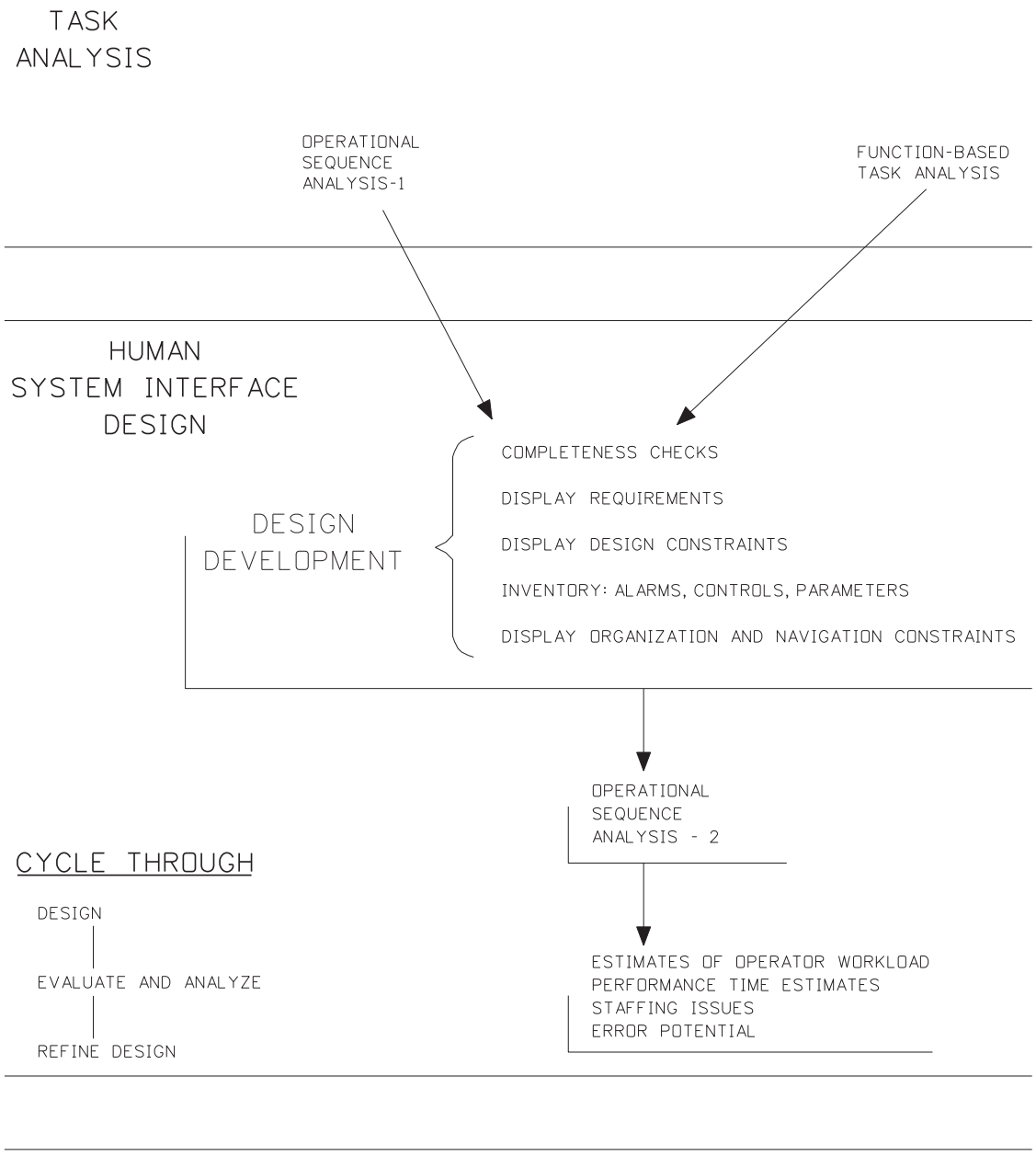


Figure 18.5-2
Task Analysis Utilized as Design Input

18.6 Staffing

Table 13.1-201 contains the estimated staffing levels for those categories of personnel that are addressed by the Human Factors Engineering program per NUREG-0711, “Human Factors Engineering Program Review Model” (Reference 201), as follows:

- Licensed operators
- Shift Supervisors
- Non-licensed operators
- Shift technical advisors
- Instrumentation and control technicians
- Mechanical maintenance technicians
- Electrical maintenance technicians
- Radiation protection technicians
- Chemistry technicians
- Engineering support

The minimum level of staffing for control room personnel who directly monitor and control the plant is stated in Table 13.1-202 and meets the requirements of 10 CFR 50.54(m). Information about the staffing levels of security personnel is contained in the separately submitted physical security plan.

Qualification requirements of plant personnel listed above are discussed in Subsections 13.1.1.4, Qualifications of Technical Support Personnel, and 13.1.3, Qualification Requirements of Nuclear Plant Personnel, and, for security personnel, in the physical security plan.

The baseline level of staffing for the categories of personnel discussed above is derived from experience in current operating nuclear power plants. The number of personnel in operating plants has evolved over many years to a level that is safe and efficient and provides adequate personnel to operate the plant under all conditions, including abnormal and emergency, meets regulatory requirements, and supports individual training and personal needs.

Iterative adjustments are implemented to the level of staffing, as necessary, based on findings and input from periodic reviews and staffing analysis. Input to this analysis includes information derived from the other elements of the human factors engineering program, particularly operating experience review, functional requirements analysis and function allocation, task analysis, human reliability analysis, human-system interface design, procedure development, and training program development.

In addition to the regulatory requirements referenced, input to the analyses and the level of staffing is provided by WCAP-14694, “Designer’s Input to Determination of the AP600 Main Control Room Staffing Level” (Reference 1), AP1000 Combined License Technical Report APP-GW-GLR-010, “AP1000 Main Control Room Staff Roles and Responsibilities” (Reference 202), and EPRI Technical

Report 1011717, “Program on Technology Innovation: Staff Optimization Scoping Study for New Nuclear Power Plants” (Reference 203).

18.6.1 Combined License Information Item

The staffing levels and qualifications of plant personnel including operations, maintenance, engineering, instrumentation and control technicians, radiological protection technicians, security, and chemists, and the number of operators needed to directly monitor and control the plant from the main control room, including the staffing requirements of 10CFR50.54(m), is addressed in Section 18.6.

18.6.2 References

1. WCAP-14694, "Designer's Input To Determination of the AP600 Main Control Room Staffing Level," Revision 0, July 1996.

201. United States Nuclear Regulatory Commission, “Human Factors Engineering Program Review Model,” NUREG-0711, Revision 2, February 2004.

202. Westinghouse, “AP1000 Main Control Room Staff Roles and Responsibilities,” APP-GW-GLR-010, Rev. 2, June 2007.

203. EPRI, “Program on Technology Innovation: Staff Optimization Scoping Study for New Nuclear Power Plants,” Technical Report 1011717, Final Report, August 2005.

18.7 Integration of Human Reliability Analysis with Human Factors Engineering

Human reliability analysis (HRA) evaluates the potential for human error that may affect plant safety. There are important interfaces between the human factors engineering program and human reliability analysis. Human reliability analysis makes use of outputs of human factors engineering/HSI design activities including analyses of operator functions and tasks and specifications of HSI characteristics. Human reliability analysis is a source of input to human factors engineering/HSI design in identifying plant scenarios, human actions, and HSI components that are important to plant safety and reliability.

[*The objective of integration of human reliability analysis with human factors engineering is to specify the interfaces between human reliability analysis and human factors engineering activities. Reference 1 documents the implementation plan for the integration of human reliability analysis with human factors engineering design.*]* Reference 2 documents the execution and documentation of this implementation plan.

[*The objective of the human reliability analysis/human factors engineering integration implementation plan is to enable:*

- *Human reliability analysis activity to integrate the results of the human factors engineering design activities*
- *Human factors engineering design activities to address critical human actions, risk important tasks, and human error mechanisms, in order to minimize the likelihood of personnel error and to provide for error detection and recovery capability*]*

Human reliability analysis methodology and results are described in Chapter 30 of the AP1000 PRA.

18.7.1 Combined License Information

The execution and documentation of the human reliability analysis/human factors engineering integration implementation plan that is presented in Section 18.7 is addressed in Reference 2 (APP-GW-GL-011, WCAP-16555).

18.7.2 References

[*1. WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan," Revision 2, May 1997.*]*

2. WCAP-16555, "AP1000 Identification of Critical Human Actions and Risk Important Tasks," Revision 0, March 2006.

*NRC Staff approval is required prior to implementing a change in this information.

18.8 Human System Interface Design

This section provides an implementation plan for the design of the human system interface (HSI) and information on the human factors design for the non-HSI portion of the plant. The human system interface includes the design of the operation and control centers system (OCS) and each of the human system interface resources.

The operation and control centers system includes the main control room, the technical support center, the remote shutdown room, emergency operations facility, local control stations and associated workstations for each of these centers. The AP1000 human system interface resources include:

- Wall panel information system
- Alarm system
- Plant information system
- Computerized procedure system
- Soft controls/dedicated controls
- PMS safety displays

The wall panel information system presents information about the plant for use by the operators. No control capabilities are included. The wall panel information system provides dynamic display of plant parameters and alarm information so that a high level understanding of current plant status can be readily ascertained. It is located at one end of the main control area at a height such that persons seated at the reactor operator and senior reactor operator workstations can view it while sitting at their respective workstations. It provides information important to maintaining the situation awareness of the crew and for supporting crew coordination. The wall panel information station provides a dynamic display of the plant. It also serves as the alarm system overview panel display. The display of plant disturbances (alarms) and plant process data is integrated on this wall panel information system display. The wall panel information system is a nonsafety-related system. It is designed to have a high level of reliability.

The mission of the AP1000 alarm system, together with the other human system interface resources, is to provide the operation and control centers operating staff with the means for acquiring and understanding the plant's behavior. The alarm system improves the performance of the operating crew members, when acting both as individuals and as a team, by improving the presentation of the plant's process alarms. [*The alarm system supports the control room crew members in the following steps or activities of Rasmussen's operator decision-making model (Reference 25):*]*

- The "alert" activity, which alerts the operator to off-normal conditions

- The "observe what is abnormal" activity, which aids the user in focusing on the important issue(s)

- The process "state identification" activity, which aids the user in understanding the abnormal conditions and provides corrective action guidance. It guides the operating crew into the information display system.

The plant information system is a subset of the data display and processing system (non-Class 1E system), presenting plant process information for use by the operators. The plant information system provides dynamic indications of plant parameters and visual alerts so that an understanding of current plant conditions and status is readily ascertained. The plant information system uses color-graphic visual display units located on the operation and control centers workstations to display plant process data. These displays provide information important to monitoring, planning, and controlling the operation of plant systems and obtaining feedback on control actions. The displays provided by

*NRC Staff approval is required prior to implementing a change in this information.

the plant information system are nonsafety-related displays, but provide information on both safety-related and nonsafety-related systems.

The computerized procedure system has a mission to assist plant operators in monitoring and controlling the execution of plant procedures. The computerized procedures system is a software system. It runs on the hardware selected for the operation and control centers. The computerized procedure system is accessible from the workstations in the main control room. A procedure writer's guide is developed as part of the human system interface design implementation plan for the computerized procedure system. The writer's guide is the design guidelines document for the computerized procedure system. Information on the writer's guide and on the computerized procedure system is found in Reference 31. Application of the computerized procedure system for emergency operating procedures is licensed outside the United States and is being used in an operating nuclear power plant. Additionally, the application of the computerized procedure system for turbine-generator startup and shutdown is being used in another operating nuclear power plant located outside the United States. Human factors engineering review guidance for computer-based procedures is presented by Reference 9. The design of a backup to the computerized procedure system, to handle the unlikely event of a loss of the computerized procedure system, is developed as part of the human system interface design process. Design options include the use of a paper backup. [*The acceptability of the computerized procedure system and its backup will be confirmed as integral elements of the AP1000 design by the implementation of the AP1000 verification and validation program (Reference 24).*]* Procedure development is addressed in Sections 13.5 and 18.9.

The mission of the controls in the main control room is to allow the operator to operate the plant safely under normal conditions, and to maintain it in a safe condition under accident conditions. The main control room includes both safety-related and nonsafety-related controls. The types of controls in the main control room include both discrete (dedicated) control switches and soft controls. The discrete control switches are controls dedicated to a single function. Figure 18.8-1 shows a representative model of the soft controls used in AP1000. The soft control units are control devices whose resulting actions are selectable by the operator. The instrumentation and control architecture uses both discrete control switches and soft control units. The soft control units are used to provide a compact alternative to the traditional control board switches by substituting virtual switches in the place of the discrete switches.

The final configuration of these elements is dependent upon the results of the human system interface design process described in Subsection 18.8.1 below.

The mission of the PMS safety displays is to provide a Class 1E system to present to the main control room operators the plant parameters which demonstrate the safety of the plant. The qualified data processing system provides for the display of the variables as described in Section 7.5. The informational content of qualified data processing system is provided to the remote shutdown workstation through the plant information system.

18.8.1 Implementation Plan for the Human System Interface Design

Figure 18.2-3 provides an overview of the AP1000 human factors engineering process, including the design stages of the human system interface. The relationship of other human factors engineering process elements to the human system interface design is shown.

The functional design of the operation and control centers system and the human system interface is the activity where the functional requirements for the human system interface resources of the main control room and related operation and control centers system are developed. The output of the functional design is a set of documents that specify the mission, design bases, performance requirements, and functional requirements for each human system interface resource. These

*NRC Staff approval is required prior to implementing a change in this information.

functional requirement documents and the human system interface design guidelines are used to develop the design specifications. The design specifications are provided as input to the hardware and software system designers for design implementation.

The following subsections describe the activities conducted as part of the human system interface design and the documents that are produced.

18.8.1.1 Functional Design

A system specification document for the operation and control centers system documents and tracks human system interface requirements and design specifications. The operation and control centers system specification document is the umbrella document for capturing human factors requirements and providing a uniform operational philosophy, and design consistency among the individual human system interface resources.

Included in the operation and control centers system specification document are functional requirements and specifications for the AP1000 operation and control centers system, including the main control room, the technical support center, the remote shutdown room, and local control stations. In addition, functional requirement documents are generated for each of the individual human system interface resources. These documents are referenced by the operation and control centers system specification document.

The operation and control centers system specification document and the individual human system interface functional requirement documents include mission statements and performance requirements. The mission statements establish the high level goals and main tasks to be supported by the control center or human system interface resource. Performance requirements represent high level design goals and help to clarify the functional designer's intent. They are high level requirements that may not be readily verifiable by testing or other quantitative means, but are important considerations for meeting the goals defined in the mission statements. The design bases establish the foundation for the design and the rationale behind engineering decisions made and criteria established for the design. Functional requirements include requirements needed to meet the criteria defined in the applicable codes, standards, and customer requirements.

The operations and control centers functional requirements document includes requirements to meet failure, diversity, electrical separation, and other applicable criteria. This document establishes requirements related to access control, redundancy, independence, identification and test capability, and defines requirements on system inputs and outputs. It specifies the system safety classification and defines applicable quality assurance, reliability goals, and environmental qualification requirements. The specification of the cognitive activities in the operator decision-making model that each human system interface resource is intended to support is provided in the operation and control centers functional requirements document.

Reference 25 describes the operator decision-making model and associated operator cognitive activities. As shown in Figure 18.8-2, the HSI interface resources are mapped to four major classes of operator cognitive activities in the model (detection and monitoring, interpretation, control, and feedback).

The contents of this map are then considered in terms of sources of operational complexity that add operator performance demands. The two general sources of complexity considered are 1) use of multiple as opposed to single HSI resources, and 2) increasing situational or scenario-based complexity. Considering the impact of complexity on the mapping leads to "issues"; that is, general cases where adequate human performance should be confirmed.

Table 18.8-1 presents the resulting set of human performance issues. Note that “feedback” issues have been addressed under “control,” rather than as a separate activity, because feedback activities follow directly from control activities. These human performance issues serve as input to the development of the performance requirements for the operation and control centers system specification document and to the individual human system interface functional requirement documents. The human performance issues and requirements will be addressed by the verification and validation activities described by Reference 24.

18.8.1.2 Design Guidelines

Guidelines for the human system interface design have been developed for the human system interface resources to facilitate the standard and consistent application of human factors engineering (HFE) principles to the design (see Reference 1). Reference 1 contains standards and conventions guidelines and tailors generic human factors engineering guidance to the AP1000 human system interface design and defines how those human factors engineering principles are applied.

These guidelines enable groups of people to simultaneously develop the human system interface in a consistent manner in accordance with the human factors engineering principles established for the design. [*The guidelines are used to perform the human factors engineering design verification activity of the human factors verification and validation plan (Reference 24).*]*

Human system interface design guideline documents include:

- Anthropometric guidelines
- Alarm guidelines
- Display guidelines
- Controls guidelines
- Computerized procedures guidelines

The AP1000 human system interface design guidelines document provides:

- Statements of their intended scope, references to source materials, and instructions for their proper use.

- Specification of accepted human factors engineering guidelines, standards, and principles to which the AP1000 human system interface conforms.

- Specification of design conventions (for example, coding conventions) to which the AP1000 human system interface conforms.

- Documentation of deviations from human factors engineering guidelines, standards and principles, and justification based on documented rationale such as trade study results, literature-based evaluations, demonstrated operational experience, and tests and experiments.

The accepted human factors engineering guidelines documents that were used in compiling the AP1000 human system interface design guidelines document are found in References 2 through 8.

18.8.1.3 Design Specifications

Design specifications are written for the operation and control centers system and the human system interface resources. The design specification documents are the result of applying the guidelines to the functional design. They provide the design for each human system interface resource, including the integration of the hardware and software modules, to satisfy the human system interface

*NRC Staff approval is required prior to implementing a change in this information.

functional design requirements. Included in these specifications are layout and arrangement drawings, algorithms, display layouts, display task descriptions, navigation mechanisms and resource lists.

The functional requirement documents are used to define the bases for the system design specifications.

The operation and control centers system specification document and human system interface functional requirements and design specification documents provide input to the generation of instrumentation and control system specification documents, such as the system specification document for the data display and processing system. These specification documents are used as inputs to the hardware and software system designers to generate implementation documents such as hardware and software specifications.

18.8.1.4 Man-in-the-Loop Testing

An integral part of the human system interface design process is the conduct of man-in-the-loop engineering tests to obtain feedback from prototype design products early in the design process.

The use of engineering tests is a good engineering practice, which reflects an iterative design process. By providing feedback early, before the detailed design is complete, engineering tests can help to improve the design and to avoid problems in the final product. Engineering tests also may offer concrete insight on questions that cannot be resolved logically (for example, by guidance or analysis). Finally, results from engineering tests provide evidence of design adequacy. Engineering tests thus serve to increase confidence and reduce project risk in the design process.

Engineering tests are performed to obtain empirical results that can be applied directly to understanding and improving the design product. More specifically, engineering tests are designed to produce the following types of results for the prototype design:

- Design-specific operating experience
- Confirmation of necessary performance and integration
- Identification of specific problems
- Subjective feedback from expert users and observers

[*The man-in-the-loop test plan to obtain feedback from prototype design products early in the design process is defined and documented in Reference 46.*]* The results of the engineering testing are used to refine the design of the operation and control centers system and the human system interface.

18.8.1.5 Mockup Activities

A mockup of portions of the main control room working area is constructed as part of the human system interface design process. The partial mockup consists mainly of non-operational representations of the desks, displays, and panels. The mockups are constructed to the anthropometric profiles and arranged in the floor layout intended for the main control room.

The partial mockup is used to examine and verify, as needed, physical layout aspects such as availability of workspace, physical access, visibility, and related anthropometric and human factors engineering issues. It will also be used for walk-through exercises to examine issues such as staffing levels, task allocation, and procedure usage.

*NRC Staff approval is required prior to implementing a change in this information.

18.8.1.6 Human System Interface Design Documentation

The human system interface design is documented through a system specification document for the operation and control centers system, functional requirement documents, design criteria documents, design review documents, and documentation of design configuration change control.

18.8.1.7 Task-Related Human System Interface Requirements

As shown in Figure 18.2-3, the results of other human factors engineering program elements are used as input and bases for developing the operation and control center system and human system interface resources functional design (mission statements, performance requirements, design bases, functional requirements), guideline documents and the design specification documents. Staffing assumptions, operating experience reviews, functional requirements analysis and allocations, task analysis, and integration of human reliability analysis provide the bases for identifying the human system interface requirements needed to support human functions and tasks. The resulting human system interface requirements are documented in the human system interface resource functional design documents (operation and control centers system specification document and the individual human system interface resource functional requirements document), guidelines document and design specification documents. Subsections 18.8.1.1 through 18.8.1.3 provide descriptions of these documents.

The AP1000 task analysis, described in Section 18.5, includes two complementary activities: function-based task analysis (FBTA) and traditional task analysis, or operational sequence analysis (OSA). The function-based task analysis identifies the indications, parameters, and controls that the operator needs to make decisions about the respective function. There is also a verification that the indications and controls identified in the process analysis are included in the design. The operational sequence analysis, completed as part of the task analysis process, focuses on specifying the operational requirements for the complete set of tasks selected. One of the guidelines used in selecting tasks for analysis are those tasks that represent the full range of activities in the AP1000 emergency response guidelines. One type of information provided by the operational sequence analysis is an inventory of alarms, controls, and parameters needed to perform the task sequences. The operational task analysis results include the identification of controls, alarms, and parameters needed by the operator to execute task sequences found within the emergency response guidelines. These results serve as a cross-check with the function-based task analysis results. Design reviews held during the human system interface design serve as another means of verifying completeness and identifying and correcting omissions. [*The task support verification activity of the human factors verification and validation (Reference 24) verifies that the human system interface design provides the necessary alarms, displays, and controls to support personnel tasks.*]*

The collective results of the task analysis activities identify the tasks and operational information needed by the operator to execute these tasks. For each display, a display task description is written. The display task description includes the identification of the informational needs to be supported by the display. The features, dynamic characteristics, calculated values, and supporting algorithms for the display are part of the display task description. The design specification of a display includes the range, precision, and measurement units of the parameters provided in the display. These parametric characteristics are chosen to support the task and the operator informational needs. The parametric characteristics, identified in the design specification, are provided using the guidelines presented in the design guidelines document for displays. The basis for the parametric characteristics chosen for the displays is found in the design guidelines document.

18.8.1.8 General Human System Interface Design Feature Selection

The AP1000 human system interface resources include the wall panel information system, alarm system, plant information system, computerized procedure system, controls, (soft and dedicated)

*NRC Staff approval is required prior to implementing a change in this information.

and the PMS safety displays. These human system interface resources are used as a starting point to define how the human system interface supports operator performance. [*Reference 25 describes the operator decision-making model that is used by the task analysis activities to identify the operator's information and control requirements.*]* The human system interface resources are mapped to the major classes of operator activities identified from this model. Figure 18.8-2 illustrates this mapping. The human performance requirements that each human system interface resource supports are identified as part of the design process.

The human system interface resources are chosen based upon utility requirements and review of operating experience. The goal of the human system interface design is to provide the operators with effective means for acquiring and understanding plant data and executing actions to control the plant's processes and equipment. Through implementation of the human system interface design process, the identified AP1000 human system interface resources are developed.

Design alternatives for a feature within a human system interface resource (such as the use of a mouse, trackball, or touchscreen for soft controls) are evaluated. A decision is made based upon evaluation methods including human factors/trade-off studies, reviews of nuclear industry operating experience or reviews of other industry experience, experience gained from past projects, and utility input. The basis and rationale for the decisions are provided in the functional design documentation.

18.8.1.9 Human System Interface Characteristics: Identification of High Workload Situations

Identification of high operator workload situations and their consequent changes in operator response times or likelihood of operator error is a usability issue. Potential impact on operator workload is a criterion in selecting the human performance issues identified in Table 18.8-1.

Identification of high-workload situations through analytic techniques and part-task simulations is part of the human factors engineering program (Section 18.5 on Task Analysis).

Use of Workload Measurement Techniques

As part of task analysis activities (Section 18.5), analytic approaches are used to estimate workload. Analytic methods include the use of task analysis.

Usability Guidance

Usability guidance is included in the human system interface design guidelines, as discussed in Subsection 18.8.1.2.

Workstation Usage Scenarios

The physical layout of the AP1000 control room and related control centers follows established ergonomic guidelines including consideration of fatigue and alertness of operators sitting at workstations.

Environmental Conditions

Determination of environmental conditions (lighting, noise, ambient working temperatures, radiation, air quality, and humidity) in the control room, the remote shutdown room, and at local control stations employ well-accepted standards from the fields of industrial and human engineering such as References 14, 15 and 16. Relevant guidance from prior studies in the nuclear power area (References 17 through 20) is also used.

*NRC Staff approval is required prior to implementing a change in this information.

The worst credible conditions that can be encountered by operators in the main control room are identified as outcomes of design basis scenarios. Effects on operator performance and the effects of extremes of habitability during degraded conditions are considered in the design specification.

Local Control Actions

Critical human actions and risk important tasks are identified by the probabilistic risk assessment/ human reliability analysis process. [*Reference 23 presents the process of identifying the critical human actions and risk important tasks and the implementation plan for integrating human reliability analysis into the human factors engineering program*.]* Critical human actions or risk important tasks are examined by task analysis, human system interface design, and procedure development, to identify changes to the operator task or the control and display environment to reduce or eliminate sources of error.

18.8.1.10 Human System Interface Software Design and Implementation Process

This subsection describes the software design, implementation, and verification process established to verify that human system interface functional requirements are implemented by the software. The software design, implementation, and verification process uses a top-down approach to incorporate the system design requirements and the functional requirements into software module design.

Software refers to the computer instructions and information provided to implement a subset of the human system interface functional requirements. The software design and implementation process is a subset of the overall human system interface design process. It consists of system software design specifications, software design, software implementation, and software verification.

The system software design specification activity takes as its input the system functional requirement and specification documents and produces software design requirements documents and the software verification test procedures. Software design requirements documents list the functions, performance, design constraints, and attributes of the system software.

The software design activity takes software design requirements and produces software design specification documents. Software design specification documents provide the details for the software design at the module level and assembly level. These documents define the software language, logical structure, variable names, information flow, logical processing steps, and data structure of the system software programs. They also describe the functions performed, support software, storage and execution limitations, interface constraints, error conditions, error detection, error response actions, and details of the software operation in the hardware environment.

The software implementation activity implements the software design specifications in the form of documented source programs and object code. The source program and associated documentation contain the comments, functional diagrams, external references, and internal module descriptions.

The object code is generated from the source program and installed in processor memory to perform the functions specified by the software design specifications.

In the software verification testing activity, the software is tested to verify that it complies to the system software design requirements. The software is tested according to the software verification test procedures.

Nonconformances of the software to the software verification test procedures are documented by trouble reports, and changes are made. In the case where the error is a result of an error in the system software design requirements or the software design specifications, these documents are revised. The software test results report presents a summary of the software verification testing results.

*NRC Staff approval is required prior to implementing a change in this information.

18.8.2 Safety Parameter Display System (SPDS)

[*The Safety Parameter Display System is designed following the human system interface design implementation plan*]* described in Subsection 18.8.1. [*The Safety Parameter Display System is integrated into the design of the AP1000 human system interface resources*.]*

As noted in Section 4.1.a of Reference 27 "...the principle purpose and function of the Safety Parameter Display System is to aid the control room personnel during abnormal and emergency conditions in determining the safety status of the plant and in assessing whether abnormal conditions warrant corrective action by operators to avoid a degraded core. This can be particularly important during anticipated transients and the initial phase of an accident." Since the main intended use is during relatively rare occurrences, human-factors engineering suggests that the operators will find that the use of data acquisition habits acquired and repeated during the normal operation of the plant will be the most successful. A system in the control room that only varies its output during abnormalities may require a shift in mental focus and in data acquisition habits and subsequent analysis. An effective means for conveying the safety state of the plant is to provide data and displays for normal operation that employs the Safety Parameter Display System required principles for data synthesis, concentration and display. This operator interface is operational over the range of plant conditions specified by the Safety Parameter Display System requirements, as well as during normal operations.

The operator-interface to the plant is improved by integrating Safety Parameter Display System requirements into the overall human system interface design to avoid the need for another system that is infrequently used.

The following subsections describe [*the approach to meeting the regulatory requirements for a Safety Parameter Display System by addressing the Safety Parameter Display System requirements of References 26 and 27*.]*

18.8.2.1 General Safety Parameter Display System Requirements

The AP1000 human system interface resources used to address the Safety Parameter Display System requirements are the alarm system, plant information system (workstation visual display unit displays), and the computerized procedure system. The AP1000 human system interface data display (alarms and visual display unit displays) is organized around the Safety Parameter Display System requirement of plant process functions. Expressing plant state in terms of process functions is incorporated in the AP1000 control room design. This is expected to improve the human interface by making the data presentation interface seamless as the plant moves from one operational state to another.

An alarm system which organizes the presentation of alarms by process function and adapts a "dark board" approach (for all plant modes) continually indicates the state of each of the functions. By remaining dark when the process is performing as expected, the process functions are interpreted as being satisfied. An alarm indication displayed in any function indicates that the function is in jeopardy. In this way, the set of alarms that is active is the minimum set. The alarm system is capable of displaying a full range of alarms based on important plant parameters and data trends. The alarms indicate when process limits are being approached and exceeded.

Section 18.7 and [*Reference 23 present an implementation plan for integrating the human reliability analysis with human factors engineering*.]* The critical human actions and the risk important tasks identified through the execution of this plan are used as an input to the task analysis activities and subsequently to the design of the human system interface. They are also used to evaluate the Safety Parameter Display System functions and parameters selected to monitor these functions. The human system interface, which includes the integration of Safety Parameter Display System

*NRC Staff approval is required prior to implementing a change in this information.

requirements, is designed to reduce the likelihood of operator error and provide for error detection and recovery capability for the identified critical human actions and risk important tasks.

18.8.2.2 Display of Safety Parameters

The functionally organized plant information system displays, including the Safety Parameter Display System-related displays, are accessed on the workstation visual display units (VDU) using a cursor. The AP1000 operator workstations employ a windowing system which allows a single cursor to cover the visual display unit screens. The design allows the operator to recover a specific parameter within one or two actuations of the pointing device.

The design goal for the AP1000 human system interface is to update the displays every 1 to 2 seconds. The process data sampling rate is 1 second or less. Sequence of events (SOE) points can be sampled at a rate of once every milli-second and are available within the AP1000 human system interface. The Safety Parameter Display System responds to user commands in less than 10 seconds. The design goal for graphical display response time, from user command to developed graphical display, in the AP1000 human system interface is 2 seconds.

The AP1000 alarm system includes plant overview alarms that are organized around the concept of plant process functions. These process functions address the five SPDS functions. The alarm system overviews, including the functional organization, are integrated into the wall panel information system displays.

During the execution of emergency operating procedures, the computerized procedure system provides a continuous display of the status of each critical safety function.

The Safety Parameter Display System data and data display organization are available to the control room staff.

[*The AP1000 human system interface process display set (from the plant information system) is organized into two hierarchies that are linked together. One is focused upon providing the process data from a functional perspective and the other from a physical perspective. Both follow the concept of abstraction/aggregation suggested by Rasmussen as described in Reference 25. Top levels in the hierarchy are plant wide summaries, lower levels are component details. The hierarchy is structured so as to reflect the plant process functional decomposition performed during the function based task analysis described in Reference 25.*]*

Process display presentation for the control room users is organized by functions. The function based task analysis integrates the functional organization design principles dictated by the Safety Parameter Display System requirements into the AP1000 human system interface.

Plant process displays and plant controls necessary to operate the plant are located on the reactor operator console. There are a total of six redundant workstations on the reactor operator console.

Because the Safety Parameter Display System requirements are an integral part of the AP1000 human system interface design, the Safety Parameter Display System workstation is the AP1000 human system interface control room workstation, the Safety Parameter Display System displays are the workstation displays; and the display accessing “controls” used to access Safety Parameter Display System displays are the same as those used to access any workstation display.

Safety Parameter Display System-related information is physically displayed such that the information can be read from the Safety Parameter Display System user’s position. Each reactor operator’s workstation contains the human system interface operator process displays. The senior

*NRC Staff approval is required prior to implementing a change in this information.

reactor operator has separate workstations that have the operator process displays. The wall panel information system is available to the main control room staff.

The AP1000 human system interface provides the status of the Safety Parameter Display System functions. The Safety Parameter Display System functions include:

- Reactivity control
- Reactor core cooling and heat removal from the primary system
- Reactor coolant system integrity
- Radioactivity control
- Containment conditions

The AP1000 alarm system provides overview alarms addressing the five Safety Parameter Display System functions. These overview alarms, integrated into the wall panel information system displays, are continuously displayed. Most of the safety parameters used to monitor the status of each Safety Parameter Display System function are continuously displayed on the wall panel information system displays. Those that are not continuously displayed on the wall panel are accessible at the operator's workstation. During the execution of emergency operating procedures, the AP1000 computerized procedure system provides a continuous display of the status of the critical safety functions.

Safety Parameter Display System-related information is physically displayed such that the information is readable from the reactor operator workstation. Each reactor operator's workstation contains the plant information system process displays. The control room supervisor (shift foreman) has an independent workstation that also has the process displays. The wall panel information system is available to the main control room staff.

18.8.2.3 Reliability

The AP1000 instrumentation and control (I&C) systems, including the human system interface, have reliability/availability design criteria. A description of the instrumentation and control system design features is found within Section 7.1.

The human system interface design includes the capability to build password or key-lock accessibility on the human system interface database. In addition, the system carries and displays data quality on the data in the system.

The alarm overviews integrated into the wall panel information system include indication of the operability of the alarm system itself.

18.8.2.4 Isolation

The Safety Parameter Display System as integrated into the overall human system interface is isolated from safety systems. Electrical isolation devices are discussed in Subsection 7.1.2.

18.8.2.5 Human Factors Engineering

Section 5 of Reference 28 presents the need for human-factors engineering in the design of the Safety Parameter Display System. The Safety Parameter Display System is designed using the implementation plan described in Subsection 18.8.1. [*This implementation plan includes the application of human factors engineering principles that address the criteria of the Human Factors Engineering Program Review Model (Reference 29).*]* This is also in accordance with Reference 48.

The AP1000 main control room and human system interface design reduces the number of individual computerized operator support systems by incorporating the requirements of the Safety Parameter

*NRC Staff approval is required prior to implementing a change in this information.

Display System into the design requirements for the AP1000 human system interface. This is accomplished primarily by those human system interface resources that produce and display the process abnormality alarms and the process graphical visual display units.

Parameter units of measure, labels, and abbreviations displayed by the human system interface resources are consistent with the units of measure, labels, and abbreviations included in the emergency operating procedures.

The human system interface displays information is in a form that does not require transformation or calculation. High- and low-level setpoints are consistent with the reactor protection system setpoints. The high- and low-level setpoints are visible in both the messages created by the AP1000 alarm system and on the indications, trends and graphs that appear as part of the process displays of the AP1000 plant information system.

Consistency of calculated values, such as subcooling margin, is maintained. The AP1000 instrumentation and control and human system interface architecture shares process data through a database.

The technical basis for software specifications are verified with plant data (for example, heat-up and cool-down limits, steam generator setpoints and high- and low-level alarm setpoints). The AP1000 human system interface is designed so that the plant data is a separate data file independent of the software specifications.

18.8.2.6 Minimum Information

The AP1000 human system interface resources used to address the Safety Parameter Display System requirements are the alarm system, plant information system, and the computerized procedure system. The AP1000 human system interface displays sufficient information to determine plant safety status with respect to the Safety Parameter Display System safety functions. [*The safety functions and respective parameters presented in Table 2 of Reference 32 are used as a starting point for the AP1000.*]* The human system interface design implementation plan is described in Subsection 18.8.1 and includes the integration of Safety Parameter Display System requirements into the human system interface. [*The Safety Parameter Display System design issue of "minimum information" is tracked by the human factors engineering issues tracking system.*]*

18.8.2.7 Procedures and Training

Sections 13.2 and 13.5 describe the development of training programs and plant procedures respectively. Reference 30 describes how training insights are passed from the designer to operations personnel who participate as subjects in the HFE V&V activities. Reference 31 provides input to the development of plant operating procedures.

18.8.3 Operation and Control Centers System

The human system interface includes the design of the operation and control centers system. The design of each of these control centers is conducted using the human system interface implementation plan presented in Subsection 18.8.1. The mission for each of the operation and control centers in the AP1000 is provided in the following subsections. Coupled with each mission statement is a brief description of the major tasks and design features that are supported by that center.

*NRC Staff approval is required prior to implementing a change in this information.

18.8.3.1 Main Control Room Mission and Major Tasks

The mission of the main control room is to provide a seismically qualified habitable and comfortable location for housing the resources for a limited number of humans to monitor and control the plant processes.

The major tasks performed in the main control room include monitoring, supervising, managing, and controlling those aspects of the plant processes related to the thermodynamic and energy conversion processes under normal, abnormal, and emergency conditions. Operating staff can monitor, supervise, manage, and control processes that have a real-time requirement for protecting the health and safety of operating personnel. The main control room supports the operator's decision-making process, and promotes the interaction with other plant personnel, while preventing distractions by non-operating personnel. The main control room provides the interfacing resources between the operation of the plant and the maintenance of the plant. Its areas include the main control area, the operations work area, the shift supervisor's office, and the operations break room (see Figure 1.2-8). Habitability systems are described in Sections 6.4 and 9.4.

18.8.3.2 Main Control Area Mission and Major Tasks

[*The mission of the main control area is to provide the support facilities necessary for the operators to monitor and control the AP1000 efficiently and reliably. Figure 6.4-1 provides a view of the main control area. The main control area includes the reactor operator workstations, the supervisor's workstation, the dedicated safety panel and the wall panel information system. The layout, size and ergonomics of the operator workstations and the wall panel information system depicted in this figure does not reflect the results of the human system interface design implementation plan*]* described in Subsection 18.8.1. The actual size, shape, ergonomics and layout of the operator workstations and the wall panel information system is an output of the implementation plan.

[*The major task of the main control area is to provide the human system interface resources that determine the plant state and implement the desired changes to the plant state during both normal and emergency plant operations. The main control area provides alarms to alert the operator to the need for further investigation. Plant process data displays permit the operator to observe abnormal conditions and identify the plant state. The controls enable the operator to execute actions. The process data displays and the alarms provide feedback to enable the operator to observe the effects of the control actions.*

Each reactor operator workstation contains the displays and controls to start up the plant, maneuver the plant, and shut down the plant.]* Reference 44 presents input for the determination of the staffing level of the operating crew in the main control room. [*Each workstation is designed to be manned by one operator. There is sufficient space and operator interface devices for two operators. The physical makeup of the reactor operator workstations is identical. The human system interface resources available at each workstation are:*

- *Plant information system displays*
- *Control displays (soft controls)*
- *Alarm system support displays*
- *Computerized procedure displays*
- *Screen and component selector controls*

The supervisor workstation is identical to the reactor operator workstations, except that its controls are locked-out. The supervisor workstation contains both internal plant and external plant communications systems.

*NRC Staff approval is required prior to implementing a change in this information.

Upon failure of a reactor operator workstation, the failed workstation is locked out, and the supervisor workstation controls are unlocked. This modified workstation configuration maintains independent, redundant workstations.

A dedicated safety panel is located in the main control area. The PMS safety displays and the dedicated safety system controls are provided in this panel. These visual display units are the only monitoring display devices in the main control room that are seismically qualified and provide the post-accident monitoring capabilities in accordance with Regulatory Guide 1.97. Dedicated system-level safety system control switches are located on the dedicated safety panel to provide the operators with safety system actuation capabilities.]* A minimum inventory of these dedicated displays and controls are presented in Section 18.12.

[*There is storage space for supplies, protective clothing and some spare parts. Cabinets are provided for necessary documents, and a drawing laydown area is provided for the operators' use. Restroom and kitchen facilities are provided for the main control room operations crew.*]*

18.8.3.3 Operations Work Area Mission and Major Tasks

The operations work area provides an area for personnel who support plant operations to work in close proximity to the main control area, but not in the main control area, in order to minimize distractions to the plant operators. Personnel in the operations work area can access plant data via one or more workstations to enable personnel to monitor the current state of systems, major components, and equipment. Additional support equipment may be provided as needed.

18.8.3.4 Remote Shutdown Workstation Mission and Major Tasks

[*The mission of the remote shutdown workstation is to provide the resources to bring the plant to a safe shutdown condition after an evacuation of the main control room. The remote shutdown workstation resources are based on an assumed evacuation of the main control room without an opportunity to accomplish tasks involved in the shutdown except reactor trip.*]* Subsection 7.4.3 discusses safe shutdown using the remote shutdown workstation, including design basis information.

18.8.3.5 Technical Support Center Mission and Major Tasks

The mission of the technical support center (TSC) is to provide an area and resources for use by personnel providing plant management and technical support to the plant operating staff during emergency evolutions. The TSC relieves the reactor operators of peripheral duties and communications not directly related to reactor system manipulations and prevents congestion in the control room. The Technical Support Center (TSC) location is described in the Emergency Plan.

Communications needs are established for the staff within the TSC, and between the TSC and the plant (including the main control room and operational support center), the emergency operations facility, the Combined License holder management, the outside authorities (including the NRC), and the public.

The design includes adequate shielding as discussed in Chapter 12. Adequate space, resources and access is provided for maintenance, emergency equipment and storage.

Consistent with NUREG 0737, the technical support center is nonsafety-related and is not required to be available after a safe shutdown earthquake.

The size of the TSC complies with the size requirements of Reference 28. [*The TSC complies with the habitability requirements of Reference 27 when electrical power is available.*]*

*NRC Staff approval is required prior to implementing a change in this information.

Should habitability be challenged within the TSC due to lack of cooling or a high radiation level resulting from a beyond-design-basis accident, the plant management function of the TSC is transferred to the main control room.

The EOF design is discussed in Chapters 13 and 18, including the specification of its location (Subsection 18.2.6) and emergency planning, and associated communication interfaces among the main control room, the TSC, and the EOF (Section 13.3).

Subsection 18.2.1.2 provides a description of assumptions and constraints, including utility requirements, that are used as inputs to the human factors engineering program and the human system interface design. As stated earlier under Section 18.8, the human system interface design includes the design of the operation and control centers system (main control room, TSC, remote shutdown room, emergency operations facility, local control stations and associated workstations) and each of the human system interface resources. The main control room design (environment, layout, number and design of workstations) supports emergency operations with a maximum crew compliment consisting of eleven individuals. These eleven include two individuals with senior reactor operator licenses, three with reactor operator licenses, one observer from the NRC, one from the plant owner's management and one communicator.

[*The design of the TSC's interfaces is included with the design of the human system interface.*]* Subsection 18.8.1 provides an implementation plan for the design of the human system interface. As shown in Figure 18.2-3, the results of the human factors engineering program elements are used as input and bases for developing the operation and control center system and human system interface resources functional design. This includes task analysis. Section 18.5 provides the implementation plan for the task analysis activities.

An uninterruptible power supply system provides approximately two hours of backup power supply to the TSC displays should ac power become unavailable.

18.8.3.6 Operations Support Center Mission and Major Tasks

The operations support center (OSC) is not within the scope of the human factors engineering program, but it is an emergency response facility. The mission of the operations support center is to provide a habitable area for operations support personnel and the resources to coordinate the assignment of duties and tasks to personnel outside of the main control room and the technical support center in support of plant emergency operation. The operations support center and the TSC are in different locations. The Operations Support Center (OSC) location is described in the Emergency Plan.

The major task of the operations support center is to provide a centralized area and the necessary supporting resources for the assembly of predesignated operations support personnel during emergency conditions. The operations support center provides the resources for communicating with the main control room and the technical support center. This permits personnel reporting to the operations support center to be assigned to duties in support of emergency operations.

18.8.3.7 Radwaste Control Area Mission and Major Tasks

The mission of the radwaste control area is to provide a habitable area and the appropriate resources for the operation of the radwaste processing systems. These resources include alarms, displays, controls, and procedures. These resources are located in a control area outside of the main control room.

*NRC Staff approval is required prior to implementing a change in this information.

18.8.3.8 Local Control Stations Mission and Major Tasks

The mission of local control stations is to provide the resources, outside of the main control room, the remote shutdown room, and the radwaste control area, for operations personnel to perform monitoring and control activities. The capability to access displays and controls (controls as assigned by the main control room operators) for local control and monitoring, from selected locations throughout the plant, is provided. Activities that are implemented through local control stations are reviewed to verify that their removal from the main control room is consistent with the operator staffing and performance considerations. Human system interface locations are provided for single task operations such as the operation of a manual valve.

18.8.3.9 Emergency Operations Facility

The design of the emergency operations facility, including specification of the location, in accordance with the AP1000 human factors engineering program, is discussed in Subsection 18.2.6.

18.8.4 Human Factors Design for the Non-Human-System Interface Portion of the Plant

18.8.4.1 General Plant Layout and Design

The AP1000 design process incorporates a human engineering approach to operations and maintenance. Maintainability design guidelines and human factors and as-low-as-reasonably-achievable (ALARA) checklists are used to meet the requirements of a human engineered environment. The design objectives include reducing worker exposure and eliminating unnecessary inspection and maintenance tasks.

18.8.4.1.1 Maintainability

Design features such as component selection, layout and standardization increase the probability that targeted repair times are achieved. These features coupled with a preventative maintenance program help the AP1000 meet its objectives for operation and maintenance. Design requirements from the utility industry and industry design practices establish criteria for layout, changeout, and replacement for parts and components; access for major pieces of equipment; and vehicle passage.

Critical path outage models are prepared for the AP1000. A typical refueling and maintenance outage schedule is used by design engineers. The model indicates maintenance windows for major outage events. Maintenance and testing of equipment and necessary plant operations (for example, refueling, heatup, and cooldown) are scheduled within the outage window.

18.8.4.1.2 Accessibility and Equipment Laydown Provisions

AP1000 maintainability design guidelines assist designers in identifying top-level layout requirements for equipment accessibility. Component engineers specify space requirements for routine maintenance, inservice inspection, testing and component replacement.

Frequency of inspection and maintenance dictates whether permanent platforms, ladders, and scaffolding are provided.

Overhead access is considered when equipment or tooling must be lifted into place or supported by a crane. Removable floor gratings and plugs are examples of features that provide overhead accessibility.

Permanent lifting devices are provided to enhance maintainability.

The use of robotics and automated devices are considered in the AP1000 design.

Robotic devices, such as refueling cavity decontamination units, are considered in the layout of the refueling cavity so that such interferences as light fixtures, tool hangers and personnel ladders are removable or do not affect the use of the robotic units.

Valve space enveloping drawings indicate the minimum space requirements. Equipment and module designers locate and arrange the valves to maintain the required space envelope.

The turbine-generator contains built-in features to increase accessibility for in-place inspection and maintenance. Access ports in the turbine housings allow routine inspections to be performed without dismantling the turbine casing. Laydown area is provided in the turbine building to access components and to allow for concurrent work.

18.8.4.1.3 Lighting

The AP1000 normal and emergency lighting system is designed to provide illumination levels required for the safe performance of plant operation under normal and emergency conditions.

18.8.4.1.4 Radiation Protection and Safety

The AP1000 design process incorporates radiation exposure reduction principles to keep worker dose ALARA. ALARA checklists are used in design evaluations. Exposure length, distance, shielding, and source reduction are the fundamental criteria incorporated into the design process.

Design features such as readily detachable insulation, as-built smooth surfaces for non-destructive examination, and “modular type” replacement components reduce worker time in radiation areas.

The large AP1000 containment vessel provides laydown space to transfer subcomponents to storage areas until needed. The reactor head is remotely located on the operating deck to reduce background radiation to refueling personnel.

Provisions for remotely operated tooling are considered during the design process. Space is provided to clean and inspect the reactor vessel O-ring grooves using a remotely operated device. Remotely controlled radiation and surveillance equipment is considered for high radiation areas.

Special provisions for radiation shielding are included in the AP1000 design. Permanent shielding built into the integrated head package reduces worker exposure resulting from the incore instrumentation operation.

Material selection and surface conditioning are important elements in radiation exposure reduction. Electropolishing of surfaces exposed to reactor coolant primary water is considered to reduce crud deposits and aid in decontamination.

The AP1000 radioactive waste processing facilities are designed to concentrate radioactive waste processing and drumming activities in remote areas to reduce contact with the majority of plant personnel.

18.8.4.1.5 Communication

The AP1000 communication system provides voice communication during normal operations, plant outages, and emergency operations. The system includes broadcast of alarm signals in plant-wide emergency situations. The wireless telephone system enables plant personnel to remain in direct communication via wireless, hand-carried telephones throughout the plant. Headset-style telephones

are available for individuals requiring hands-free operation. Some communication devices have built-in compatibility with protective clothing including respirators.

A paging system is used as a backup to the wireless telephone system. In the event of a failure of the wireless system, personnel communicate via a plant-wide broadcast and five party lines. Emergency broadcasts are announced through this system.

Communication during AP1000 refueling and maintenance outages is enhanced by a sound-powered communication system. Refueling, maintenance, and cold shutdown loops are provided. Jacks are placed in locations where plant personnel are located during these activities.

A private branch exchange system is capable of duplex voice communication between stations. These telephones are placed in acoustic booths in those areas having high ambient noise levels to improve user interface. See Subsection 9.5.2 for information on the communication system.

18.8.4.1.6 Temperature, Humidity, Ventilation

Radioactive and nonradioactive ventilation systems are provided in required areas. The ventilation systems are designed to control the environment within the plant and to protect the environment outside the plant. Requirements for temperature, humidity, and ventilation vary, depending on work location, frequency of use, and work description.

18.8.4.1.7 Emergency Equipment

Emergency equipment for treatment of injured personnel is placed in appropriate locations. Provisions for emergency equipment are considered during plant layout.

18.8.4.1.8 Storage

Storage facilities are identified in the AP1000. Radioactively clean and contaminated storage areas are designated.

18.8.4.1.9 Coding and Labeling

Equipment located in the AP1000 has a unique identifier and plant descriptive name. The configuration management system includes the identification of the equipment in the plant. Each component is assigned an identifier during the design process. The identifier is maintained through manufacturing, construction, and operation. The components are labeled according to the assigned identifier. These labels help avoid errors in operating or working on the wrong equipment and in reporting problems or conditions observed in the plant. The labels help reduce the training burden for operating and maintenance personnel.

Color, syntax, abbreviations and symbols are consistently applied. The labels are located in an easily visible location on the component and are not hidden by insulation, equipment covers, or surrounding equipment. Labels are fastened to the component to prevent easy detachment of the label.

18.8.5 Combined License Information

The execution and documentation of the human system interface design implementation plan that is presented by Section 18.8 is addressed in APP-GW-GLR-082 (Reference 47), and the applicable changes are incorporated into the UFSAR.

18.8.6 References

1. APP-OCS-J1-002, “AP1000 Human System Interface Design Guidelines,” (Westinghouse Proprietary).

2. CEI/IEC 964, “Design for Control Rooms of Nuclear Power Plants,” International Electrotechnical Commission, Geneva, Switzerland, 1989.

3. IEEE Std 1023-2004, “IEEE Recommended Practice for the Application of Human Factors Engineering to Systems, Equipment and Facilities of Nuclear Power Generating Stations and Other Nuclear Facilities.”

4. IEEE Std 1289-1998, “IEEE Guide for the Application of Human Factors Engineering in the Design of Computer-Based Monitoring and Control Displays for Nuclear Power Generating Stations.”

5. NUREG-0700, “Human-System Interface Design Review Guideline,” Rev. 2, U.S. Nuclear Regulatory Commission, Washington, D.C., May 2002.

6. Not used.

7. NUREG/CR-6105, “Human Factors Engineering Guidelines for the Review of Advanced Alarm Systems,” U.S. Nuclear Regulatory Commission, Washington, D.C., September 1994.

8. MIL-STD-1472, Department of Defense Design Criteria Standard: Human Engineering, Revision F, August 1999.

9. NUREG/CR-6634, “Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance,” U.S. Nuclear Regulatory Commission, Washington, D.C., March 2000.

10. AP600 Document Number OCS-J1-008, “Effects of Control Lag and Interaction Mode on Operators’ Use of Soft Controls,” Revision 0, September 1994.

11. Hoecker, D. G. and Roth, E. M., “Man-Machine Design and Analysis System (MIDAS) Applied to a Computer-Based Procedure-Aiding System,” Westinghouse STC Report 1SW5-CHICR-P2, May 25, 1994; also in “Proceedings of the Human Factors and Ergonomics Society 35th Annual Meeting,” October 1995.

12. Hoecker, D. G. and Roth, E. M., “MIDAS in the Control Room: Applying a Flight Deck Cognitive Modeling Tool to Another Domain,” Westinghouse STC Report 1SW5-CHICR-P3, September 26, 1994; also in RAF Institute of Research and Development, “Proceedings of the Third International Workshop on Human-Computer Teamwork,” Cambridge, UK, September 26, 1994.

13. Roth, E. M. and Hoecker, D. G., “Human Factors Issues Associated with Soft Controls: Design Goals and Available Guidance,” 1994.

14. Beranek, L. L., “Revised Criteria for Noise in Buildings,” Noise Control, Vol. 3, Nr.1, p. 19ff.

15. Grandjean, E., “Fitting the Task to the Man: An Ergonomic Approach,” London: Taylor and Francis Ltd., 1981.

16. Van Cott and Kinkade, “Human Engineering Guide to Equipment Design,” Washington D.C.: U.S. Government Printing Office, 1972.

17. Electric Power Research Institute, “Human Factors Guide for NPP Control Room Development,” Final Report on Project 1637-1. EPRI NP-3659, 1984.

18. Electric Power Research Institute, “Advanced Light Water Reactor Utility Requirements Document, Vol. III. ALWR Passive Plant, Chapter 10: Man-Machine Interface Systems,” Revision 6, December 1993.

19. International Electrotechnical Commission, “Design for Control Rooms of Nuclear Power Plants,” IEC Standard 964, 1989.

20. International Electrotechnical Commission, “Operating Conditions for Industrial-Process Measurement and Control Equipment,” IEC Standard 654-1, 1979.

21. Proctor, D. H. and Hughes, J. P., “Chemical Hazards of the Workplace,” 1978.

22. 29CFR1910, “Occupational Safety and Health Standards,” 1975.

[*23. WCAP-14651, “Integration of Human Reliability Analysis With Human Factors Engineering Design Implementation Plan,” Revision 2, May 1997.*]*

[*24. WCAP-15860, “Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan,” Revision 2, October 2003.*]*

[*25. WCAP-14695, “Description of the Westinghouse Operator Decision Making Model and Function Based Task Analysis Methodology,” Revision 0, July 1996.*]*

[*26. 10 CFR 50.34 (f) (2) (iv).*]*

[*27. NUREG-0737, Supplement 1; “Requirements for Emergency Response Capability.”*]*

28. NUREG-0696, “Functional Criteria For Emergency Response Facilities.”

[*29. NUREG-0711, “Human Factors Engineering Program Review Model,” U.S. NRC, July 1994.*]*

30. WCAP-14655, “Designer’s Input for the Training of the Human Factors Engineering Verification and Validation Personnel,” Revision 1, August 1996.

31. WCAP-14690, “Designer’s Input to Procedure Development for the AP600,” Revision 1, June 1997.

[*32. NUREG-1342, “A Status Report Regarding Industry Implementation of Safety Parameter Display Systems.”*]*

33. Rasmussen, J., 1986, “Information Processing and Human-Machine Interaction, An Approach to Cognitive Engineering,” (New York, North-Holland).

34. O’Hara, J. M. and Wachtel, J., 1991, “Advanced Control Room Evaluation: General Approach and Rationale” in “Proceedings of the Human Factors 35th Annual Meeting,” pp. 1243-1247, (Santa Monica, CA, Human Factors Society).

*NRC Staff approval is required prior to implementing a change in this information.

35. Woods, D. D. and Roth, E. M., 1988, “Cognitive Systems Engineering,” Helander, M. (ed.), “Handbook of Human-Computer Interaction,” pp. 3-43, (New York, NY, Elsevier Science Publishing Co., Inc.).

36. Woods, D. D., Wise, J. A., and Hanes, L. F., 1982, “Evaluation of Safety Parameter Display Concepts,” NP-2239, (Palo Alto, CA, Electric Power Research Institute).

37. Woods, D. D. and Roth, E. M., 1986, “The Role of Cognitive Modeling in Nuclear Power Plant Personnel Activities,” NUREG-CR-4532, Volume 1, (Washington, D.C., U.S. Nuclear Regulatory Commission).

38. Woods, D. D., Roth, E. M., Stubler, W. F., and Mumaw, R. J., 1990, “Navigating Through Large Display Networks in Dynamic Control Applications” in “Proceedings of the Human Factors Society 34th Annual Meeting,” pp. 396-399, (Santa Monica, CA, Human Factors Society).

39. Reason, J. T., 1990, “Human Error,” (Cambridge, UK, Cambridge University Press).

40. Stubler, W. F., Roth, E. M., and Mumaw, R. J., 1991, “Evaluation Issues for Computer-Based Control Rooms” in “Proceedings of the Human Factors Society 35th Annual Meeting,” pp. 383-387, (Santa Monica, CA, Human Factors Society).

41. Woods, D. D., 1982, “Application of Safety Parameter Display Evaluation Project to Design of Westinghouse Safety Parameter Display System,” Appendix E to “Emergency Response Facilities Design and V & V Process,” WCAP-10170, submitted to the U.S. Nuclear Regulatory Commission in support of their review of the Westinghouse Generic Safety Parameter Display System Non-Proprietary, (Pittsburgh, PA, Westinghouse Electric Corp.).

42. Not used.

43. American National Standards Institute, 1988, “ANSI/HFS 100-1988, American National Standard for Human Factors Engineering of Visual Display Terminal Workstations,” (Santa Monica, CA, Human Factors Society, American National Standards Institute).

44. WCAP-14694, “Designer’s Input to Determination of the AP600 Main Control Room Staffing Level,” Revision 0, July 1996.

45. AP1000 Probabilistic Risk Assessment.

[*46. WCAP-14396, “Man-in-the-Loop Test Plan Description,” Revision 3, November 2002.*]*

47. APP-GW-GLR-082, “Execution and Documentation of the Human System Interface Design Implementation Plan,” Westinghouse Electric Company LLC.

48. NUREG-0711, Revision 2, “Human Factors Engineering Program Review Model,” U.S. NRC, February 2004.

*NRC Staff approval is required prior to implementing a change in this information.

Table 18.8-1 (Sheet 1 of 2)
[*HUMAN PERFORMANCE ISSUES TO BE ADDRESSED BY THE HSI DESIGN*]*

Operator Activity: Detection and Monitoring
Issue 1: Do the wall panel information system and the workstation summary and overview displays support the operator in maintaining an awareness of plant status and system availability without needing to search actively through the workstation displays?
Issue 2: Does the wall panel information system support the operator in getting more detail about plant status and system availability by directed search of the workstation functional and physical displays?
Issue 3: Do the HSI features support efficient navigation to locate specific information?
Issue 4: Do the HSI features effectively support crew awareness of plant condition?
Operator Activity: Interpretation and Planning
Issue 5: Does the alarm system convey information in a way that enhances operator awareness and understanding of plant condition?
Issue 6: Does the physical and functional organization of plant information on the workstation displays enhance diagnosis of plant condition and the planning/selection of recovery paths?
Issue 7: Does the integration of alarms, wall panel information system, workstation, and procedures support the operator in responding to single-fault events?
Issue 8: Does the integration of alarms, wall panel information system, workstation and procedures support the operator in interpretation and planning during multiple-fault events?
Issue 9: Does the integration of alarms, wall panel information system, workstation and procedures support the crew in interpretation and planning during multiple-fault events?
Issue 10: Does the integration of alarms, wall panel information system, workstation, and procedures support the crew in interpretation and planning during severe accidents?

*NRC Staff approval is required prior to implementing a change in this information.

Table 18.8-1 (Sheet 2 of 2)
[*HUMAN PERFORMANCE ISSUES TO BE ADDRESSED BY THE HSI DESIGN*]*

Operator Activity: Controlling Plant State
Issue 11: Do the HSI features support the operator in performing simple, operator-paced control tasks?
Issue 12: Do the HSI features support the operator in performing control tasks that require assessment of preconditions, side effects and post-conditions?
Issue 13: Do the HSI features support the operator in performing control tasks that require multiple procedures?
Issue 14: Do the HSI features support the operator in performing event paced control tasks?
Issue 15: Do the HSI members features support the operator in performing control tasks that require coordination among crew?

*NRC Staff approval is required prior to implementing a change in this information.

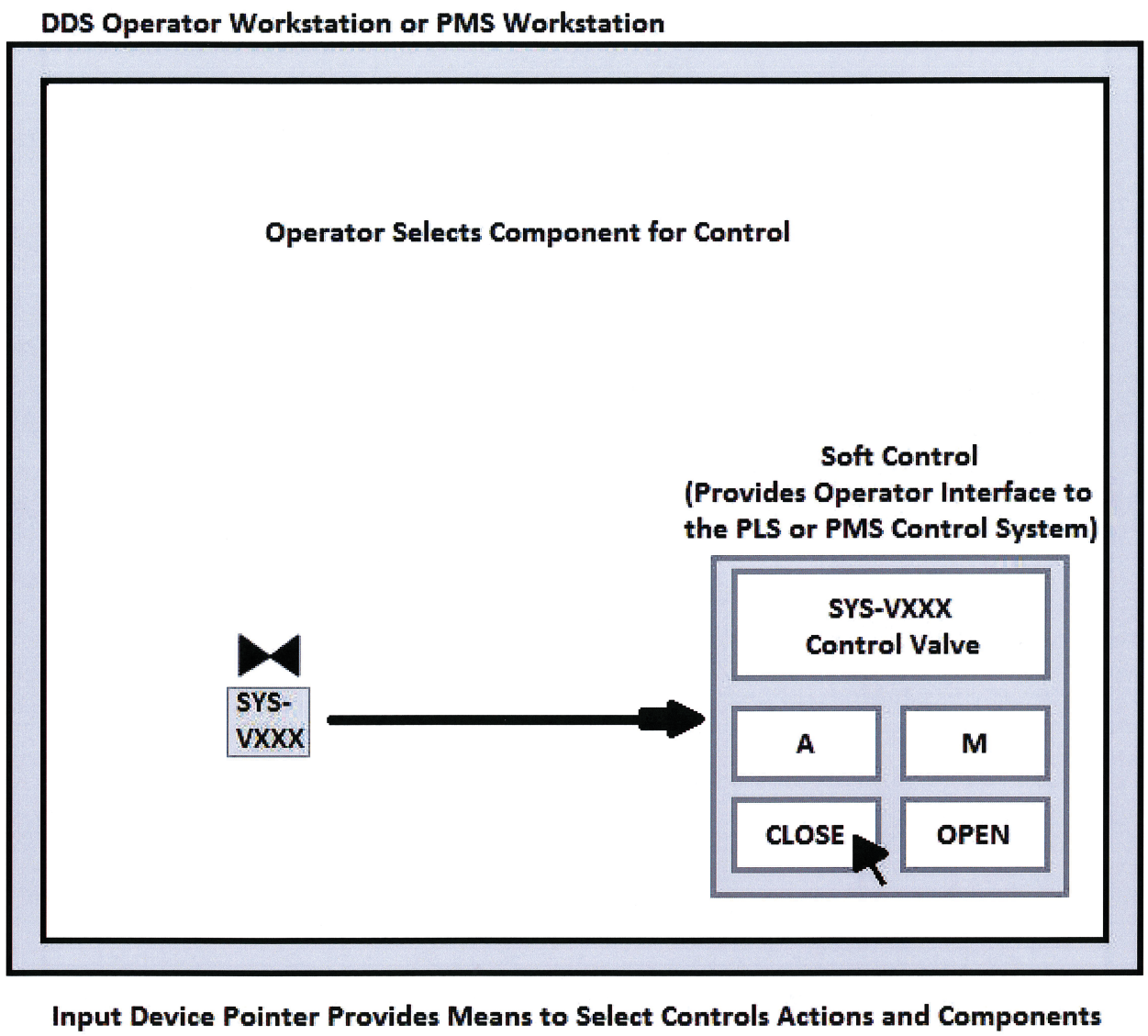


Figure 18.8-1
Soft Control Interactions

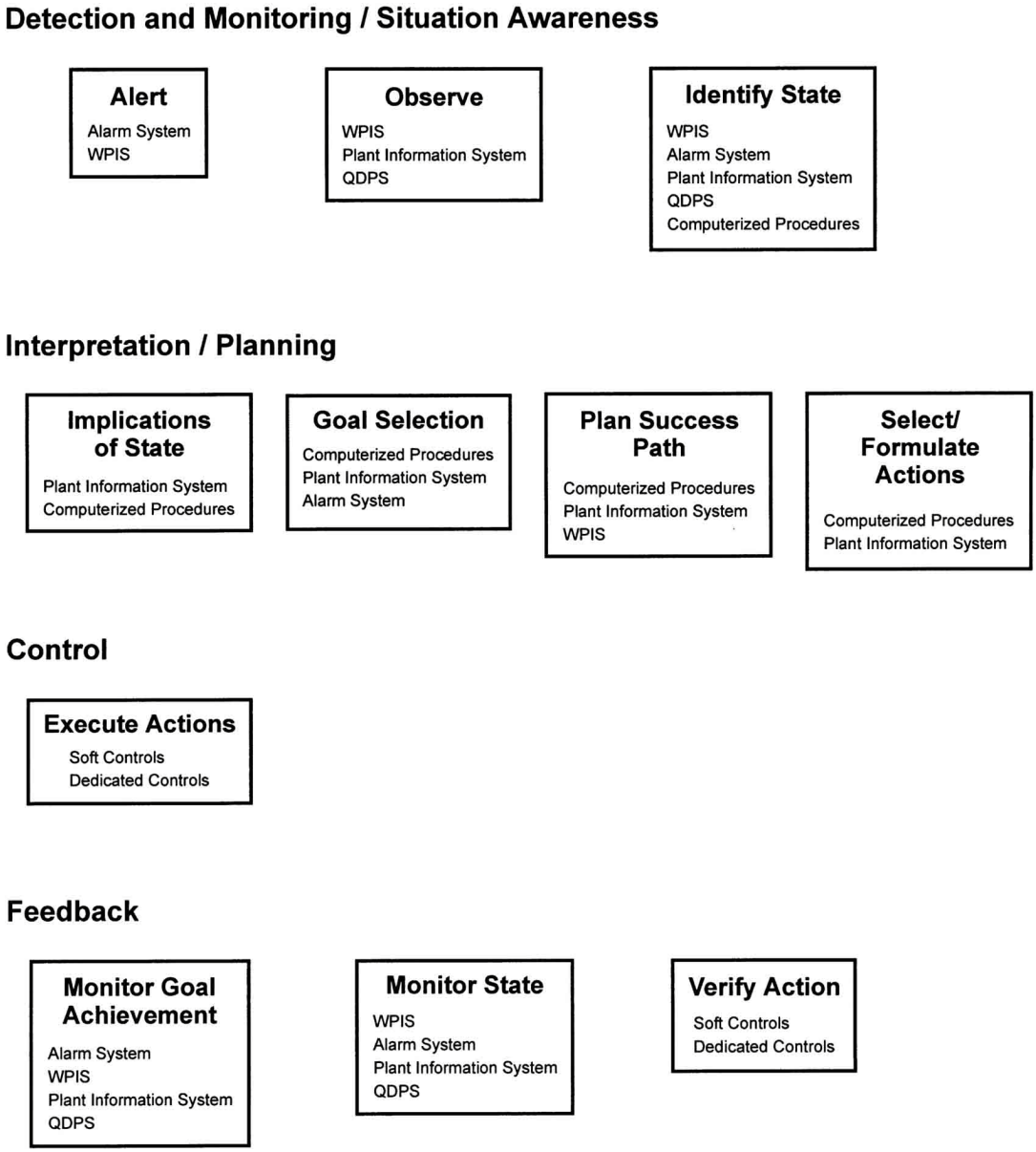


Figure 18.8-2
Mapping of Human System Interface Resources to Operator Decision-Making Model

18.9 Procedure Development

WCAP-14690, "Designer's Input to Procedure Development for the AP600" (Reference 1), provides input for the development of plant operating procedures, including information on the development and design of the AP600 emergency response guidelines and emergency operating procedures. It applies directly to AP1000 since AP1000 is operated in the same manner as AP600. The WCAP also includes information on the computerized procedure system, which is the human system interface through which operators execute the plant procedures.

18.9.1 Combined License Information

The responsibility for procedure development is addressed in APP-GW-GLR-040 (Reference 2), and the applicable changes are incorporated into the UFSAR.

18.9.2 References

1. WCAP-14690, "Designer's Input to Procedure Development for the AP600," Revision 1, June 1997.

2. APP-GW-GLR-040, "Plant Operations, Surveillance, and Maintenance Procedures," Westinghouse Electric Company LLC.

18.10 Training Program Development

WCAP-14655, "Designer's Input to the Training of the Human Factors Engineering Verification and Validation Personnel" (Reference 1), describes the design and implementation of the training program for the training of the operations personnel who participate as subjects in the Human Factors Engineering (HFE) Verification and Validation. The WCAP also describes the process used to develop the specification of the role of the operator for AP1000 and how this role and training insights can be passed from the designer to the developer of the training program.

Information regarding training program development is located in Section 13.2, Training. The training organization and roles and responsibilities of training personnel are discussed in Section 13.1, Organizational Structure of Applicant.

18.10.1 Combined License Information

The responsibility for training program development is addressed in Sections 18.10, 13.1, and 13.2.

18.10.2 References

1. WCAP-14655, "Designer's Input to the Training of the Human Factors Engineering Verification and Validation Personnel," Revision 1, August 1996.

18.11 Human Factors Engineering Verification and Validation

A programmatic level description of the AP1000 human factors engineering verification and validation program is provided by Reference 1. Using the programmatic level description, the development of an implementation plan for the AP1000 human factors engineering verification and validation is executed and documented as discussed in Reference 2. The implementation of the verification and validation activities is detailed in the five documents References 3 to 7.

The verification and validation activities are in accordance with Reference 1. There are a number of exceptions in respect to human factors engineering verification and validation. The details of these exceptions and the corresponding justifications are provided in References 3 to 5.

18.11.1 Combined License Information

The development, execution and documentation of an implementation plan for the verification and validation of the AP1000 human factors engineering program is addressed in Reference 2 (APP-GW-GLR-084).

18.11.2 References

[1. *WCAP-15860 , "Programmatic Level Description of the AP1000 Human Factors Verification and Validation Plan," Revision 2, October 2003.*]*

2. APP-GW-GLR-084, "AP1000 Human Factors Engineering Verification and Validation," Westinghouse Electric Company LLC.

[3. *APP-OCS-GEH-120, "AP1000 Human Factors Engineering Design Verification Plan,"*]* Revision 3, Westinghouse Electric Company LLC.(1)

[4. *APP-OCS-GEH-220, "AP1000 Human Factors Engineering Task Support Verification Plan,"*]* Revision 4, Westinghouse Electric Company LLC.(2)

[5. *APP-OCS-GEH-320, "AP1000 Human Factors Engineering Integrated System Validation Plan,"*]* Revision 6, Westinghouse Electric Company LLC.(3)

[6. *APP-OCS-GEH-420, "AP1000 Human Factors Engineering Discrepancy Resolution Process,"*]* Revision 2, Westinghouse Electric Company LLC.(4)

[7. *APP-OCS-GEH-520, "AP1000 Plant Startup Human Factors Engineering Design Verification Plan,"*]* Revision 4, Westinghouse Electric Company LLC.(5)

Notes:

1. [*Section 1, Section 2, and Section 3 of APP-OCS-GEH-120 are Tier 2*. Changes to these portions of the document require prior NRC approval.*]* The remainder of the document, including its revision number, is Tier 2.

2. [*Section 1, Section 2, Section 3, Section 4, and Section 5 of APP-OCS-GEH-220 are Tier 2*. Changes to these portions of the document require prior NRC approval.*]* The remainder of the document, including its revision number, is Tier 2.

3. [*Section 1, Section 2, Section 3, Section 4, Section 5, Section 6, and Section 7 of APP-OCS-GEH-320 are Tier 2*. Changes to these portions of the document require prior NRC approval.*]* The remainder of the document, including its revision number, is Tier 2.

*NRC Staff approval is required prior to implementing a change in this information.

4. [*Section 1 and Section 2 of APP-OCS-GEH-420 are Tier 2*. Changes to these portions of the document require prior NRC approval.*]* The remainder of the document, including its revision number, is Tier 2.

5. [*Section 1, Section 2, and Section 3 of APP-OCS-GEH-520 are Tier 2*. Changes to these portions of the document require prior NRC approval.*]* The remainder of the document, including its revision number, is Tier 2.

*NRC Staff approval is required prior to implementing a change in this information.

Figure 18.11-1 Not Used
(See Reference 5, Figure 1.1-1, "AP1000 Verification and Validation Activities.")

18.12 Inventory

18.12.1 Inventory of Displays, Alarms, and Controls

[*An inventory of instruments, alarms, and controls for the AP1000 systems is provided in the respective system piping and instrumentation diagrams and/or the respective system specification documents.*

The AP1000 system design engineers determine the specific sensors, instrumentation, controls, and alarms that are needed to operate the various plant systems. The instruments, alarms, and controls for each system are documented in the piping and instrumentation diagram and/or the respective system specification documents. An instrument, alarm, and control is specified by the system design engineer if it is needed to control, verify, or monitor the operation of the system and its components. System functions and their respective functional requirements are considered by the system designer when determining the need for a specific instrument, alarm, or control.

The role of the Human System Interface design team in the determination of the total inventory list is one of verification. As described in Section 18.5, human system interface design team has functionally decomposed the plant. The top four levels of this model for the AP1000 are shown in Figure 18.5-1. Each Level 4 function has a function-based task analysis (FBTA) performed as described in the Task Analysis Implementation Plan. Considering the plant operating modes and emergency operations, the function-based task analysis:

- *Identifies the functions goals*
- *Identifies the processes used to achieve each goal*
- *Documents the performance of a cognitive task analysis of each process*

The cognitive task analysis of each process answers the monitoring/feedback, planning, and controlling questions. The answers to these questions identify the data for each functional process (instrumentation, indications, alarms, and controls) needed by the operator to make decisions. The results of the cognitive task analysis phase of each function-based task analysis are used to verify the inventory list of instruments, controls, and alarms developed by the AP1000 system designers and documented in the respective design documents.]*

18.12.2 Minimum Inventory of Main Control Room Fixed Displays, Alarms, and Controls

Background

[The human system interface design includes the appropriate plant displays, alarms, and controls needed to support a broad range of expected power generation, shutdown, and accident mitigation operations. Soft control displays and plant information displays are generated by a computer and can be changed to perform different functions, allow control of different devices, or display different information. These displays appear on display devices such as cathode ray tubes, flat panel screens, or visual display units. Alarms are used to direct operator attention. Soft controls are provided through devices such as a keyboard, touch screen, mouse, or other equivalent input devices. The majority of the operations for both the AP1000 main control room and the remote shutdown workstation are expected to employ soft control displays and plant information displays.

The AP1000 human system interface design also includes a minimum inventory of dedicated or fixed-position displays and controls. The minimum inventory of AP1000 fixed-position instrumentation includes those displays, controls, and alarms that are used to monitor the status of critical safety functions and to manually actuate the safety-related systems that achieve these critical safety functions.

*NRC Staff approval is required prior to implementing a change in this information.

Fixed-position alarms and displays are available at a fixed location and are continuously available, though not necessarily displayed, to the operator. Fixed-position displays can be accessed by the operator to monitor the plant status, based on indications from critical plant variables or parameters. Fixed-position alarms are designed to direct operator attention to the need to perform safety-related functions for which there is no automatic actuation function. Although not continuously displayed, the fixed-position displays and alarms are quickly and easily retrievable.

Fixed-position controls provide a means for manual reactor and turbine trip, and safety-related system/component actuation. Fixed-position controls are available to the operator to perform tasks in the operation of safety-related systems and components used to mitigate the consequences of an accident and to establish and maintain safe shutdown conditions following an accident. The fixed-position controls are a manual backup to the automatic protection signals provided by the protection and safety monitoring system.]*

Design Basis and Minimum Inventory

[*A systematic process was implemented to identify the minimum inventory of AP1000 fixed-position controls, displays, and alarms, using established selection criteria directly related to the specific AP1000 accident mitigation operator actions and the critical safety functions identified in the emergency response guidelines.*

The AP1000 design basis for accident mitigation protects the following three fission product barriers:

- *Fuel matrix/fuel rod cladding*
- *Reactor coolant system pressure boundary*
- *Containment*

Therefore, the minimum inventory of fixed instrumentation includes those displays, controls, and alarms used to monitor the status of these fission product barriers and manually actuate the safety-related systems that achieve the critical safety functions protecting these barriers.

Six critical safety functions are identified in the Emergency Response Guidelines (ERGs). These critical safety functions are physical processes, conditions, or actions designed to maintain the plant conditions within the acceptable design basis.

The AP1000 critical safety functions are:

- *Reactivity control*
- *Reactor core cooling*
- *Heat sink maintenance*
- *Reactor coolant system integrity*
- *Containment environment*
- *Reactor coolant system inventory control*

The minimum inventory of AP1000 fixed instrumentation includes those displays, controls, and alarms that are used to monitor the status of these critical safety functions and to manually actuate the safety-related systems that achieve these critical safety functions.]*

Minimum Inventory Selection Criteria

[*The following selection criteria are used to develop the minimum inventory of instrumentation controls, displays, and alarms:*

- *Regulatory Guide 1.97 Types A, B, and C, Category 1 instrumentation*

*NRC Staff approval is required prior to implementing a change in this information.

- *Dedicated controls for manual safety-related system actuation (reactor trip, turbine trip, engineered safety feature actuation)*
- *Controls, displays, and alarms required to perform critical manual actions as identified from the PRA analysis*
- *Alarms provided for operator use in performing safety functions to respond to design basis events for which there is no automatically-actuated safety function*
- *Controls, displays, and alarms necessary to maintain the critical safety functions and safe shutdown conditions*

For the main control room, the minimum inventory of displays is provided by the PMS safety displays. For the remote shutdown workstation, the minimum inventory of displays is provided by the nonsafety-related displays of the plant information system.

An alarm is a device that provides warning by means of a signal or sound. The parameters and associated alarms, listed in DCD Table 18.12.2-1, identify challenges to the critical safety functions. This minimum inventory of alarms is embedded in displays as visual signals. For example, the visual signal may involve a change of color, brightness, flashing, or a combination of these. For clarity, these alarms are called visual alerts to distinguish them from other alarms which may include sound. For the main control, the visual alerts are embedded in the safety-related displays. For the remote shutdown workstation, the visual alerts are embedded in the nonsafety-related displays.

*The minimum inventory resulting from the implementation of these selection criteria is provided in Table 18.12.2-1.]**

Regulatory Guide 1.97

[*The guidelines in Regulatory Guide 1.97 provide an effective basis for selection criteria to identify the minimum inventory of fixed displays, controls, and alarms, since these guidelines are consistent with monitoring the status of the fission product barriers and the associated critical safety functions in the AP1000 Emergency Response Guidelines.*

Regulatory Guide 1.97 provides a method to identify the post-accident monitoring (PAMS) instrumentation to monitor plant variables and systems during and following an accident. Selected post-accident monitoring instrumentation is required to remain functional over the range of the accident conditions and must be able to survive the accident environment for the length of time its function is required. The instrumentation helps the operator to identify the accident, to implement proper corrective actions, and to observe plant response to these actions in order to determine the need for additional actions. Five types of accident monitoring instrumentation and associated performance criteria are provided in the regulatory guide.

Within each type of post-accident monitoring instrumentation, there are three categories (Categories 1, 2, and 3) that are related to the qualification (seismic and environmental conditions) and reliability (safety-related power supply and single failures) of the specific instrumentation.

The Category 1 variables are considered as primary variables and meet appropriate qualification, design, and interface requirements discussed in subsection 7.5.2.2.1 and listed in Tables 7.5-2 and 7.5-3. These variables provide the appropriate capabilities and reliability that are required for the parameters. Only the Category 1 (primary) variables are included in the minimum inventory selection criteria. Category 2 and Category 3 instrumentation are not included in the selection criteria for the minimum inventory.

*NRC Staff approval is required prior to implementing a change in this information.

Type A, Type B, and Type C are considered in developing the selection criteria for identification of the minimum inventory, since these three types are related to monitoring the three fission product barriers. The details of instrumentation designed to meet the guidelines in Regulatory Guide 1.97 are presented in Section 7.5.

Type A variables are defined in subsection 7.5.2.1. As discussed in subsection 7.5.3.1, Type A variables provide primary information to permit the main control room operating staff to:

- *Perform the diagnosis in the AP1000 emergency operating procedures*
- *Take specified preplanned, manually-controlled actions, for which automatic controls are not provided, and that are required for safety-related systems to accomplish their safety-related function to recover from a design basis accident*

There are no specific, preplanned, manually-controlled actions for safety-related systems to recover from design basis events in the AP1000 design. Therefore, as reflected in Table 7.5-4, there are no Type A variables.

Type B variables are defined in subsection 7.5.2.1. As discussed in subsection 7.5.3.2, Type B variables provide information to the main control room operating staff to assess the process of accomplishing critical safety functions in the emergency response guidelines. The Type B variables are identified in Table 7.5-5.

Type C variables are defined in subsection 7.5.2.1. As discussed in subsection 7.5.3.3, Type C variables provide the control room operating staff with information to monitor the potential for breach or the actual gross breach of:

- *Incore fuel cladding*
- *Reactor coolant system boundary*
- *Containment boundary*

The Type C variables are identified in Table 7.5-6.]*

Dedicated Controls

[*The selection criteria of AP1000 minimum inventory include dedicated, fixed-position controls that provide the capability to manually initiate system-level actuation signals for the safety-related systems and components that are used to achieve the critical safety functions. These dedicated controls provide the capability to initiate manual reactor and turbine trip, safeguards actuation, individual actuation of various safety-related, passive components and containment isolation.*]*

Probabilistic Risk Assessment Critical Human Actions

[*As described in Section 18.7 and Reference 1, the human factors engineering design process includes integration of PRA and the associated human reliability analysis insights into the AP1000 design. The human reliability analysis integration includes the identification of critical human actions through the consideration of specific deterministic and PRA criteria. These selection criteria for minimum inventory identify dedicated, fixed-position displays, alarms, and controls required to support critical human actions identified from the integration of human reliability analysis into the human factors engineering design process.*]*

Dedicated Alarms

[*As specified by Criterion 1, the minimum inventory of instrumentation requires dedicated instrumentation displays of the Regulatory Guide 1.97 Type A variables so that the operator can identify the need to take preplanned manually-controlled actions to mitigate the consequences of a*

*NRC Staff approval is required prior to implementing a change in this information.

design basis event, where a safety-related system needed to support a critical safety function is not automatically actuated.

The fourth criterion for minimum inventory is included to identify alarms needed to automatically alert the operator to the need to take these preplanned manually controlled actions.

One of the design goals of the AP1000 is to minimize the need for operator actions to mitigate the consequences of design basis events. As part of the implementation of this design goal, the safety-related systems required to mitigate the consequences of design basis events are automatically actuated. There are no specific preplanned, manually-controlled actions required for the safety-related systems to mitigate design basis events in the AP1000 design.

Another design goal for the AP1000 is to enhance defense in depth, which includes the use of automatically actuated safety-related systems as a backup to other automatically actuated safety-related systems. For example, if beyond-design-basis failures occurred such that the safety-related passive residual heat removal heat exchanger failed to actuate, other safety-related systems would automatically actuate to provide core cooling, without the need for operator action for either group of safety-related components. This design approach enhances overall plant safety.

The AP1000 minimum inventory includes a criterion for evaluating the need for dedicated alarms for preplanned operator actions. However, as a result of these two design approaches, the level of protection available to mitigate the consequences of an accident and to achieve the critical safety functions is provided without the need for preplanned operator actions for either the primary safety-related systems or the backup safety-related systems. Since there are no specific preplanned, manually-controlled actions for safety-related systems required to respond to design basis events in the AP1000 design, there are also no dedicated, fixed-position alarms identified in the minimum inventory list.]*

Critical Safety Functions and Safe Shutdown

[*The design basis for the AP1000 requires protecting the three fission product barriers in the plant (the fuel matrix and cladding, the reactor coolant system pressure boundary, and containment) following design basis events. The AP600 system/event matrix (Reference 2) identifies four safety-related, post-accident mitigation functions that are required as part of the design basis for the AP600 to protect the integrity of these fission product barriers. This document is directly applicable to AP1000. The design basis of the AP1000 requires safety-related systems that can perform these four safety-related functions for design basis events.*

The AP1000 Emergency Response Guidelines were developed by using the system/event matrix document as the plant response design basis and following the standardized process for Emergency Response Guideline development for Westinghouse PWRs. The design approach described in the system/event matrix document organizes the identified safety-related and nonsafety-related Systems, structures and components into the appropriate groups that perform the four safety-related design basis functions. In developing the AP1000 Emergency Response Guidelines, the same groups of safety-related and nonsafety-related systems in the system/event matrix are used to perform their basic design functions, but they are organized somewhat differently from the system/event matrix to support development of symptom-based functional guidelines that can be more effectively used by the operators. These four design basis safety functions identified in (Reference 2) are expanded into the six critical safety functions in writing the symptom-based AP1000 Emergency Response Guidelines.

The six Emergency Response Guidelines critical safety functions (and the four design basis safety functions that the critical safety functions must satisfy) are physical processes, conditions, or actions taken using the safety-related and nonsafety-related systems to maintain the plant conditions within

*NRC Staff approval is required prior to implementing a change in this information.

the acceptable design basis. These systems provide the physical equipment used to initiate and control the processes that achieve the critical safety functions.

By accomplishing the emergency response guideline critical safety functions following a design basis event, the plant is able to mitigate the consequences of the event and to establish and maintain safe shutdown conditions. The minimum inventory list identifies sufficient controls, displays, and alarms to monitor and control operation of the safety-related systems to achieve the six critical safety functions identified in the Emergency Response Guidelines and to establish and maintain safe shutdown conditions following an accident.

Tables 7.5-4, 7.5-5, and 7.5-6 identify the instrumentation and the associated Emergency Response Guidelines critical safety functions that each instrument supports for each of the Type A, B, and C post-accident instrumentation, respectively.]*

Minimum Inventory Selection Criteria Implementation Process

[*Section 7.5 provides a discussion of the development of the requirements of Regulatory Guide 1.97 and the implementation process for the AP1000 (Criteria 1, 2, and 4).*

Section 18.7 and Reference 1 provide a discussion of the implementation process for identification of critical PRA operator actions (Criteria 3). Chapter 30 of the AP1000 PRA describes the process for the human reliability analysis.]*

18.12.3 Remote Shutdown Workstation Displays, Alarms, and Controls

[*Subsection 7.4.3 discusses safe shutdown using the remote shutdown workstation following an evacuation of the main control room.*

The main control room provides the capability to perform accident mitigation and safe shutdown tasks for design basis events. The only types of events that would require evacuation of the main control room and control from the remote shutdown workstation are localized emergencies where the main control room environment is unsuitable for the operators or where the main control room workstations and equipment become damaged.

Evacuation of the main control room is not expected to occur coincident with any other design basis events. Subsection 9.5.1 of the Standard Review Plan (NUREG-0800) specifically excludes consideration of other design basis events coincident with a fire.

The design capability for the remote shutdown workstation is to provide the capability to establish and maintain safe shutdown conditions following a main control room evacuation, as described in subsection 7.4.3.1.1. The controls, displays, and alarms listed in Table 18.12.2-1 are retrievable from the remote shutdown workstation.]*

18.12.4 Combined License Information

This section contained no requirement for additional information.

18.12.5 References

[*1. WCAP-14651, "Integration of Human Reliability Analysis With Human Factors Engineering Design Implementation Plan," Revision 2, May 1997.*]*

2. WCAP-13793, "The AP600 System/Event Matrix," June 1994.

*NRC Staff approval is required prior to implementing a change in this information.

Table 18.12.2-1 (Sheet 1 of 2)
Minimum Inventory of
Fixed Position Controls, Displays, and Alerts

Description	Control	Display	Alert[2]
Neutron flux		x	x
Neutron flux doubling[3]			x
Startup rate		x	x
RCS pressure		x	x
Wide range T_{hot}		x	
Wide range T_{cold}		x	x
RCS cooldown rate compared to the limit based on RCS pressure		x	x
Wide range T_{cold} compared to the limit based on RCS pressure		x	x
Change of RCS temperature by more than 5°F in the last 10 minutes			x
Containment water level		x	x
Containment pressure		x	x
Pressurizer water level		x	x
Pressurizer water level trend		x	
Pressurizer reference leg temperature		x	
Reactor vessel - Hot leg water level		x	x
Pressurizer pressure		x	
Core exit temperature		x	x
RCS subcooling		x	x
RCS cold overpressure limit		x	x
IRWST water level		x	x
PRHR flow		x	x
PRHR outlet temperature		x	x
PCS storage tank water level		x	
PCS cooling flow		x	
IRWST to RNS suction valve status[3]		x	x
Remotely operated containment isolation valve status[3]		x	
Containment area high range radiation level		x	x
Containment pressure (extended range)		x	
CMT level[1]		x	

Table 18.12.2-1 (Sheet 2 of 2)
Minimum Inventory of
Fixed Position Controls, Displays, and Alerts

Description	Control	Display	Alert[2]
Manual reactor trip (Also initiates turbine trip Figure 7.2-1, sheet 14.)	x		
Manual safeguards actuation	x		
Manual CMT actuation	x		
Manual main control room emergency habitability system actuation[4]	x		
Manual ADS actuation (1-3 and 4)	x		
Manual PRHR actuation	x		
Manual containment cooling actuation	x		
Manual IRWST injection actuation	x		
Manual containment recirculation actuation	x		
Manual containment isolation	x		
Manual main steam line isolation	x		
Manual feedwater isolation	x		
Manual containment hydrogen igniter (nonsafety-related)[5]	x		
Manual ADS and IRWST injection unblock[6]	x		

Notes:

1. Although this parameter does not satisfy any of the selection criteria of Subsection 18.12.2, its importance to manual actuation of ADS justifies its placement on this list.
2. These parameters are used to generate visual alerts that identify challenges to the critical safety functions. For the main control room, the visual alerts are embedded in the safety-related displays as visual signals. For the remote shutdown workstation, the visual alerts are embedded in the nonsafety-related displays as visual signals.
3. These instruments are not required after 24 hours. (Subsection 7.5.4 includes more information on the class 1E valve position indication signals, specified as part of the post-accident monitoring instrumentation.)
4. This manual actuation capability is not needed at the remote shutdown workstation.
5. At the remote shutdown workstation, containment hydrogen igniter control is provided as a “soft” control.
6. These controls are not required at the remote shutdown workstation.

18.13 Design Implementation

This process element is added by Reference 2 to the Program Review Model specified in Reference 1. However, it mostly applies to plant modernization. The portions of the added element that apply to new plants were formerly addressed under the Verification and Validation element in Reference 1. Since these aspects of the Program Review Model are unchanged, AP1000 will continue to address them under Section 18.11 as “Issue Resolution Verification” and “Final Plant HFE Verification.”

18.13.1 References

1. NUREG-0711, “Human Factors Engineering Program Review Model,” U.S. NRC, July 1994.

2. NUREG-0711, Rev. 1, “Human Factors Engineering Program Review Model,” U.S. NRC, May 2002.

18.14 Human Performance Monitoring

Human performance monitoring applies after the plant is placed in operation. The human performance monitoring process implements the guidance and methods as described in Reference 1.

The human performance monitoring process provides reasonable assurance that:

- The design can be effectively used by personnel, including within the control room and between the control room and local control stations and support centers.
- Changes made to the human system interface(s), procedures, and training do not have adverse effects on personnel performance, (e.g., a change does not interfere with previously trained skills).
- Human actions can be accomplished within time and performance criteria.
- The acceptable level of performance established during the design integrated system validation is maintained.

The human performance monitoring process is structured such that:

- Human actions are monitored commensurate with their safety importance.
- Feedback of information and corrective actions are accomplished in a timely manner.
- Degradation in performance can be detected and corrected before plant safety is compromised (e.g., by use of the plant simulator during training exercises).

The human performance monitoring process for risk-informed changes is integrated into the corrective action program, training program and other programs as appropriate. Identified human performance conditions/issues are evaluated for human factors engineering applicability.

Human factors engineering conditions are assigned specific human factors cause determination codes, trended for indications of degraded performance or potential human performance failures and have specific corrective actions identified.

The cause investigation:

- Identifies the cause of the failure or degraded performance to the extent that corrective action can be taken consistent with the corrective action program requirements.
- Addresses failure significance which includes the circumstances surrounding the failure or degraded performance, the characteristics of the failure, and whether the failure is isolated or has generic or common cause implications.
- Identifies and establishes corrective actions necessary to preclude the recurrence of unacceptable failures or degraded performance in the case of a significant condition adverse to quality.

When appropriate, design changes are integrated into training exercises to monitor for degradation in performance and allow for early detection and corrective actions before plant safety is challenged (e.g., by use of the plant simulator during training exercises).

Plant or personnel performance under actual design conditions may not be readily measurable. When actual conditions cannot be simulated, monitored, or measured, the available information that most closely approximates performance data in actual conditions should be used.

Monitoring strategies for human performance trending after the implementation of design changes is capable of demonstrating that performance is consistent with that assumed in the various analyses conducted to justify the change.

Risk-informed changes are screened commensurate with their safety importance to determine if the change requires monitoring of actions. For changes which require monitoring, the appropriate monitoring requirements are determined and implemented in the training program or other program as appropriate.

18.14.1 References

1. NUREG-0711, Rev. 1, “Human Factors Engineering Program Review Model,” U.S. NRC, May 2002.