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
- Qualified data processing system

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 both operators and the shift supervisor 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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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 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, with each switch having a single action. As shown in Figure 18.8-1, 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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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 qualified data processing system 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 through safety-related displays. The informational content of qualified data processing system displays 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 functional requirement documents and the human system inferface 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 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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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; see DCD Introduction Section 3.5.

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 basis, 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

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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) and the qualified data processing system. 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 an 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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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.

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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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.

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

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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 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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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 each of two redundant workstations. These two reactor operator workstations are in the main control area of the AP1000 control room.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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 control room supervisor (shift foreman) has an independent workstation that has 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).*]*

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 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

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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.

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*

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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.

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 qualified data processing system visual display units 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*

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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 bases 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 TSC is located in the control support area (CSA)*]*

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.*]*

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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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

18.8.3.6 Operational Support Center Mission and Major Tasks

The operational 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 operational 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 operational support center and the TSC are in different locations. The location of the operational support center is shown in Figure 1.2-18.

The major task of the operational 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 operational support center provides the resources for communicating with the main control room and the technical support center. This permits personnel reporting to the operational support center to be assigned to duties in support of emergency operations.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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.

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 automatic 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 Combined License information requested in this subsection has been fully addressed in APP-GW-GLR-082 (Reference 47), and the applicable changes are incorporated into the DCD. No additional work is required by the Combined License applicant to address the Combined License information requested in this subsection.

The following words represent the original Combined License Information Item commitment, which has been addressed as discussed above:

> Combined License applicants referencing AP1000 certified design will address the execution and documentation of the human system interface design implementation plan that is presented by Section 18.8.

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.

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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).

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. U.S. Department of Defense, 1989, "Military Standard 1472D; Human Engineering Design Criteria for Military Systems, Equipment and Facilities," (Washington, D.C., U.S. Department of Defense).

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

43. American National Standards Institute, 1988, "ANSI/HF 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 Probability 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 Proprietary).

*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5.

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; see DCD Introduction Section 3.5.

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; see DCD Introduction Section 3.5.

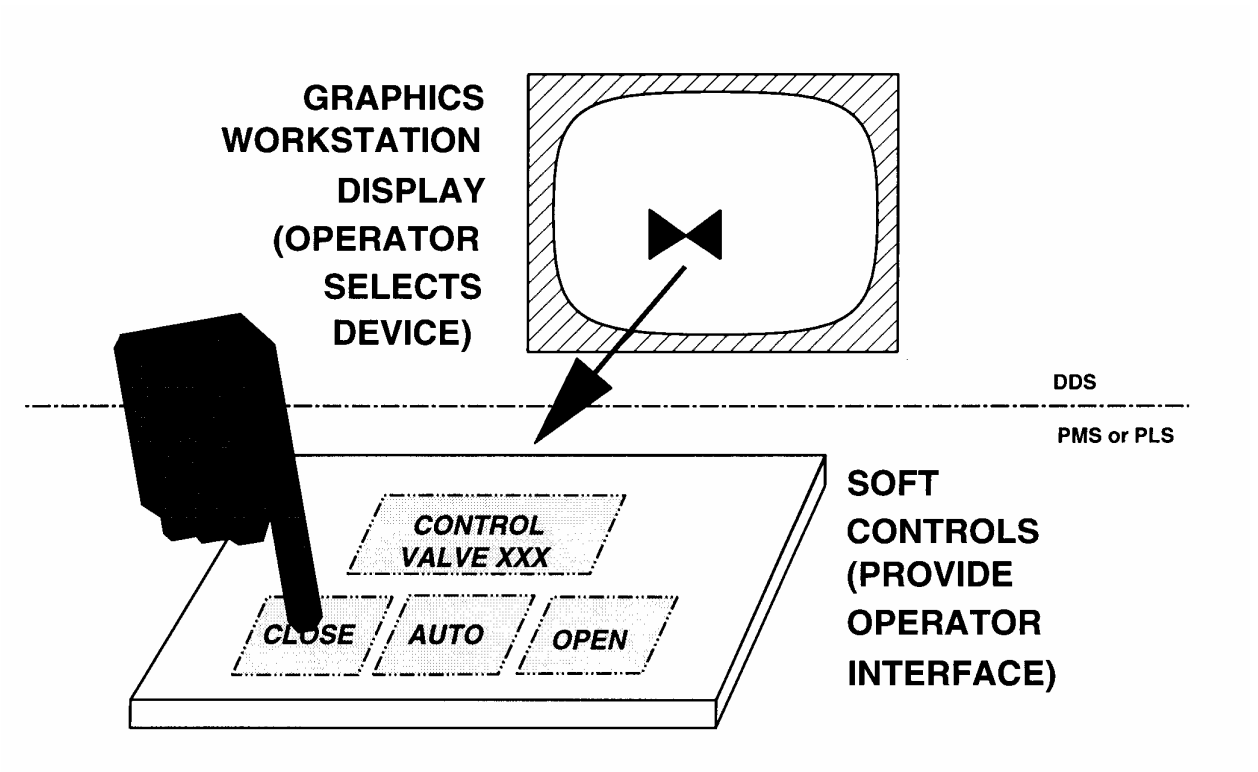

Figure 18.8-1

Soft Control Interactions

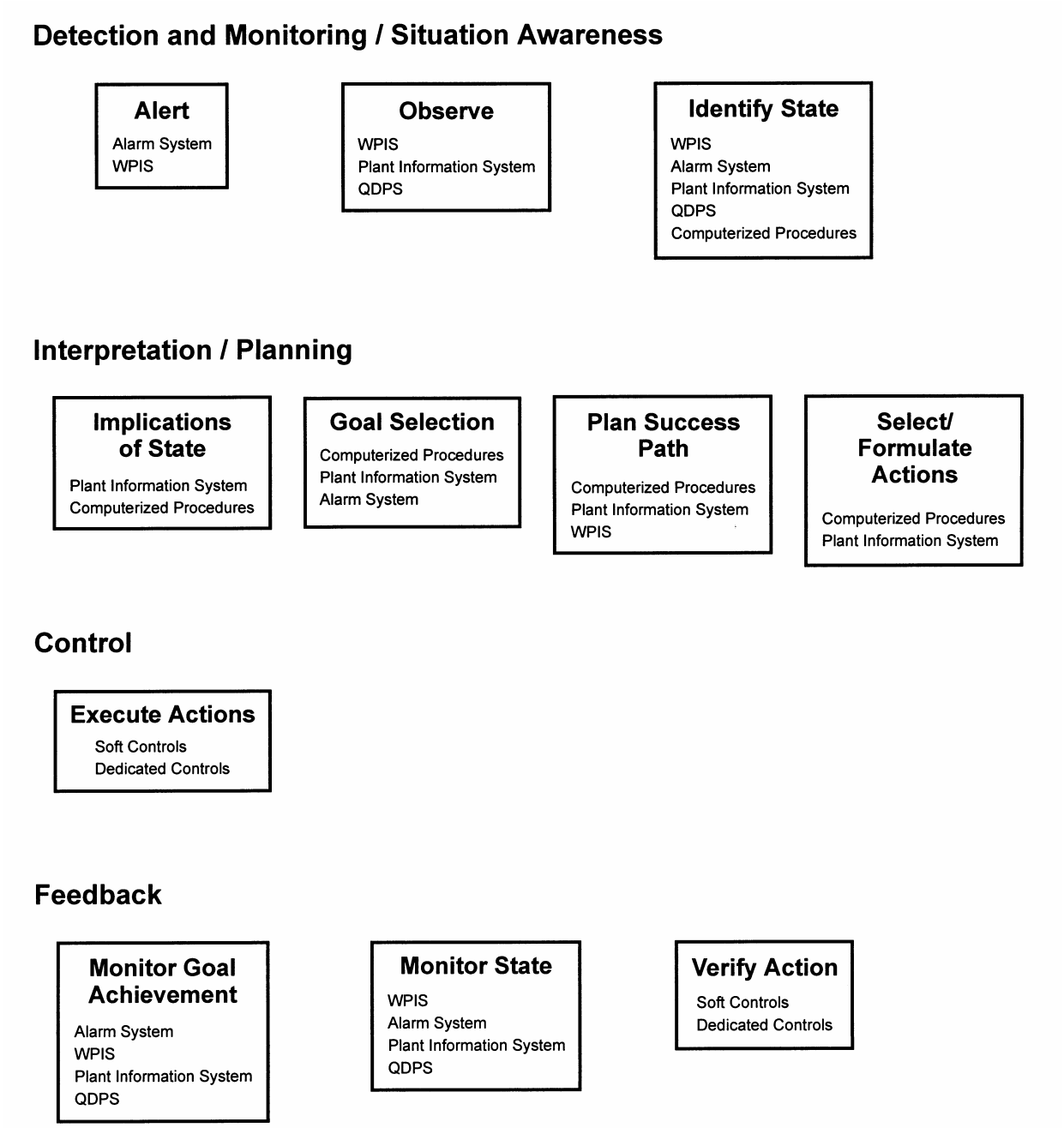

Figure 18.8-2

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