Westinghouse Non-Proprietary Class 3

WCAP-16801-NP
APP-GW-GLR-082
Revision 0

May 2007

Execution and Documentation of the Human System Interface Design Implementation Plan

WCAP-16801-NP
APP-GW-GLR-082
Revision 0

Execution and Documentation of the Human System Interface Design Implementation Plan

J.I. Reed*, Principal Engineer
Control Room and Human Factors Design I, RRAS

May 2007

Reviewer: P. J. Hunton*, Project Manager
Control Room and Human Factors Design I, RRAS

W. C. Kolb*, Manager
Computer Aided Engineering, Nuclear Power Plants

Approved: A. P. Drake*, Program Manager
RRAS NuStart/DOE Design Finalization

*Electronically approved records are authenticated in the electronic document management system.

Westinghouse Electric Company LLC
P.O. Box 355
Pittsburgh, PA 15230-0355

TABLE OF CONTENTS

LIST OF ACRONYMS AND ABBREVIATIONS

The following abbreviations and acronyms are defined to allow an understanding of their use within this document.

Acronyms	Definition
COL	Combined Operating License
CSA	Control Support Area
DCD	Design Control Document
EOF	Emergency Operations Facility
FBTA	Function-Based Task Analysis
HFE	Human Factors Engineering
HRA	Human Reliability Analysis
HSI	Human System Interface
ITAAC	Inspections, Tests, Analyses, and Acceptance Criteria
MCA	Main Control Area
MCR	Main Control Room
NRC	Nuclear Regulatory Commission
OCS	Operation and Control Centers Systems
OER	Operations Experience Review
OSA	Operational Sequence Analysis
QDPS	Qualified Data Processing System
RO	Reactor Operator
SRO	Senior Reactor Operator
RSR	Remote Shutdown Room
SSD	System Specification Document
SOE	Sequence of Events
SPDS	Safety Parameter Display System
TSC	Technical Support Center
V&V	Verification and Validation
VDU	Visual Display Unit
WPIS	Wall Panel Information System

1 PURPOSE

Chapter 18 of APP-GW-GL-700, "AP1000 Design Control Document" (Reference 1) describes the human factors engineering (HFE) aspects of AP1000. Section 18.8 of Reference 1 details the human system interface (HSI) design element of the HFE program.

The first purpose of this document is to address Combined Operating License (COL) Information Item 18.8-1, "Human System Interface Design." The second purpose of this technical report is to support the revision of the DCD (Reference 1) from Revision 15 to Revision 16. The mark-ups to Section 18.8 are documented, along with explanations for the changes. In addition, this document also describes the revision to the DCD Tier 1 Design Commitment that addresses the HSI design process.

2 BACKGROUND INFORMATION

Section 18.8 of the DCD (Reference 1) provides an implementation plan for the design of the operation and control centers system (OCS) and the HSI resources. The OCS includes the main control room (MCR), the technical support center (TSC), operations support center, radwaste control area, remote shutdown room, emergency operations facility (EOF) and local control stations. The HSIs include the plant information system, alarm system, computerized procedures, soft controls, dedicated controls, wall panel information system (WPIS) and the qualified data processing system (QDPS).

Section 18.8 of the DCD also describes the HFE design and implementation process and the method by which the human reliability analysis (HRA), concept of operations, operations experience review (OER), task analyses, engineering tests and the functional requirements analysis and allocation are integrated into the design process. The HSI design and implementation process encompasses a number of areas of work, as follows:

- Operations and Control Centers Functional Design
- HSI Resource Functional Design
- HSI Design Guidelines
- HSI Engineering Tests
- HSI Design Specifications
- HSI Design Implementation

[

]^{a,c,e}

3 CURRENT STATUS

This section provides an outline of the scope of the HFE work activities that have been completed in support of the HSI design as described in the DCD Section 18.8 (Reference 1). It also provides references that document the completed work.

3.1 OPERATION AND CONTROL CENTERS FUNCTIONAL DESIGN

[

]a,c,e

3.2 CONCEPT OF OPERATIONS

[

]a,c,e

3.3 OPERATIONS AND CONTROL CENTERS SYSTEM FUNCTIONAL REQUIREMENTS

[

]a,c,e

[

]a,c,e

3.4 HSI RESOURCES FUNCTIONAL DESIGN

[

]a,c,e

3.5 HSI DESIGN GUIDELINES

[

]a,c,e

[

]a,c,e

3.6 HSI ENGINEERING TESTS

[

]a,c,e

3.7 DESIGN SPECIFICATIONS

[

]a,c,e

4 WAY FORWARD

This section describes the continuing and planned HFE work that is being undertaken in support of the HSI design process as detailed in the DCD Section 18.8 (Reference 1).

4.1 DESIGN SPECIFICATIONS

[

]a,c,e

4.2 DESIGN IMPLEMENTATION

[

]a,c,e

5 DCD MARK-UPS

5.1 TIER 2 MARK-UPS

5.1.1 General Information

This section details the intended DCD mark-ups for Revision 16 of the DCD Sections 18.8. In instances where DCD text is bracketed with an asterisk the asterisk refers to the following note, "*NRC Staff approval is required prior to implementing a change in this information; see DCD Introduction Section 3.5."

DCD Section 18.8 is relatively lengthy and the mark-ups are distributed throughout Section 18.8. To assist the reader, the mark-ups are shown in this document in context; just showing the marked-up text on its own may make little sense to the reader. Therefore, all of the subsection headings in Section 18.8 are replicated. The text in each relevant subsection which includes a mark-up is replicated with the mark-up(s) clearly depicted, and at the end of the subsection, an explanation is provided for each change and denoted by the subheading "*Rationale*." The explanation is not to be incorporated into the DCD Revision 16, but is presented here in this document to provide the supporting explanation. If the subsection does not contain any changes, the subsection heading is followed by the statement, "There are no changes in this section." Likewise, this statement is not to be incorporated into the DCD Revision 16.

All inserted text is represented by underlining the text, and all the text to be deleted is represented by striking through the text. The use of sidelines to denote changed or additional text has not been used in order to avoid potential confusion between changes to the DCD and changes to this report (if required).

To assist in differentiating between the text replicated from the DCD and the notes added for this technical report, all of the DCD text is contained within quotation marks.

5.1.2 Chapter 18 Section 18.8 Mark-Ups and Explanations

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. ~~Execution and documentation of this implementation plan is the responsibility of the Combined License applicant.~~

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 ~~plant~~ 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 ~~video~~ 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 ~~operator~~ workstations in the main control room. ~~Procedure development, as stated in Section 13.5 and 18.9, is the responsibility of the Combined License applicant.~~ 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 ~~the responsibility of the Combined License applicant, as stated~~ 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.

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."

Rationale:

Change 1: "~~Execution and documentation of this implementation plan is the responsibility of the Combined License applicant.~~"

The above statement is no longer required.

Change 2: "The wall panel information station provides a dynamic ~~plant~~ display of the plant."

The above change is a grammatical correction for clarification.

Change 3: "The plant information system uses color-graphic ~~video~~ visual display units located on the operation and control centers workstations to display plant process data."

The change from "video" to "visual" is to provide consistency in the terminology used throughout Section 18.8.

Change 4: "The computerized procedure system is accessible from the ~~operator~~ workstations in the main control room."

The deletion of "operator" is to clarify that the computerized procedure system is accessible from the supervisor workstations as well as the operator workstations.

Change 5: "Procedure development, as stated in Section 13.5 and 18.9, is the responsibility of the Combined License applicant" changed to "Procedure development is addressed in Sections 13.5 and 18.9."

The statement regarding the responsibility of the Combined License applicant is no longer required.

Note there are no changes to Figure 18.8-1, "Soft Control Interactions."

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 interface ~~are applied to an appropriate set of human factors engineering~~ 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."

Rationale:

Change 1: "These functional requirement documents and the human system interface ~~are applied to an appropriate set of human factors engineering~~ design guidelines are used to develop the design specifications."

The original sentence was misleading. The rewording correctly represents the HSI design process and clarifies that the HSI design guidelines is a single document (and not a set of documents).

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 documents includes requirements to meet failure, diversity, electrical separation, and other applicable criteria~~; they establish~~. This document establishes requirements related to access control, redundancy, independence, identification and test capability,~~; they~~ and defines requirements on system inputs and outputs~~; they specify~~. It specifies the system safety classification and defines applicable quality assurance, reliability goals, and environmental qualification requirements. The ~~functional requirements document for each human system interface resource includes a~~ specification of the cognitive activities in the operator decision-making model that ~~the~~ 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."

Rationale:

Change 1: The operations and control centers functional requirements documents includes requirements to meet failure, diversity, electrical separation, and other applicable criteria~~; they establish~~. This document establishes requirements related to access control, redundancy, independence, identification and test capability,~~; they~~ and defines requirements on system inputs and outputs~~; they specify~~. It specifies the system safety classification and defines applicable quality assurance, reliability goals, and environmental qualification requirements. The ~~functional requirements document for each human system interface resource includes a~~ specification of the cognitive activities in the operator decision-making model that ~~the~~ each human system interface resource is intended to support is provided in the operation and control centers functional requirements document.

The rewording clarifies that the operations and control centers functional requirements document captures requirements for failure, diversity, electrical separation and other applicable criteria. This document also maps the cognitive activities to the supporting HSI resource. The original intention was to provide this information in the functional requirements document for each HSI resource. However, it was determined that it would be more appropriate and informative if the description of the mapping between the cognitive activities and the supporting HSI resources is available in a single location. This facilitates the explanation of how multiple HSI resources support operator decision-making.

Note there are no changes to Figure 18.8-2, "Mapping of Human System Interface Resources to Operator Decision-Making Model."

Note there are no changes to Table 18.8-1, "Human Performance issues to be Addressed by the HSI Design."

18.8.1.2 Design Guidelines

"Guidelines for the human system interface design ~~are~~ have been developed for ~~each of~~ the human system interface resources to facilitate the standard and consistent application of human factors engineering (HFE) principles to the design (see Reference 1). ~~This guidance is contained in a set of~~ Reference 1 contains standards and conventions guidelines ~~documents~~ that 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 ~~become a tool that~~ 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 documents 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

~~An illustrative subset of~~ The accepted human factors engineering guidelines documents that ~~will be~~ were used in compiling ~~human factors engineering guidelines, standards, and principles to be included in the AP600~~ the AP1000 human system interface design guidelines documents are found in References ~~1~~ 2 through 8. ~~These documents apply directly to AP1000."~~

Rationale:

The modifications detailed above take into account that the HSI design guidelines have been produced and to include the corresponding reference (APP-OCS-J1-002, "AP1000 Human System Interface Design Guidelines," Reference 11). This was addressed in "AP1000 Standard Combined License Technical Report on Human System Interface Design Guidelines" (APP-GW-GLR-091, Reference 12). The text was also changed to reflect that the HSI design guidelines is a single document, and is not a set of documents.

In addition, the references in section 18.8.6 were updated to specify the documents that were utilized in the development of the HSI design guidelines. The details of these updates are as follows:

1. The American National Standards Institute, ANSI HFS-100-1988, "American Standard for Human Factors Engineering of Visual Display Terminal Workstations," was deleted. The information in this document is included and/or superseded in NUREG-0700.

2. NUREG-0899, "Guidelines for the Preparation of Emergency Operating Procedures," was deleted. The preparation of procedures is not within the scope of the HSI design guidelines. The development of procedures is addressed in DCD Chapter 13 (Reference 1).

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," has been added. This document provides useful information and is relatively up-to-date.

4. NUREG-1358, "Lessons Learned from the Special Inspection Program for Emergency," was deleted. The lessons learned in this relatively aged document have been included and/or superseded in other comparable guides, codes and standards documents.

5. 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," has been added. This document provides useful, relatively up-to-date information in an area in which HFE guidance is not abundant.

6. The reference to NUREG-0700, "Human-System Interface Design Review Guideline," was changed from Revision 1 to Revision 2. Revision 2 contains the most up-to-date guidance.

7. NUREG/CR-5908, "Advanced Human-System Interface Design Guidelines," was not used. The relevant information in NUREG/CR-5908 is included and/or superseded in NUREG-0700.

8. The U.S. Department of Defense, "Human Engineering Guidelines for Management Information Systems," DOD-HDBK-761A, was deleted. The relevant information from this Department of Defense document is included and/or superseded in NUREG-0700 and MIL-STD-1472.

9. MIL-STD-1472, "Department of Defense Design Criteria Standard: Human Engineering," was added. This document contains up-to-date HFE guidance and is particularly useful for addressing areas such as anthropometrics.

The detailed references can be found at the end of this Section 5.1 where the DCD Chapter 18 references from Section 18.8.6 are listed. By updating the references to those that were used in the development of the AP1000 HSI design guidelines, the statement regarding the applicability of the references that were utilized for AP600 is no longer pertinent and has been deleted.

18.8.1.3 Design Specifications

There are no changes in this section.

18.8.1.4 Man-in-the-Loop Testing

There are no changes in this section.

18.8.1.5 Mockup Activities

There are no changes in this section.

18.8.1.6 Human System Interface Design Documentation

There are no changes in this section.

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 ~~complimentary~~ 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."

Rationale:

Change 1: "The AP1000 task analysis, described in Section 18.5, includes two ~~complimentary~~ complementary activities: function-based task analysis (FBTA) and traditional task analysis, or operational sequence analysis (OSA)."

This change is a grammatical correction.

18.8.1.8 General Human System Interface Design Feature Selection

There are no changes in this section.

18.8.1.9 Human System Interface Characteristics: Identification of High Workload Situations

There are no changes in the first two paragraphs of this section.

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 ~~computer-based models of cognitive responses to control room events. This tool or functionally similar tools are used to support workload~~ task analysis."

Rationale:

Change 1: "Analytic methods include the use of ~~computer-based models of cognitive responses to control room events. This tool or functionally similar tools are used to support workload~~ task analysis."

This change is to bring this subsection in-line with the changes made in Section 18.5 of the DCD. In summary, the term "computer based models" was removed to enable the task analysis implementation plan to determine the most appropriate method to measure workload and to not prescribe that computer based modeling tools will be utilized. Details of this change can be found in APP-GW-GLR-081 (Reference 17).

Usability Guidance

~~"Design guideline documents are developed that synthesize results of reviews of the relevant human system interface literature and experience in nuclear power plants and related industries. These documents contribute to the design basis for design of human system interface resources. For example, the use of soft controls in the design of the AP1000 human system interface builds on existing human system interface guidelines and experience with the use of "soft controls" in existing plants (fossil plants)~~ Usability guidance is included in the human system interface design guidelines, as discussed in Section 18.8.1.2."

Rationale:

As stated in the inserted text, usability guidance is included in the HSI design guidelines. Therefore, the subsection for "Usability Guidance" has been changed to refer the reader to Section 18.8.1.2, "Design Guidelines."

Workstation Usage Scenarios

There are no changes in this section.

Environmental Conditions

There are no changes in this section.

Local Control Actions

There are no changes in this section.

18.8.1.10 Human System Interface Software Design and Implementation Process

There are no changes in this section.

18.8.2 Safety Parameter Display System (SPDS)

There are no changes in this section.

18.8.2.1 General Safety Parameter Display System Requirements

There are no changes in this section.

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.

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 ~~through one navigational action~~. 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."

Rationale:

Change 1: "Those that are not continuously displayed on the wall panel are accessible at the operator's workstation ~~through one navigational action.~~"

The statement that one navigational action is required was deleted because the detailed design of the displays is under development, and therefore, this statement may be incorrect or cause confusion. The design of the displays may result in the safety parameters actually being continuously displayed at the operator's workstation. Alternatively, two "navigational actions" may be required, which is acceptable from a HFE perspective. The HSI design guidelines, Reference 11, states that the HSI design should enable user access to all key or primary displays by no more than two control actions. Furthermore, the original text "navigational action" was vague. For example, a "navigational action" may be the selection of an on-screen target or icon, the use of a pull-down or pop-up menu or the entering of a display page reference number.

18.8.2.3 Reliability

There are no changes in this section.

18.8.2.4 Isolation

There are no changes in this section.

18.8.2.5 Human Factors Engineering

There are no changes in this section.

18.8.2.6 Minimum Information

There are no changes in this section.

18.8.2.7 Procedures and Training

~~"As stated in~~ Sections 13.2 and 13.5, describe the development of training programs and plant procedures ~~are the responsibility of the Combined License applicant~~, respectively. Reference 30 describes how training insights are passed from the designer to ~~the Combined License applicant~~ operations personnel who participate as subjects in the human factors engineering V&V activities. Reference 31 provides input to the ~~Combined License applicant for the~~ development of plant operating procedures."

Rationale:

The statements regarding the Combined License applicant are no longer required.

18.8.3 Operation and Control Centers System

There are no changes in this section.

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 switching and tagging~~ the operations work area, the shift supervisor's office, ~~the shift supervisor's clerk's office~~, and the operations ~~staff's area~~ break room (see Figure 1.2-8). Habitability systems are described in Sections 6.4 and 9.4."

Rationale:

Driven by a utility review of the AP1000 by operations personnel, the design of the MCR, MCA and surrounding areas has progressed since the issuance of Revision 15 of the DCD (Reference 1). Therefore, the text in the description of these areas has been updated accordingly. In summary, the changes that have occurred during the design development of these areas is as follows:

- The switching and tagging area has been renamed the "operations work area." The switching and tagging functions may be conducted from an area outside the MCR boundary. The operations work area is where personnel may undertake non-MCA tasks while remaining within the MCR boundary.

- The operations staff's area has been renamed the "operations break room." This terminology is more representative in that this area will be provided with kitchen and restroom facilities.

- The shift supervisor's clerk's office has been removed. A clerk is not required to be within the MCR. Therefore, by removing this role and its corresponding office, better use is made of the available floor space within the MCR.

18.8.3.2 Main Control Area Mission and Major Tasks

Changes to section 18.8.3.2 are made as described in "Editorial Format Change to 'COL Applicant' Items" (APP-GW-GLR-130, Reference 19).

18.8.3.3 ~~Switching and Tagging~~ Operations Work Area Mission and Major Tasks

~~"The mission of the switching and tagging area is to provide an interface between plant maintenance and plant operations personnel. Figures 1.2-8 and 6.4-1 provide the layout of the switching and tagging area. The operations staff monitors and approves the state of systems, major components, and equipment. The maintenance staff is informed of maintenance required by the operations staff. The means for initiating, tracking, and logging maintenance work orders is provided.~~

~~The major task of the switching and tagging area is to ease the management and implementation of the switching and tagging operations. The switching and tagging area generates notifications that equipment is not available due to testing, maintenance, or equipment failure. These notifications alert plant operating personnel to the unavailability of equipment. Notifications are provided to plant maintenance personnel, alerting them that operating personnel are aware of the equipment status. The switching and tagging area facilitates a systematic and organized approach to removing equipment from service as well as returning it to service.~~

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."

Rationale:

The explanation for 18.8.3.1 directly applies to the changes in 18.8.3.3. The additional text in 18.8.3.3 provides further details regarding the missions and tasks associated with the operations work area.

18.8.3.4 Remote Shutdown Workstation Mission and Major Tasks

There are no changes in this section.

18.8.3.5 Technical Support Center Mission and Major Tasks

Changes to section 18.8.3.5 are made as described in "AP1000 Technical Support Center" (APP-GW-GLR-107, Reference 18) and "Editorial Format Change to 'COL Applicant' Items" (APP-GW-GLR-130, Reference 19).

18.8.3.6 Operational Support Center Mission and Major Tasks

Changes to section 18.8.3.6 are made as described in "AP1000 Technical Support Center" (APP-GW-GLR-107, Reference 18).

18.8.3.7 Radwaste Control Area Mission and Major Tasks

There are no changes in this section.

18.8.3.8 Local Control Stations Mission and Major Tasks

There are no changes in this section.

18.8.3.9 Emergency Operations Facility

Changes to section 18.8.3.9 are made as described in "Editorial Format Change to 'COL Applicant' Items" (APP-GW-GLR-130, Reference 19).

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

There are no changes in this section.

18.8.4.1.1 Maintainability

There are no changes in this section.

18.8.4.1.2 Accessibility and Equipment Laydown Provisions

There are no changes in this section.

18.8.4.1.3 Lighting

There are no changes in this section.

18.8.4.1.4 Radiation Protection and Safety

There are no changes in this section.

18.8.4.1.5 Communication

There are no changes in this section.

18.8.4.1.6 Temperature, Humidity, Ventilation

There are no changes in this section.

18.8.4.1.7 Emergency Equipment

There are no changes in this section.

18.8.4.1.8 Storage

There are no changes in this section.

18.8.4.1.9 Coding and Labeling

There are no changes in this section.

18.8.5 Combined License Information

"The Combined License information requested in this subsection has been fully addressed in this document (APP-GW-GLR-082). No additional work is required by the Combined Operating License applicant to address the Combined License information requested in this subsection."

The following words represent the original Combined Operating 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 8.8."

Rationale:

The explanation for this change is provided within the above text. In summary, by virtue of the HFE work completed to date and the formal plans to conduct and document the forthcoming work, it is concluded that the COL Information Item 18.8-1 has been addressed.

18.8.6 References

1. American National Standards Institute, ANSI HFS-100-1988, "American Standard for Human Factors Engineering of Visual Display Terminal Workstations," Santa Monica, California, 1988. 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. ~~NUREG-0899, "Guidelines for the Preparation of Emergency Operating Procedures," U.S. Nuclear Regulator Commission, Washington, D.C., August 1982.~~ 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. ~~NUREG-1358, "Lessons Learned from the Special Inspection Program for Emergency," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1989.~~ 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., ~~February 1995. (Draft Report)~~ May 2002.

6. ~~NUREG/CR-5908, "Advanced Human-System Interface Design Guidelines," U.S. Nuclear Regulatory Commission, Washington, D.C., July 1994.~~ 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. ~~U.S. Department of Defense, "Human Engineering Guidelines for Management Information Systems," DOD-HDBK-761A, Office of Management and Budget, Washington, D.C., 1990.~~ 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 997.

[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).

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).

Rationale:

See "Rationale" for DCD Section 18.8.1.2 for the explanation of the changes to the above References.

5.2 TIER 1 MARK-UPS

A DCD mark-up of the Table 3.2-1 Design Commitment Item 3 "Acceptance Criteria" (3rd column) is intended for Revision 16 of the DCD. The basis for this change is to identify those areas of work that are complete.

Note that the Table 3.2-1 Design Commitment Items 6 to 13 that relate to the provision and specific features of the OCSs and HSI resources remain unchanged.

"A report exists and concludes that the HSI design for the OCS was conducted in conformance with the implementation plan and includes the following documents:

- ~~Operations and Control Centers System Specification Document~~ Deleted.

- ~~Functional requirements and design basis documents for the alarm system, plant information system, wall panel information system, controls (soft and dedicated) and the qualified data processing subsystems~~. Deleted.

- ~~Design guideline documents (based on accepted HFE guidelines, standards and principles) for the alarm system, displays, controls and anthropometrics.~~ Deleted.

- Design specifications for the alarm system, plant information system, wall panel information system, controls (soft and dedicated) and the qualified data processing subsystem.

- ~~Engineering test report document summarizing outcomes of each man-in-the-loop engineering test iteration performed to support HSI design.~~" Deleted.

6 REFERENCES

1. APP-GW-GL-700, Revision 15 (Non-Proprietary), "AP1000 Design Control Document," Westinghouse Electric Company LLC.

2. APP-OCS-GBH-001, (Proprietary), "AP1000 Human Factors Engineering Program Plan," Westinghouse Electric Company LLC.

3. APP-OCS-J7-001, (Proprietary), "AP1000 Operations and Control Centers System System Specification Document," Westinghouse Electric Company LLC.

4. APP-OCS-GJR-002, (Proprietary), "Concept of Operation," Westinghouse Electric Company LLC.

5. APP-OCS-J1-009, (Proprietary), "AP1000 Operations and Control Centers System Functional Requirements," Westinghouse Electric Company LLC.

6. APP-OCS-J1-001, (Proprietary), "AP1000 Alarm System Functional Requirements," Westinghouse Electric Company LLC.

7. APP-OCS-J1-020, (Proprietary), "Computerized Procedures System Functional Requirements," Westinghouse Electric Company LLC.

8. APP-OCS-J1-010, (Proprietary), "AP1000 Display Functional Requirements," Westinghouse Electric Company LLC.

9. APP-OCS-J1-007, (Proprietary), "AP1000 Wall Panel Information System Functional Requirements," Westinghouse Electric Company LLC.

10. APP-PMS-J4-001, (Proprietary), "Post Accident Monitoring System Functional Specification," Westinghouse Electric Company LLC.

11. APP-OCS-J1-002, (Proprietary), "AP1000 Human System Interface Design Guidelines," Westinghouse Electric Company LLC.

12. APP-GW-GLR-091, "AP1000 Standard Combined License Technical Report on Human System Interface Design Guidelines," Westinghouse Electric Company LLC.

13. APP-OCS-T2R-020, (Proprietary), "AP1000 Engineering Test Phase I Test Report," Westinghouse Electric Company LLC.

14. APP-OCS-T2R-022, (Proprietary), "AP1000 Engineering Test Phase II Test Report," Westinghouse Electric Company LLC.

15. APP-DDS-J4V-001, (Proprietary), "AP1000 Display Design Specification," Westinghouse Electric Company LLC.

16. APP-DDS-J4V-002, (Proprietary), "AP1000 Specification of Static and Dynamic Symbols," Westinghouse Electric Company LLC.

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

18. APP-GW-GLR-107, "AP1000 Technical Support Center," Westinghouse Electric Company LLC.

19. APP-GW-GLR-130, "Editorial Format Change to 'COL Applicant' Items," Westinghouse Electric Company LLC.