Westinghouse Electric Corporation Energy Systems

Box 355
Pittsburgh Pennsylvania 15230-0355

NSD-NRC-96-4874
DCP/NRC0660
Docket No.: STN-52-003

December 16, 1996

Document Control Desk
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

Attention: T. Quay

Subject: Progress Towards Resolving Element 2 and 4 Open Items for AP600

References:

1. WCAP-14645; "Human Factors Engineering Operating Experience Review Report For the AP600 Nuclear Power Plant", Revision 1, October 1996.
2. Letter from NRC to Westinghouse, Huffman to Liparulo, Comments on AP600 Related Open Items Associated with Element 2 of the Human Factors Engineering Program Review Model (HFEPRM), dated 12/4/96.
3. Letter from NRC to Westinghouse, Huffman to Liparulo, Comments on AP600 Related Open Items Associated with Element 4 of the Human Factors Engineering Program Review Model (HFEPRM), dated 12/4/96.
4. Letter from NRC to Westinghouse, Martin to Liparulo, Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) for the AP600, dated 11/26/96.

Enclosures:

1. Design Issues Tracking System Database Report For Human Factors Engineering Issues Associated With The Operating Experience Review
2. Design Issues Tracking System Database Report For Human Factors Engineering Issues Associated With Design Reviews
3. Design Issues Tracking System Database Report For Human Factors Engineering Issues Associated With The Design of The Human System Interface and The Operation and Control Center Systems
4. SSAR Chapter 18 markup to be incorporated into SSAR Revision 10.

E004

3003a

190079

December 16, 1996

NSD-NRC-96-4874
DCP/NRC0660

Dear Mr. Quay:

Enclosed are copies of Design Issues Tracking reports for human factors issues and a markup of AP600 SSAR Chapter 18 to reflect resolution of the following DSER Open Item Tracking System items for NUREG-0711 Elements 2 and 4. These resolutions were discussed with Messrs. Sebrosky and Bongarra via telecons on December 9 and 11, 1996.

Element 2:

Open Item	OITS	Status (Westinghouse/NRC)
18.3.3.1-1	1316	Closed/Resolved per Reference 2.
18.3.3.1-2	1317	Action W/Action W

There were four parts of this item which were considered Action W as described below. This item will be considered Closed/Resolved upon submittal of WCAP-14645 Revision 2 on December 20, 1996, to reflect the following:

1. Item 7 - WCAP-14645 Revision 1 will be revised to address the instrumentation to be used by operators for monitoring the buildup of clams, mussels, and corrosion products.

2. Item 165 - WCAP-14645 Revision 1 will be revised to address valve position indication for risk-significant valves (as defined in SSAR Section 16.2).

3. The transmittal letter to WCAP-14645 Revision 2 will specify that Westinghouse reviewed the remaining 50 percent of the items from the BNL OER report and that no deficiencies were identified.

4. The "transfer mechanism" issue is considered resolved based on the attached markup, to be incorporated in SSAR Revision 10, for section 18.3.1 which specifies where the COL action items identified in the OER report are found in the SSAR. Based on a review of the Combined License Applicant information items identified in WCAP-14645, the reference to a COL responsibility for SSAR Section 11.5 has been deleted from OER Report Table 1, item 168.

18.3.3.1-3	1318	Closed/Resolved per Reference 2.
18.3.3.1-4	1319	Closed/Resolved by this letter. To close this item, Westinghouse has

		included the appropriate operator interview commitments as documented in item 4179 of Enclosure 1.
18.3.3.2-1	1320	Closed/Resolved per Reference 2.
18.3.3.2-2	1321	Closed/Resolved per Reference 2.
18.3.3.2-3	1322	This item is statused Closed/Resolved based on Westinghouse submittal of Enclosures 1 through 3. Since the DIT HFE items have not been approved at this point, the requested design file documents are not available.

The AP600 design issues tracking system is described in SSAR subsection 18.2.4. Tracking of the human factors engineering issues is accomplished within the framework of the overall plant design process. In this manner, human factors engineering issues are addressed in the same way as those for other disciplines. Human factors engineering design issues are identified from the following three sources and are entered into the design issues tracking system database:

- Operating experience review
- Design reviews
- Design issues associated with the design of the human system interface and the operation and control center systems

Enclosure (1) is a copy of the design issues tracking system database report for human factors engineering issues identified as a result of the operating experience review (Reference 1). Note that the "DIT-OER" entry in column 2 (Type column) of the report identifies each issue as one specified by Reference (1).

Enclosure (2) is a copy of the tracking system database report for human factors issues identified as a result of design reviews. There are currently about 400 design issues in the tracking system database that have been identified from the various design reviews conducted. Enclosure (2) presents the subset of these that have been identified as human factors engineering design issues. A human factors engineering design issue is one that is related to or associated with any of the ten elements of the Human Factors Engineering Program Review Model (NUREG-0711). Note that the "DIT-DRCHITH" entry in column 2 (Type column) of the report identifies each issue as a human factors issue resulting from a design review.

Enclosure (3) is a copy of the tracking system database report for human factors issues identified by the human system interface designers as issues directly associated with the design of the human system interface and the operation and control center systems. Note that the "DIT-MMI" entry in column 2 (Type column) of the report identifies the issue as a human factors issue directly associated with the design of the human system interface.

Element 4:

Open Item	OITS	Status (Westinghouse/NRC)
18.5.3-1	1338	Closed/Resolved per Reference 3.
18.5.3-2	1339	Closed/Resolved per Reference 3.
18.5.3-3	1340	Closed/Resolved per Reference 3.
18.5.3-4	1341	Closed/Resolved by the attached markup of SSAR Section 18.5.4 modification to the Combined License applicant item.
18.5.3-5	1342	Closed/Resolved per Reference 3.
18.9.3-2	1364	Closed/Resolved based on the December 11 telecon regarding designer input to procedure development and training program development and the relationship between task analysis and these programs.
18.12.3-1	1395	NRC action to review the minimum inventory issue.

Also item 1397 remains open with Westinghouse action to respond to NRC comments on the ITAACs received by Reference 4.

If you have any questions regarding this transmittal, please contact Robin K. Nydes at (412) 374-4125.

Brian A. McIntyre, Manager
Advanced Plant Safety and Licensing

3003a

December 16, 1996

NSD-NRC-96-4874
DCP/NRC0660

/jml

enclosures

cc: J. Bongarra, NRC (all enclosures)
W. Huffman (all enclosures)
J. O'Higgins (all enclosures)
J. O'Hara (all enclosures)
N. Liparulo (w/o enclosures)

Enclosure 1

AP600 Open Item Tracking System: Design Issues Tracking

Date: 12/13/96

Selection: [type] like 'DIT-OER' Sorted by Item #

Item No.	Type	(W) Status	Resp Engineer	Description / Closure Path / Detail Status
3461	DIT-OER	Action W	T.L. Schulz	Open item from OER (WCAP-14645): Number of actuation cycles for the emergency core cooling system and reactor protection system; As part of the specification, allowable actuation cycles and the method by which cycles will be defined, recorded, and tracked by the operating crew should be evaluated for human factors engineering implications. References: NUREG-0711, App. B, B.2 (12); TMI issue 2xvi
				Responsibility: Systems Engineering
3462	DIT-OER	Action W	J. Easter	Open item from OER (WCAP-14645): Main control room alarms, operator selectable alarms; The operators may need a low priority operator-selectable alarm to call attention to a component (e.g., a valve) that may be out of its normal position. Alarm systems should have the flexibility for the operators to easily add alarms to a screen when a potentially deviant situation is identified that they need called to their attention. Reference: NUREG-0711, App. B supplement, subsection 2.2.6
				Responsibility: Man-Machine Design
3463	DIT-OER	Action W	K. Deutsch	Open item from OER (WCAP-14645): Component related insights - power connections, dislodged connectors; Power connectors have become accidently dislodged resulting in undesired transients. One example is power connectors for the feedwater control system, which led to a reactor scram. Reference: NUREG-0711, App. B supplement, section 4.7
				Responsibility: Plant Instrumentation and Control Systems
3464	DIT-OER	Action W	S. Kerch	Open item from OER (WCAP-14645): Importance of predictability: The operators should know where a requested display will appear. In this fossil application, sometimes it appeared in an unexpected place and covered critical information. Reference: WCAP-14645, Table 2
				Responsibility: Man-Machine Design
3970	DIT-OER	Action W	D.J.McDermott	Open item from OER (WCAP-14645): Shutdown Operations--Equipment; CONTAINMENT EQUIPMENT HATCH An equipment upgrade that would improve shutdown safety is: A containment equipment hatch design that allows for expeditious closure by operators when needed during a shutdown abnormal event. Similiar provisions should be made other containment penetrations that may be open during shutdown evolutions.
				Responsibility: Systems Engineering
				The equipment hatch will be maintained closed for operation modes requiring containment integrity or the capability of rapid closure will be incorporated into the design of the maintenance hatches. An open item is assigned to follow the resolution of this item. Other containment penetrations including containment purge and personnel airlocks provide the ability for rapid closure independent of non-safety related support services including ac power.
3971	DIT-OER	Action W	J.Easter; S.Kerch	Open item from OER (WCAP-14645): From Table 2 (Ref. 2.1 item 4) of the referenced WCAP; Providing guidance or design features on how to configure/coordinate a multiple VDU display space.
				Responsibility: Man-Machine Design

AP600 Open Item Tracking System: Design Issues Tracking

Date: 12/13/96

Selection: [type] like 'DIT-OER' Sorted by Item #

Item No.	Type	(W) Status	Resp Engineer	Description / Closure Path / Detail Status
3972	DIT-OER	Action W	S.Kerch	Open item from OER (WCAP-14645): From Table 2 (Ref. 2.1 item 7) of the referenced WCAP. Control task characteristics and soft controls: a) operators question the value of touch screens because operators were accustomed to a mouse, and touch poke points were to thick and inaccurate; b) potential problem of multiple individuals simultaneously controlling the same piece of equipment from VDUs at different locations.
				Responsibility: Man-Machine Design
3973	DIT-OER	Action W	S.Kerch	Open item from OER (WCAP-14645): From Table 2 (Ref. 2.2 item 1) of the referenced WCAP. Soft control lessons learned from aircraft industry: Lifting finger off the target area touch logic to actuate is more forgiving than when the finger enters the target area to actuate.
				Responsibility: Man-Machine Design
3974	DIT-OER	Action W	S.Kerch; K.Deutsch	Open item from OER (WCAP-14645): From Table 3 (Ref. 3.3 item 1) of the referenced WCAP. Operator interviews on AP600 soft controls: Excessive lag in response time from the moment an operator initiates a controlling action to the moment the respective component responds can be an impediment to the operator's ability to carry out manual control tasks.
				Responsibility: Man-Machine Design and Plant Instrumentation and Control Systems
4179	DIT-OER	Action W	S.Kerch	References: NRC letter, "Comments on AP600 Related Open Items Associated With Element 2 of the Human Factors Engineering Program Review Model", Dec 4, 1996 and NUREG-0711 section 3.4.1 (4). WCAP-14645 addresses operator interviews (section 5.0 and table 3). Remote shutdown and staffing were not addressed in the operator interviews documented by the eight references to Table 3. Per the referenced NRC letter and NUREG-0711 licensed operators need to be interviewed covering various topics including remote shutdown operations and staffing. Any human factors issues on these two topics need to be identified and addressed.
				Responsibility: Man-Machine Design

Enclosure 2

AP600 Open Item Tracking System: Design Issues Tracking

Date: 12/13/96

Selection: [type] like 'DIT-DRCHITHF' Sorted by Item #

Item No.	Type	(W) Status	Resp Engineer	Description / Closure Path / Detail Status
3546	DIT-DRCHITH	Action W	Schulz	It is my understanding that PRHR Hx operation is no longer needed to prevent pzr overfill. If so, automatic PRHR actuation follwoing an S-signal should be elimated. Current activation causes unnecessary cooldown transient, has adverse interaction with SGS, decay heat goes into IRWST instead of outside containment, requires operator to take action to regain control.
				Remove auto. PRHR Hx actuation on S-signal. (Note, actuation could be dependent on CMT heatup and Lo-Lo RCS pressure (1200psig). See Chit #10.
3562	DIT-DRCHITH	Action W	Schulz	The safety related criteria state that "no operator actions for 72 hours for DBE's". I understand that emergency response guidelines call for operators to isolate CMTs and PRHR after inadvertent S-signal, CMT, PRHR, etc. These actions may defeat auto safety response if anything else happens (like TMI). Operators will become accustomed to isolating PXS and like TMI may do so at wrong time due to habit or m' aken interpretation of situation.
				Elimination of auto PRHR Hx actutation and inadvertent PRHR Hx operation suggested in previous Chits should eliminate need for operation actions to isolate PXS components and terminate cooldown and restored SG heat removal. Revise ERG's to eliminate PXS isolation.
3575	DIT-DRCHITH	Action W	Schulz	Section 4.2.3.3 of the PXS SSAR mentions an alarm in containment which is intended to alert maintenance personnel of impending IRWST injection. What interfacing system provided this alarm? Is this a unique alarm or do we have other similar alarms in containment? Have the functional requirements for this personnel protection alarm been developed? Where do they appear?
				Insure that this alarm is part of the AP600 design baseline.
3577	DIT-DRCHITH	Action W	Schulz	The statement that no operator action is required for 72 hours after a DBA may not be true. Even on an ordinary reactor trip, shutdown margin is beginning to be lost after about 24 hours and up to 3% delta k SDM is lost 72-100 hours. It is not clear the boration aspects have 'een fully investigated.
				Investigate need for boration or note as an exception to the operator action criterion.
3672	DIT-DRCHITH	Action W	Wills	In the thermal analysis the initial temperature was 78 F which corresponds to the maximum URD control room operating temperature. The technical specifications (75 F) is recognized to be out of date but needs to be increased beyond 78 F to allow margin between the normal operating range and the analysis value. In addition to URDs limit the maximum allowable temperature rise during transient to 15 F which appears to be adding significantly to design complexity and to the cost of control room construction.
				Perform the thermal analysis at an initial starting temperature that provides for sufficient margin between the normal operating range and the analysis value. Investigate wheather a relaxation of the 15 F temperature rise limit is possible and wheather such a relaxation would allow for the deletion of the finned cooling arrangement on the control room ceiling. The magnitude of the relaxation would be limited by the requirement of providing adequate control room contitions for both operators and equipment.
3673	DIT-DRCHITH	Action W	Wills	The logic and reasons for automatic actuation of the VES need further justification. This seems to be unnecessarily complex and may lead to the unwarranted actuation of safeguards equipment which would then require NRC notification and follow up actions. As an example, the VES is actuated on loss of all AC power. Is the automatic actuation required? Could credit be taken for radiation monitors that would allow the deletion of actuation on loss of all AC power?
				Further justify the logic and reasons for automatic actuation of the VES. If the need for automatic actuation cannot be demonstrated consider the design of a manual system.

AP600 Open Item Tracking System: Design Issues Tracking

Date: 12/13/96

Selection: [type] like 'DIT-DRCHITHF' Sorted by Item #

Item No.	Type	(W) Status	Resp Engineer	Description Closure Path Detail Status
3677	DIT-DRCHITH	Action W	Wills	The control room is designed to be leak tight with only minimal leakage expected. With a constant inflow of air from the VBS or VES in certain operating modes it is expected that the control room may overpressurize and impact control room operators and equipment (eg access doors). In addition, a FMEA needs to be conducted on the VES. For example, the fail open of the VES regulator valve and the resulting impact on the control room needs to be addressed. Evaluate the need for a control room overpressure mitigation system.
3685	DIT-DRCHITH	Action W	Wills	The design basis for the number of people in the control room needs to be confirmed and used consistently throughout the various analyses (eg thermal, dose etc.). The frequency of ingress and egress is also input to the dose analyses. It was stated during the presentations that a shift turnover occurred at 4 hours and then once every 12 hours thereafter in the event of an accident. The only ingress and egress occurred at the time of shift turnover. In the committees view this low frequency needs to be clearly justified. Determine the design basis number of people in the control room and determine the shift duration and basis for frequency of ingress and egress to the control room. Utilize these numbers consistently in the analyses.
3691	DIT-DRCHITH	Action W	Wills	It is a technical specification requirement that the flow and pressurization capabilities of the VES be measured. If the VES is tested at power have the impacts on the control room and control room occupants been considered? Perform the assessment if the VES is to be tested at power.
3938	DIT-DRCHITH	Action W	Hutchings	The Current layout arrangement of the spent resin storage tanks does not incorporate adequate shielding or space allocation for maintenance and inspection. The new Spent Resin Storage Tank layout should factor these criteria into the design and arrangement.

Enclosure 3

AP600 Open Item Tracking System: Design Issues Tracking

Date: 12/3/96

Selection: [type] like 'DIT-MMI' Sorted by Item #

Item No.	Type	(W) Status	Resp Engineer	Description Closure Path Detail Status
3465	DIT-MMI	Action W	J. Easter	Safety Parameter Display System (SPDS): Is a 2 second display response time for operator support during transient operations adequate or does it result in operator frustration? Reference: SSAR Chapter 18, subsection 18.8.2.2; NRC letter, "Status of AP600 Draft Safety Evaluation Report (DSER) Open Item Related To Requirements For The Safety Parameter Display System (SPDS)", dtd Sept. 28, 1995. The acceptability of a display response time of 2 seconds for operator support during transient operations is determined during man-in-the-loop concept testing. If 2 seconds is determined to be unacceptable, then a revised display response time is determined.
3466	DIT-MMI	Action W	J. Easter	Safety Parameter Display System (SPDS): Minimum Information; The AP600 human system interface must display suficient information to determine the plant safety status with respect to the SPDS safety functions. Reference: SSAR Chapter 18, subsection 18.8.2.6; NRC letter, "Status of AP600 Draft Safety Evaluation Report (DSER) Open Item Related To Requirements For The Safety Parameter Display System (SPDS)", dtd Sept. 28, 1995. The safety functions and respective parameters presented in Table 2 of NUREG-1342 are used as a starting point for specifying the AP600 SPDS functions and respective parameters. The list needs to be evaluated and revised to address the AP600 passive plant design.
3467	DIT-MMI	Action W	S. Kerch	Open item from ARC USG M-MIS working group: November 1995 presentations to ARC on the computerized procedure system strawman proposed a dynamic roadmap screen and a main interface screen for the computerized procedure system. It was proposed that the dynamic road map information be displayed as part of the wall panel information system display. During the MMI working group session of May 31, 1996; ARC stated that many times, an operator is executing more than one procedure in parallel to control the plant. How is this reflected or incorporated into the dynamic roadmap screen? Reference: Meeting minutes from ARC USG M-MIS Working Group session as documented by ARC letter ARC/FOK0527; dtd June 14, 1996; "ALWR AP600 First-of-a-Kind Engineering Program Minutes From May 31, 1996 ARC USG M-MIS Working Group/Westinghouse Meeting"
3474	DIT-MMI	Action W	M. Lipner / Steve Ke	AP600 main control room operators will execute plant procedures through the computerized procedure system. Current plants, using paper medium, have a process to implement "pen and ink" changes to a paper-based procedure when a situation is encountered where the procedure can not be executed as written. This capability needs to be addressed by the AP600 computerized procedure system.

ENCLOSURE 4

(Only those pages that have changes to them have been enclosed.)

methodology used to arrive at the AP600 level of automation for the plant functions, processes, and systems involved in maintaining plant safety, and documents the results and rationale for function allocation decisions.

18.5 Task Analysis

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

18.6 Staffing

Section 18.6 and Reference 5 provide input from the designer to the Combined License applicant for the determination of the staffing level of the operating crew in the AP600 main control room.

18.7 Integration of Human Reliability Analysis with Human Factors Engineering

Section 18.7 and Reference 6 present the implementation plan for the integration of human reliability analysis with the human factors engineering program.

18.8 Human System Interface Design

Section 18.8 presents the implementation plan for the design of the human system interface.

18.9 Procedure Development

Section 18.9 and Reference 7 provide input to the Combined License applicant for the development of plant operating procedures, including information on the AP600 emergency response guidelines and emergency operating procedures.

18.10 Training Program Development

Section 18.10 and Reference 8 provide input from the designer on the training of the operations personnel who participate as subjects in the human factors verification and validation.

18.11 Human ~~Factors Verification and Validation~~ System Interface Design Test Program

Section 18.11 and Reference 9 present a programmatic level description of the human factors verification and validation.

18.3 Operating Experience Review

The objective of the operating experience review is to identify and analyze human factors engineering-related problems and issues encountered in previous designs that are similar to the AP600. Reference 1 documents the results of this review, including descriptions of how the AP600 design addresses each identified issue.

18.3.1 Combined License Information

~~This section has no requirement for information to be provided in support of the Combined License application.~~

Combined License applicant responsibilities identified in Reference 1 are presented in Sections 10.4.12, 16.2, 18.2.6, 18.6.1 18.9.1 and 18.10.1.

18.3.2 References

1. WCAP-14645, "Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant."

18.5 AP600 Task Analysis Implementation Plan

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

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

This section describes the scope of the AP600 task analysis activities and the task analysis implementation plan. In addition to Reference 1, References 2 through 12 are inputs to this plan.

Insert (1)

18.5.1 Task Analysis Scope

The scope of the AP600 task analysis is divided into two complementary activities: function-based task analysis (FBTA) and traditional task analysis, or operational sequence analysis (OSA). The scope of the function-based task analysis is the Level 4 functions identified in Figure 18.5-1. This figure is the functional decomposition (goal-means analysis) for normal power operations in a standard pressurized water reactor. Examples of functions at Level 4 are "Control RCS Coolant Pressure" and "Control Containment Pressure." This set of functions define the breadth of functions to be analyzed. The function-based task analysis will be expanded in scope to include any additional Level 4 functions identified.

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

- Tasks are selected to represent the full range of operating modes, including startup, normal operations, abnormal and emergency operations, transient conditions, and low-power and shutdown conditions.
- Tasks are selected that involve operator actions that are identified as either critical human actions or risk-important tasks, based on the criteria in Reference 13.
- Tasks are selected to represent the full range of activities in the AP600 emergency response guidelines.
- Tasks are selected that involve maintenance, test, inspection, and surveillance (MTIS) actions. A representative set of maintenance, test, inspection, and surveillance tasks are analyzed for a subset of the "risk-significant" systems/structures/components (SSCs).

The set of tasks to be analyzed are not identified as a part of design certification. The human factors engineering program review model (Reference 1) indicates that task analysis should

Insert (1) on pg.18.5-1: Execution and documentation of this task analysis implementation plan is the responsibility of the Combined License applicant.

Insert (2) on pg.18.5-5: Combined License applicants referencing the AP600 certified design will address the execution and documentation of the task analysis implementation plan presented in section 18.5.

Insert (3) on pg.18.7-1: Execution and documentation of this implementation plan is the responsibility of the Combined License applicant.

Insert (4) on pg.18.7-1: Combined License applicants referencing the AP600 certified design will address the execution and documentation of the human reliability analysis/human factors engineering integration implementation plan that is presented in section 18.7.

Insert (5) on pg. 18.8-1: Execution and documentation of this implementation plan is the responsibility of the Combined License applicant.

Along with insert 5 above, make the 3'rd sentence of the first paragraph under 18.8 the start of a new paragraph.

Insert (6) on pg. 18.8-23: Combined License applicants referencing the AP600 certified design will address the execution and documentation of the human system interface design implementation plan that is presented by section 18.8.

Insert (7) on pg. 18.11-2: Using the programmatic level description, it is the responsibility of the Combined License applicant to develop an implementation plan for the AP600 human factors engineering verification and validation. The Combined License applicant is responsible for the execution and documentation of the plan.

Insert (8) on pg. 18.11-2: Combined License applicants referencing the AP600 certified design will address the development, execution and documentation of an implementation plan for the verification and validation of the AP600 human factors engineering program. The programmatic level description of the AP600 verification and validation program that is presented and referenced by section 18.11 will be used by the Combined License applicant to develop the implementation plan.

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

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

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

18.5.3 Job Design Factors

Section 18.6 addresses the control room staffing that applies to the AP600. The staffing level of the main control room, job design considerations, and crew skills are the responsibility of the Combined License applicant.

18.5.4 Combined License Information Item

Insert (2) →

Combined License applicants referencing the AP600 certified design will ~~address~~ document the scope, and responsibilities, ~~and skills~~ of each main control room position, considering the assumptions and results of the task analysis.

18.5.5 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," 1994.

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

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

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

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

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

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

18.7 Integration of Human Reliability Analysis with Human Factors Engineering

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

The objective of integration of human reliability analysis with human factors engineering is to specify the interfaces between human reliability analysis and human factors engineering activities. Reference 1 documents the implementation plan for the integration of human reliability analysis with human factors engineering design.

Insert (3)

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

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

Human reliability analysis methodology and results are described in Chapter 30 of the AP600 PRA.

18.7.1 Combined License Information

Insert (4)

~~This section has no requirement for information to be provided in support of the Combined License application.~~

18.7.2 References

1. WCAP-14651, "Integration of Human Reliability Analysis with Human Factors Engineering Design Implementation Plan," 1996.

Start a new paragraph.

18.8 Human System Interface Design

Insert (5)

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 (OCS) and each of the human system interface resources. The operation and control centers includes the main control room, the technical support center, the remote shutdown facility, operational support center, local control stations and associated workstations for each of these centers. The AP600 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 station presents information about the plant for use by the operators. No control capabilities are included. The wall panel information station 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. This panel 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 are integrated on this wall panel information station display. The wall panel information station is a nonsafety-related system. It is designed to have a high level of reliability.

The mission of the AP600 alarm system, together with the other human system interface resources, is to provide the operations 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" acuvity, 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 presents plant process information for use by the operators. The plant information system provides dynamic display of plant parameters and alarm information so that an understanding of current plant conditions and status is readily ascertained. The plant information system uses color-graphic video display units located on the operations 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 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 operations 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. Man-in-the-loop concept tests (Reference 9) are planned as part of the human system interface design implementation plan. These tests determine how effectively computerized procedures handle plant situations and whether computer-based procedures adequately support operator performance. 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 backup is evaluated through concept testing or by executing a walk-through using the full-scale mockup of the AP600 main control room. The computerized procedure system and its backup are evaluated as part of the integrated system validation phase of the human factors verification and validation (Reference 24).

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 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 display to the main control room and remote shutdown workstation operators the plant parameters which demonstrate the safety of the plant. The qualified data processing system provides for the display of the variables as described in Section 7.5. ~~The qualified data processing system~~

~~also includes displays that help the operator use nonsafety-related systems in responding to certain types of events.~~

18.8.1 Implementation Plan for the Human System Interface Design

Figure 18.2-3 provides an overview of the AP600 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 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 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 are applied to an appropriate set of human factors engineering design guidelines to develop the design specifications. The design specifications are provided as input to the hardware and software system designers for design implementation. Rapid prototyping and man-in-the-loop concept testing are performed to establish that the human system interface design of the main control room adequately supports operator performance in the range of activities and situations that are anticipated to arise. The results of the concept testing are used to refine the functional requirements and the design specifications of the operation and control centers and the human system interface.

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 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 AP600 operations and control centers, including the main control room, the technical support center, the remote shutdown facility, 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

18.8.4.1.8 Storage

Storage facilities are identified in the AP600. Radioactively clean and contaminated storage areas are designated.

18.8.4.1.9 Coding and Labeling

Equipment located in the AP600 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

Insert (6)

~~This section has no requirement for information to be provided in support of the Combined License application.~~

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.

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.

4. NUREG-1358, "Lessons Learned from the Special Inspection Program for Emergency," U.S. Nuclear Regulatory Commission, Washington, D.C., April 1989.

5. NUREG-0700, "Human-System Interface Design Review Guideline," Rev. 1, U.S. Nuclear Regulatory Commission, Washington, D.C., February 1995. (Draft Report)

6. NUREG/CR-5908, "Advanced Human-System Interface Design Guidelines," U.S. Nuclear Regulatory Commission, Washington, D.C., July 1994.

- Evaluations for controlling plant state
- Evaluations of conformance to human factors engineering design guidelines
- Evaluations for validation of the integrated human system interface

The first 15 issues are grouped into the first three headings above.

As described in subsection 18.8.1, man-in-the-loop concept tests are performed as part of the human system interface design process. These concept tests are organized around the first 15 human performance issues. Reference 2 provides a description of the AP600 man-in-the-loop test plan which includes the concept tests.

Evaluation issues 16 and 17 describe evaluations that are performed as part of the AP600 human factors verification and validation and fall under the last two headings above. A programmatic level description of the AP600 verification and validation program is provided by Reference 3. Figure 18.8-2 shows the man-in-the-loop concept testing and the verification and validation activities conducted as part of AP600 human factors engineering program.

Insert (7)

18.11.1 Combined License Information

Insert (8)

~~This section has no requirement for information to be provided in support of the Combined License application.~~

18.11.2 References

1. WCAP-14701, "Methodology and Results Of Defining Evaluation Issues For the AP600 Human System Interface Design Test Program."

2. WCAP-14396, "Man-In-The-Loop Test Plan Description."

3. WCAP-14401, "Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan."

18.12 ~~Displays, Alarms, and Controls~~ Inventory

18.12.1 Inventory of Displays, Alarms, and Controls

An inventory of instruments, alarms, and controls for the AP600 systems is provided in the respective system piping and instrumentation diagrams.

The AP600 system design engineers determine the specific sensors, instrumentation, controls, and alarms that are needed to operate the various plant systems. The instruments, alarms, and controls for each system are documented in the piping and instrumentation diagram. An instrument, alarm, and control is specified by the system design engineer if it is needed to control, verify, or monitor the operation of the system and its components. System functions and their respective functional requirements are considered by the system designer when determining the need for a specific instrument, alarm, or control.

The role of the Human Factors Engineering (HFE) design team in the determination of the total inventory list is one of verification. As described in Section 18.5, the Human Factors Engineering design team has functionally decomposed the plant. The top four levels of this model for the AP600, are shown in Figure 18.5-1. Each Level 4 function has a function-based task analysis (FBTA) performed as described in the Task Analysis Implementation Plan. Considering the plant operating modes and emergency operations, the function-based task analysis:

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

The cognitive task analysis of each process answers the monitoring/feedback, planning, and controlling questions. The answers to these questions identify the data for each functional process (instrumentation, indications, alarms, and controls) needed by the operator to make decisions. The results of the cognitive task analysis phase of each function-based task analysis are used to verify the inventory list of instruments, controls, and alarms developed by the AP600 system designers and documented in the respective design documents.

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

Background

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

Table 1.8-2 (Sheet 4 of 4)

SUMMARY OF AP600 STANDAKD PLANT COMBINED LICENSE INFORMATION ITEMS

Item No.	Subject	Subsection
12.5-1	Radiological Protection Organization and Procedures	12.5.5
13.1-1	Organizational Structure of Combined License Applicant	13.1.1
13.2-1	Training Program for Plant Personnel	13.2.1
13.3-1	Emergency Planning and Communications	13.3.1
13.4-1	Operational Review	13.4.1
13.5-1	Plant Procedures	13.5.1
13.6-1	Security Plans, Organization and Testing	13.6.13.1
13.6-2	Vital Equipment	13.6.13.2
13.6-3	Plant Security System	13.6.13.3
13.6-4	Vulnerability Analysis Report	13.6.13.4
14.4-1	Initial Test Program	14.4
16.2-1	Design Reliability Assurance Program/Site Specific	16.2.7.1
16.2-2	Operational Reliability Assurance Activities	16.2.7.2
18.6-1	Plant Staffing	18.6.1
18.3-1	Operating Experience Review	18.3.1
18.5-1	Task Analysis	18.5.4