Westinghouse Non-Proprietary Class 3

WCAP-14645
Revision 1

Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant

Westinghouse Energy Systems

Westinghouse Non-Proprietary Class 3

WCAP-14645
Revision 1

Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant

Westinghouse Energy Systems

AP600 DOCUMENT COVER SHEET

Form 58202G(5/94) [m:\3252w-1.wpf]
0058.FRM

AP600 CENTRAL FILE USE ONLY: TDC: ______ IDS: I ______ S ______

RFS#: RFS ITEM #:

AP600 DOCUMENT NO.	REVISION NO.		ASSIGNED TO
OCS-GJR-001	1	Page 1 of ___	

ALTERNATE DOCUMENT NUMBER: WCAP-14645, Rev. 1 WORK BREAKDOWN #:

DESIGN AGENT ORGANIZATION: Westinghouse Electric

PROJECT: AP600

TITLE: Human Factors Engineering Operating Experience Review Report for the AP600 Nuclear Power Plant

ATTACHMENTS:	DCP #/REV. INCORPORATED IN THIS DOCUMENT REVISION:
CALCULATION/ANALYSIS REFERENCE:	

ELECTRONIC FILENAME	ELECTRONIC FILE FORMAT	ELECTRONIC FILE DESCRIPTION
m:\3265w.wpf m:\3265w-1.wpf	WordPerfect 5.2	

ORIGINATOR	SIGNATURE/DATE	
S. P. Kerch	S.P. Kerch	10/17/96
AP600 RESPONSIBLE MANAGER	**SIGNATURE***	**APPROVAL DATE**
J. B. Reid	[signature] for JBR	10/17/96

*Approval of the responsible manager signifies that document is complete, all required reviews are complete, electronic file is attached and document is released for use.

Form 58202G(5/94)

LIMITED RIGHTS STATEMENTS

DOE GOVERNMENT LIMITED RIGHTS STATEMENT

(A) These data are submitted with limited rights under government contract No. DE-AC03-90SF18495. These data may be reproduced and used by the government with the express limitation that they will not, without written permission of the contractor, be used for purposes of manufacturer nor disclosed outside the government; except that the government may disclose these data outside the government for the following purposes, if any, provided that the government makes such disclosure subject to prohibition against further use and disclosure:
  (I) This "Proprietary Data" may be disclosed for evaluation purposes under the restrictions above.
  (II) The "Proprietary Data" may be disclosed to the Electric Power Research Institute (EPRI), electric utility representatives and their direct consultants, excluding direct commercial competitors, and the DOE National Laboratories under the prohibitions and restrictions above.

(B) This notice shall be marked on any reproduction of these data, in whole or in part.

ARC LIMITED RIGHTS STATEMENT:

This proprietary data, furnished under Subcontract Number ARC-93-3-SC-001 with ARC may be duplicated and used by the government and ARC, subject to the limitations of Article H-17.F. of that subcontract, with the express limitations that the proprietary data may not be disclosed outside the government or ARC, or ARC's Class 1 & 3 members or EPRI or be used for purposes of manufacture without prior permission of the Subcontractor, except that further disclosure or use may be made solely for the following purposes:

This proprietary data may be disclosed to other than commercial competitors of Subcontractor for evaluation purposes of this subcontract under the restriction that the proprietary data be retained in confidence and not be further disclosed, and subject to the terms of a non-disclosure agreement between the Subcontractor and that organization, excluding DOE and its contractors.

DEFINITIONS

CONTRACT/DELIVERED DATA — Consists of documents (e.g. specifications, drawings, reports) which are generated under the DOE or ARC contracts which contain no background proprietary data.

EPRI CONFIDENTIALITY / OBLIGATION NOTICES

NOTICE 1: The data in this document is subject to no confidentiality obligations.

NOTICE 2: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for limited purposes only. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited except as agreed to in advance by the Electric Power Research Institute (EPRI) and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted.

NOTICE 3: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is forwarded to recipient under an obligation of Confidence and Trust for use only in evaluation tasks specifically authorized by the Electric Power Research Institute (EPRI). Any use, disclosure to unauthorized persons, or copying this document or parts thereof is prohibited except as agreed to in advance by EPRI and Westinghouse Electric Corporation. Recipient of this data has a duty to inquire of EPRI and/or Westinghouse as to the uses of the information contained herein that are permitted. This document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 4: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. It is being revealed in confidence and trust only to Employees of EPRI and to certain contractors of EPRI for limited evaluation tasks authorized by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. This Document and any copies or excerpts thereof that may have been generated are to be returned to Westinghouse, directly or through EPRI, when requested to do so.

NOTICE 5: The data in this document is proprietary and confidential to Westinghouse Electric Corporation and/or its Contractors. Access to this data is given in Confidence and Trust only at Westinghouse facilities for limited evaluation tasks assigned by EPRI. Any use, disclosure to unauthorized persons, or copying of this document or parts thereof is prohibited. Neither this document nor any excerpts therefrom are to be removed from Westinghouse facilities.

EPRI CONFIDENTIALITY / OBLIGATION CATEGORIES

CATEGORY "A" — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is contained in an issued reported.

CATEGORY "B" — (See Delivered Data) Consists of CONTRACTOR Foreground Data that is not contained in an issued report, except for computer programs.

CATEGORY "C" — Consists of CONTRACTOR Background Data except for computer programs.

CATEGORY "D" — Consists of computer programs developed in the course of performing the Work.

CATEGORY "E" — Consists of computer programs developed prior to the Effective Date or after the Effective Date but outside the scope of the Work.

CATEGORY "F" — Consists of administrative plans and administrative reports.

WCAP-14645 Rev. 1

HUMAN FACTORS ENGINEERING
OPERATING EXPERIENCE REVIEW REPORT
FOR THE AP600 NUCLEAR POWER PLANT

October, 1996

AP600 Document Number: OCS-GJR-001

S. P. Kerch
R. M. Span

Westinghouse Electric Corporation
Energy Systems Business Unit
P.O. Box 355
Pittsburgh, Pennsylvania 15230-0355

TABLE OF CONTENTS

1.0 INTRODUCTION 1-1

2.0 SCOPE 2-1

3.0 RESULTS OF REVIEWING OPERATOR EXPERIENCE ISSUES 3-1

4.0 RELATED HUMAN SYSTEM INTERFACE (HSI) TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR PLANT EXPERIENCE EXISTS 4-1

5.0 CONTENT AND RESOLUTION OF OPERATOR INTERVIEWS 5-1

LIST OF TABLES AND REFERENCES

Table 1 Operating Experience Review for the AP600 Design T-1

References For Table 1, Operating Experience Review for the AP600 Design T-66

Table 2 Related HSI Technologies Where Little Or No Nuclear Experience Exists T-67

References For Table 2, Related HSI Technologies Where Little Or No Nuclear Experience Exists T-72

Table 3 Operator Interview Issues T-73

References For Table 3, Operator Interview Issues T-78

ACRONYMS

ac	Alternating Current
ADS	Automatic Depressurization System
ARM	Area Radiation Monitor
AFW	Auxiliary Feedwater
ASHRAE	American Society of Heating, Refrigeration, and Air-Conditioning Engineers
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
BWR	Boiling Water Reactors
CCS	Component Cooling Water System
CIV	Containment Isolation Valve
CMT	Core Makeup Tank
COL	Combined License
CPS	Computerized Procedure System
CR	Control Room
CRT	Cathode Ray Tube
CSF	Critical Safety Functions
CST	Condensate Storage Tank
CV	Check Valve
CWS	Circulating Water System
D-RAP	Design Reliability Assurance Program
DAS	Diverse Actuation System
dc	Direct Current
DDS	Data Display and Processing System
DSER	Draft Safety Evaluation Report
EMI	Electromagnetic Interference
EOF	Emergency Offsite Facility
EOP	Emergency Operating Procedures
ERG	Emergency Response Guidelines
ESF	Engineered Safety Features
FBTA	Function-Based Task Analysis
FC	Function Centralization
HFE	Human Factors Engineering
HSI	Human System Interface
HVAC	Heating, Ventilation, and Air-Conditioning
HX	Heat Exchangers
IA	Instrument Air
I&C	Instrumentation and Control
IRM	Intermediate Range Monitors
IRWST	In-Containment Refueling Water Storage Tank
ISLOCA	Interfacing System LOCA
IST	Inservice Test
LCS	Local Control Station
LOCA	Loss of Coolant Accident
MCR	Main Control Room
MFP	Main Feedwater Pump
MMI	Man-Machine Interface
M-MIS	Man-Machine Interface System

ACRONYMS (Continued)

NPP	Nuclear Power Plant
NSR	Non-Safety Related
OER	Operating Experience Review
OSC	Operational Support Center
PABX	Private Automatic Branch Exchange
PAR	Passive Autocatalytic Recombiners
PDP	Positive Displacement Charging Pump
PHWR	Pressurized Heavy Water Reactor
PLS	Plant Control System
PMS	Protection and Safety Monitoring System
PORV	Power Operated Relief Valve
PRA	Probabilistic Risk Assessment
PRHR	Passive RHR
PWR	Pressurized Water Reactor
PXS	Passive Core Cooling System
QDPS	Qualified Data Processing System
RAI	Request for Additional Information
RCS	Reactor Coolant System
RF	Radio Frequency
RHR	Residual Heat Removal
RMS	Radiation Monitoring System
RNS	Normal Residual Heat Removal System
RV	Reactor Vessel
SART	Silence, Acknowledge and Restart Test
SBO	Station Blackout
SFS	Startup Feedwater System
SG	Steam Generator
SGL	Steam Generator Level
SGTR	Steam Generator Tube Rupture
SPDS	Safety Parameter Display System
SR	Safety-Related
SRP	Standard Review Plan
SRO	Senior Reactor Operator
SRV	Safety Relief Valve
SSAR	Standard Safety Analysis Report
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
STA	Shift Technical Adviser
SWS	Service Water System
TIP	Traveling Incore Probe
TS	Technical Specifications
TSC	Technical Support Center
UPS	Uninterruptable Power Supply
VBS	Nuclear Island Non-Radioactive Ventilation System
VDU	Visual Display Unit
VES	Emergency Habitability System
VPI	Valve Position Indication
WPIS	Wall Panel Information System

1.0 INTRODUCTION

As discussed in NUREG-0711 ("Human Factors Engineering Program Review Model"), the purpose of this operating experience review (OER) is to identify human factors engineering (HFE)-related safety issues. The objective of this AP600 review is to identify and analyze HFE-related problems and issues encountered in previous designs that are similar to the AP600 so that they are avoided in the development of the AP600 design, or in the case of positive features, to retain these features. Westinghouse will continue to review current plant operating experience and as new HFE-related issues are identified, will address or track to resolution those issues applicable to the AP600.

2.0 SCOPE

The scope of this evaluation includes pressurized water reactors (PWRs), at both Westinghouse and non-Westinghouse plants. The issues for boiling water reactors (BWRs) and a pressurized heavy water reactor (PHWR) which are applicable to the AP600 design are also addressed. Other industry man-machine interface (MMI) experience, where limited experience exists in the nuclear industry, is also addressed.

Guidance for this OER is based upon: 1) Appendix B of NUREG-0711, 2) the clarification of NUREG-0711 Appendices B.5 and B.6 provided as an attachment, ("HFE Insights For Advanced Reactors Based Upon Operation Experience," BNL Technical Report E2090-4-3-1/95) to NRC letter dated 2/13/95, and 3) comments in Draft Safety Evaluation Report (DSER) Chapter 20 related to the OER for the AP600.

3.0 RESULTS OF REVIEWING OPERATING EXPERIENCE ISSUES

Table 1 documents the NUREG-0711 Appendix B issues reviewed and how the AP600 design addresses these issues. Table 1 consists of five columns and provides the following information;

Column 1	Item
Column 2	Issue Reference
Column 3	Issue/Scope
Column 4	Human Factors Aspect/Human Performance Issue
Column 5	Human Factors/Human Performance Issue Addressed by AP600 Design

The numbers in column 1 are used throughout this document as a convenient means to reference the various issues. Column 2 identifies the reference document that presents the issue to be addressed. Column 3 identifies the specific issue/scope. Column 4 identifies the human factors aspect/human performance issue of the issue/scope identified in column 3. Column 5 documents how the AP600 design addresses the aspects/issues identified in column 4.

Tables 1, 2, and 3 also document the HFE-related issues which are not currently addressed by the AP600 design. These issues are identified in column 5 of Table 1 and in column 3 of Tables 2 and 3 by using the terminology "THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM" typed in **bold** letters. Standard Safety Analysis Report (SSAR) subsection 18.2.4 provides a description of the design issues tracking system which includes tracking of HFE issues.

Column 5 of Table 1 also identifies which HFE issues are not applicable to the AP600 design. These are identified in column 5 of Table 1 by using the terminology "NOT APPLICABLE" typed in **bold** letters. Immediately after the bold type, the reason why the issue in not applicable to the AP600 is provided.

Column 5 of Table 1 may identify the issue or part of the issue as "the responsibility of the Combined License (COL) applicant." The following is a list of those items from Table 1 that are identified totally or partially as the responsibility of the COL applicant: 1, 21, 45, 48, 49, 50, 51, 58, 63, 64, 65, 67 through 70, 157, 168, and 170 through 180.

4.0 RELATED HUMAN SYSTEM INTERFACE (HSI) TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR PLANT EXPERIENCE EXISTS

Soft controls, computerized procedures, and large screen (wall panel) displays are HSI technologies that are not used in currently operating nuclear power plants, but will be used in the HSI/M-MIS design of the AP600. Westinghouse has reviewed the operating experience of these technologies or related technologies from other industries in order to identify HFE-related issues that need to be addressed. Issues related to these technologies include navigating through large display networks, implementation of soft controls, and group situation awareness.

The AP600 computerized procedure system (CPS) is dynamic and interactive with the remaining AP600 HSI. Plant parameter values, plant state, and assessment of procedure steps are performed by the system. No system comparable to the capabilities of the AP600 CPS, with relevant operating experience, was found in other industries. If any such experience is published, it will be reviewed and identified human factors issues will be addressed.

The reviewed documents include operating experience from the following industries: fossil power plant, aircraft industry, naval programs, space program, electrical, gas, and oil. These reviews are documented in Table 2. Column 1 of Table 2 identifies the reference document which was reviewed. Column 2 identifies the HFE-related issues applicable to the AP600 design, and column 3 documents how the AP600 design addresses the identified HFE-related issues. In column 3, some cross-referencing to Table 1 occurs where the identified issue is identical to an issue already documented in Table 1. Where the issue is not currently addressed by the AP600 design, an entry is made in column 3 stating "THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM" typed in **bold** letters. The reference documents in Table 2 (References 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, and 2.7) are identified in the Reference list following Table 2.

Column 3 of Table 2 may identify the issue or part of the issue as "the responsibility of the Combined License (COL) applicant." The following is a list of those items from Table 2 that are identified totally or partially as the responsibility of the COL applicant: Ref. 2.3 item 2; Ref. 2.4 items 3, 4, and 8; Ref. 2.6 item 4; and Ref. 2.7 items 3 and 5.

5.0 CONTENT AND RESOLUTION OF OPERATOR INTERVIEWS

As part of the OER, Westinghouse has conducted operator interviews and observations during plant operations and after operating events. These interviews/observations are documented in Table 3. Column 1 of Table 3 identifies the reference that documents the operator interviews. Column 2 identifies the HFE-related issues applicable to the AP600 design, and column 3 documents how the AP600 design addresses the identified HFE-related issues. In column 3, some cross-referencing to Table 1 occurs where the identified issue is identical to an issue already documented in Table 1. Where the issue is not currently addressed by the AP600 design, an entry is made in column 3 stating "THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM" typed in **bold** letters. The reference documents in Table 3 (References 3.1, 3.2, 3.3, 3.4, 3.5, 3.6, 3.7, and 3.8) are identified in the Reference list following Table 3.

Column 3 of Table 3 may identify the issue or part of the issue as "the responsibility of the Combined License (COL) applicant." The following is a list of those items from Table 3 that are identified totally or partially as the responsibility of the COL applicant: Ref. 3.1 items 1, 2, 3, 4, and 5; Ref. 3.2 items 2, 3, and 4; Ref. 3.4 items 1, 2, and 3; Ref. 3.5 item 6; Ref. 3.6 items 1 and 2; and Ref. 3.7/3.8 items 2, 4, and 6.

TABLE 1

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
1	Item B.1 (1)	A-44, Station blackout (SBO)	This is a large and significant issue with many human-factors-related aspects, including controls, displays, training, and procedures.	A station blackout (SBO) is a design basis event for the AP600. Passive, safety-related systems utilize one-time realignment of valves to provide system initiation. After initiation, these passive systems do not require power to sustain their operation. For an SBO event, the valves that align the AP600 systems required to mitigate the event are fail-safe or battery-powered valves. Fail-safe means that on loss-of-power they move to the position that initiates system operation. Refer to SSAR subsection 7.4.1.1 for a description of the process and plant response that establishes safe shutdown conditions for the plant, using the safety-related systems and no operator action. This discussion only considers the use of safety-related systems and it assumes loss of offsite electrical power at the start of the event. Table 7.5-1 of Section 7.5 of the SSAR summarizes information on the instrumentation for post-accident monitoring. The post-accident monitoring instrumentation that is designated in the table to be displayed by the Qualified Data Processing System (QDPS) is powered from a Class 1E dc uninterruptible power system (UPS) with sufficient battery capacity to provide necessary electrical power for 72 hours. As noted in SSAR Section 7.5.4 and notes 4 and 7 of Table 7.5-1, there are a few cases where the instrumentation is powered from a 24-hour Class 1E battery. Refer to SSAR subsections 8.1.2 and 8.3.2.1 for a description of the Onsite Power System and the DC Power System. The QDPS cabinets are powered from a Class 1E 72-hour battery. The AP600 man-machine interface system (M-MIS) for controls in the main control room (MCR) consists of soft controls at the operator workstations and dedicated controls at the dedicated safety panel. Reactor operator and senior reactor operator (SRO) workstations and their displays are powered from non-1E uninterruptable power supplies. The workstations will be available for 2 hours into the SBO. After 2 hours the operators rely on the QDPS displays and the dedicated controls for control and monitoring of the plant. The QDPS provides the Class 1E, qualified display system and is powered from the Class 1E UPS. The QDPS and the dedicated controls are located at the dedicated safety panel. The design of the QDPS displays, dedicated controls, and the dedicated safety panel are all part of the Human System Interface (HSI) and therefore will be a product of the AP600 HSI design process as described in Section 18.8 of the SSAR. The dedicated controls, located on the dedicated safety panel, are for reactor trip, turbine trip, and system-level engineered safety features (ESF) actuations. These dedicated controls are powered for 24 hours from a Class 1E battery through a UPS, following an SBO. Refer to Table 8.3.2-1 for the list of safety-related loads powered from the Class 1E batteries. Training program development and procedure development are the responsibility of the COL applicant as stated in 13.2 and 13.5 of the SSAR.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
2	Item B.1 (2)	A-47, Safety implications of control systems	This issue relates to the implications of failures of nonsafety-related (NSR) control systems and their interaction with control room (CR) operators.	WCAP-14477, "The AP600 Adverse Systems Interactions Report" provides an evaluation of potential adverse interactions between the plant control system and the safety-related systems designed to mitigate accidents. This report provides the justification for inclusion or exclusion of control-grade equipment and systems in the Chapter 15 accident analyses. The implications of failures of nonsafety-related control systems and their interaction with control room operators is addressed in the AP600 Emergency Response Guidelines (ERGs). The ERGs provide both optimal recovery guidelines and function restoration guidelines using both safety-related systems and nonsafety-related systems as appropriate. Contingencies are provided to account for failures of either safety-related or nonsafety-related systems.
3	Item B.1 (3)	B-17, Criteria for safety-related (SR) operator actions	This issue involves the development of a time criterion for safety-related operator actions including a determination of whether automatic actuation is required. This issue also concerns some current PWR designs requiring manual operations to accomplish the switchover from the injection mode to the recirculation mode after a loss-of-coolant accident (LOCA).	WCAP 14644, "AP600 Functional Requirements Analysis and Function Allocation," provides a description of the basis for automatic actuations of accident mitigation (critical safety) functions and the associated capabilities for manual operations. The AP600 provides automatic mitigation of design basis accidents including initiation of the long term post-LOCA recirculation mode. Recovery actions for various emergency scenarios are specified in the AP600 ERGs and take operator action timing into consideration.
4	Item B.1 (4)	B-32, Ice effects on safety-related water supplies	The buildup of ice on service water intake can occur gradually and can require improved instrumentation to allow operators to detect its occurrence before it causes system inoperability.	The service water system (SWS) in AP600 is nonsafety-related. Refer to SSAR subsection 9.2.1 for a description of the SWS. SWS water temperature is monitored and alarmed in the MCR on low temperature. Low temperature alarm is a warning on potential icing conditions.
5	Item B.1 (5)	GI-2, Failure of protective devices on essential equipment	A large number of licensee event reports have noted the incapacitation of safety-related equipment because of the failure of protective devices, such as fuses and circuit breakers. Operators are not always aware of the failure of equipment because of the design of the instrumentation.	The AP600 is designed to minimize the effects of failures of protective devices on essential equipment. • The number of active essential devices has been minimized by the passive design of the AP600. • The AP600 is provided with an extensive distributed (nonsafety) control system that can be used by the operator to monitor the operation of the plant and quickly identify inoperable devices. • The AP600 conforms with Regulatory Guide 1.106 for the application of thermal overload protection devices. • Redundant motor-operated valves are powered by independent divisions of the Class 1E dc system. The four divisions of the Class 1E dc system are completely independent with no provision for cross-connect.
6	Item B.1 (6)	GI-23, Reactor coolant pump seal failures	This is a multifaceted issue that includes a number of proposed resolutions. One subissue is the provision of adequate seal instrumentation to allow the operators to take corrective actions to prevent catastrophic failure of seals.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
7	Item B.1 (7)	GI-51, Improving the reliability of open-cycle service water systems.	The buildup of clams, mussels, and corrosion products can cause the degradation of open cycle SWSs. Added instrumentation is one means of providing operators with the capability to monitor this buildup and take corrective action before loss of system functionality occurs.	The AP600 SWS and Circulating Water System (CWS) are nonsafety-related (NSR). The AP600 uses chemical control in the SWS (SSAR 9.2.1.2.2) and CWS (SSAR 10.4.5.2.2). The COL applicant will address the specific chemicals used for water chemistry control, algicide, and biocide applications, reflecting potential variations in site water chemistry and in micro and macrobiological life forms (SSAR 9.2.1.6 and 10.4.12.1 respectively). Chlorine residual is monitored in each system in order to assure that effective biocide treatment is being implemented.
8	Item B.1 (8)	GI-57, Effects of fire protection system actuation on safety-related equipment.	This issue resulted from spurious and inadvertent actuations of fire protection systems, often caused by operator errors during testing or maintenance. Design of systems should prevent such errors to the extent possible.	An explicit requirement exists to design the system such that inadvertent operations do not occur (SSAR 9.5.1.1.1, Rev. 4). There are no sprinkler systems or automatically initiated fire protection systems in areas containing safety-related components. (5.1.2.1.4 - SSAR Rev. 4). Also an evaluation of the fire protection system integrity analysis is performed for safety-related systems. The system is designed to be in compliance with BTP CMEB 9.5-1.
9	Item B.1 (9)	GI-75, Generic implications of Anticipated Transient without Scram (ATWS)	This issue has many subissues, several of which are related to human factors, for example, scram data for post-scram analysis, capability for post-maintenance testing of reactor protection system, and a specific subissue titled "Review of human factors issues."	The AP600 includes a DAS that provides a diverse backup to the protection system. This system is a nonsafety-related instrumentation and control (I&C) system that is an expanded version of the ATWS Mitigation System Actuation Cabinets in the present generation Westinghouse nuclear power plants. One of the functional requirements of the DAS is to mitigate consequences of a failure to trip following an ATWS. The DAS provides a diverse, alternate means of automatically tripping the reactor and actuating specified ESF functions for selected events if the Protection and Safety Monitoring System (PMS) is unable to perform these functions as a result of common mode failure. A more detailed description of the DAS, including the diverse nature of the system, is found in SSAR subsection 7.7.1.11. The AP600 I&C systems includes a Data Display and Processing System (DDS). One of the functions provided by the DDS is a distributed computer function. The distributed computer function provides data acquisition, data storage, and computational functions to support operations, engineering plant information needs and emergency response information needs within a single system. The distributed computer function interacts with the plant operators through the operational display function and the plant information system. The distributed computer function provides many computational functions, including provisions for pre- and post-trip data for review and analysis, historical data storage and retrieval, and data logging. The AP600 PMS is a safety system of electrical and mechanical equipment that senses generating station conditions, and generates the signals to actuate reactor trip and ESFs that provide the equipment necessary to monitor plant safety-related functions during and following designated events (Reference SSAR Section 7.1). The PMS provides a high degree of reliability and fault tolerance for both operating and maintenance situations. SSAR subsection 7.1.2.10 describes the specific design features that provide this capability. SSAR subsection 7.1.2.12 describes the PMS test capabilities and design features. The AP600 reactor trip switchgear has four redundant safety divisions with each division containing two circuit breakers of the reactor trip switchgear (eight breakers total). As illustrated in SSAR Figure 7.1-7, the eight circuit breakers are arranged in a two-out-of-four logic configuration (Reference SSAR subsection 7.1.2.5).

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
10	Item B.1 (10)	GI-76, I&C interactions	This issue raises several concerns, including I&C faults that could blind or partially blind the operators to the status of the plant.	The design of the operator displays is based on an analysis which identifies the appropriate display variables for monitoring conditions in the reactor coolant system (RCS), the secondary heat removal system, the containment, and the systems used for attaining a safe shutdown condition. This analysis also establishes the appropriate design basis and qualification criteria for the instrumentation which provides the input to the operator displays (Reference SSAR Section 7.5). In addition to these displays, the DAS provides separate and diverse indications which can be used by the operator. Refer to the responses of items 59, and 113 through 119 for design features of the AP600 dc Power Systems.
11	Item B.1 (11)	GI-96, Residual heat removal (RHR) suction valve testing	The design of the RHR suction valves with respect to valve position indication and instrumentation to detect potential leakage from high-to-low pressure areas is important to the prevention of interfacing system loss-of-coolant accidents (ISLOCAs). This is important for normal operations and for testing.	Based upon a conference call of 6/19/95 with the NRC Human Factors Branch, it was agreed not to include this issue as part of the OER (Reference 8).
12	Item B.1 (12)	GI-101, Break plus single failure in boiling water reactor water level instrumentation	This issue attempts to ensure that robust information is available to the operators for both reactor water level and for plant status during the progression of an accident.	Based upon a conference call of 6/19/95 with the NRC Human Factors Branch, it was agreed not to include this issue as part of the OER (Reference 8).
13	Item B.1 (13)	GI-105, Interfacing system LOCA at BWRs	This issue relates to pressure isolation valves for BWRs.	**NOT APPLICABLE:** This issue relating to pressure isolation valves is only applicable to BWR reactors.
14	Item B.1 (14)	GI-110, Equipment protective devices of engineered safety features	Failures and incapacitation of ESF equipment have occurred because of the failure or intentional bypass of protective devices. Both the design of these protective devices and the appropriate indication to CR operators are important.	The ESF design is based on the use of four separate safety divisions for the sense and command function, and two or more divisions for the execute function. The system is designed to accommodate a single failure of a process signal input by altering the sense and command logic from a two-out-of four voting logic to a two-out-of-three voting logic. Additional failures can be accommodated by altering the logic from a two-out-of-three to a one-out-of-two. Any attempt to accommodate addition failures by an intentional bypass results in actuation of the protective function. Alarms and displays are provided so that the configuration of the ESF can be determined by the operator at any time.
15	Item B.1 (15)	GI-116, Accident management	This issue relates to improved operator training and procedures for managing accidents beyond the design basis of the plant.	Based upon a conference call of 6/19/95 with the NRC Human Factors Branch, it was agreed not to include this issue as part of the OER (Reference 8).

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
16	Item B.1 (16)	GI-117, Allowable equipment outage times for diverse, simultaneous equipment outages	A key aspect of this item is providing operators with needed assistance in identifying risk-significant combinations of equipment outages. The information needed would include valve alignments, switch settings, as well as components declared inoperable.	For the AP600, the Wall Panel Information System (WPIS) will display for each plant operating mode or significant plant operating state, a mimic display that will provide a physical overview of the status of the plant's significant systems and key components. The wall panel mimic display will include the display of high-level derived quantities, e.g., those that depend on a particular logic algorithm. An example of a derived quantity is the availability of safety systems. The WPIS will provide information to the MCR personnel summarizing those components and systems that are inoperable. The AP600 Wall Panel overview alarm displays, along with the Visual Display Unit (VDU) displays, will automatically present indication of bypassed or deliberately induced inoperable safety equipment. This will include the bypassing or deliberately induced inoperability of any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system and the systems actuated or controlled by the protection system. The QDPS will contain physical displays for the representation of the performance of systems and components associated with the control of safety-related functions. These physical displays will contain enough data so that the operator can monitor the operation of the plant hardware. The type of information to be put on these displays will be derived through a function-based task analysis process (FBTA). Indicatively, the type of information to be shown on the physical displays could be of the following types: 1) flow path alignments; 2) valve positions; 3) pump states; 4) tank levels and capacities; 5) heat exchangers heat balance; 6) availability status of the support systems (electricity, cooling, etc...); 7) system or component interlocks; 8) system or component operating rules; 9) important data with interfacing systems.
17	Item B.1 (17)	GI-120, On-line testability of protection systems	The designs for on-line testability should include appropriate human factors to ensure safe testing.	The on-line testing of the protection systems is accomplished by a series of tests with sufficient overlap to test all necessary functions. Most of the testing is performed automatically once initiated by the operator. A description of the system reliability and fault tolerance during operations, maintenance, test and bypass, and a description of the built-in test capabilities are provided in SSAR subsections 7.1.2.10 and 7.1.2.12.
18	Item B.1 (18)	GI-125.I.3, Safety parameter display system availability	This issue addresses Safety Parameter Display System (SPDS) availability and the reliability of the information it displays.	Based upon a conference call of 6/19/95 with the NRC Human Factors Branch, it was agreed not to include this issue as part of the OER (Reference 8).
19	Item B.1 (19)	GI-128, Electrical power reliability	This issue includes power to vital instrument buses, direct current (dc) power supplies, and electrical interlocks. All of these issues are strongly dependent on proper indication and operator action for high reliability.	Generic Issue 128 was created by combining Issues 48, 49, and A-30. Resolution of Issue A-30 is contained in Generic Letter 91-06. The AP600 response to Generic Letter 91-06 is contained in Item 59 below. The resolutions of Issues 48 and 49 are contained in Generic Letter 91-11. The AP600 response to Generic Letter 91-11 is contained in Item 61 below. The AP600 response to Generic Issue 128 is summarized in SSAR subsection 1.9.4.2, item 128.
20	Item B.1 (20)	GI-130, Essential service water pump failures at multi-plant sites	This issue relates to the arrangement of SWS pumps and piping, including cross-ties at multi-unit sites. Both the arrangement and the operators' ability to monitor the status of cross-ties are important. This item mentions potential applicability to single-unit sites also.	The AP600 is a single-unit design. If two AP600s are placed on the same site, they will not share an SWS. The AP600 SWS is a nonsafety-related system. Cross-ties are internal to the SWS from one train to another. Proper cross-tie alignment can be determined by monitoring the Component Cooling Water System (CCS) heat exchanger (HX) temperature rise. If the rise is excessive, an alarm will be sent to the MCR indicating possible cross-tie misalignment. There is a blowdown path from the SWS to the CWS that is normally open. Closing this path has no effect on the SWS pumps.

TABLE 1 (Continued)

OP"RATING EXPERIENCE REVIEW FOR THE AP600

I-sues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
21	Item B.1 (21)	HF1.1	This issue is similar to Item I.A.1.4 in Section B.2 (item 48 of this table).	Staffing levels are the responsibility of the COL applicant as stated in SSAR Section 18.6.
22	Item B.1 (22)	HF4.4, Guidelines for upgrading other procedures	This issue addresses normal and abnormal procedures in the same manner as emergency procedures.	Based upon a conference call of 6/19/95 with the NRC Human Factors Branch, it was agreed not to include this issue as part of the OER (Reference 8).
23	Item B.1 (23)	HF4.5, M-MIS automation and artificial intelligence	See HF5.2 below.	Based upon a conference call of 6/19/95 with the NRC Human Factors Branch, it was agreed not to include this issue as part of the OER (Reference 8).
24	Item B.1 (24)	HF5.1, Local control stations (LCSs)	This issue addresses the M-MIS of local control stations and auxiliary operator interfaces.	The LCSs are included in the HFE/M-MIS design process. Among the human factors criteria that are applied across the AP600 I&C and M-MIS design is the criteria that each workstation, LCS, or other area of personnel activity, be analyzed and designed to accommodate the following: 1) expected modes of operation, including maintenance and refueling; 2) staffing levels expected under each of these expected modes. Also, refer to the responses of items 161 through 169.
25	Item B.1 (25)	HF5.2, Review criteria for human factors aspects of advanced I&C	This concern is a combinati^n of HF4.5, the original HF5.2 on annunciators, HF5.3, and HF5.4.	Refer to SSAR Sectic^ 18.4 and WCAP-14644 for the methodology and results of the functional requirements analysis and function allocation conducted for AP600. As part of the existing Element 7 process, as described in SSAR Section 18.8, an HFE design guideline document will be created for each of the AP600 HSIs.
26	Item B.1 (26)	HF5.3, M-MIS evaluation of operational aids	This issue involves guidance on M-MIS for new display and control technologies	This issue is addressed by completing Element 7 (HSI Design) of the AP600 HFE/HSI design process. As part of the Element 7 process as described in SSAR Section 18.8, an HFE design guideline document will be created for each of the AP600 HSIs.
27	Item B.1 (27)	HF5.4, M-MIS computers and computer displays	See HF5.2 above.	This issue is addressed by completing Element 3 (Functional Requirements Analysis and Function Allocation) and Element 7 (HSI Design) of the AP600 HFE/HSI design process. Refer to SSAR Section 18.4 and WCAP-14644 for the methodology and results of the functional requirements analysis and function allocation conducted for AP600. As part of the existing Element 7 process as described in SSAR Section 18.8, an HFE design guideline document will be created for each of the AP600 HSIs.
28	Item B.2 (1)	1v, High-pressure coolant injection and reactor core isolation cooling separation	The design should consider CR alarm and indication of the initiation levels and low-level restart values.	**NOT APPLICABLE:** This issue is only applicable to BWR plants.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
29	Item B.2 (2)	1vi, Reduction of challenges to safety/relief valves (SRV)	The design should consider CR alarm and indication of SRV status and important parameters.	Status indication of the pressurizer SRVs and the steam generator (SG) SRVs are provided in the MCR. The position status of these SRVs is included in the list of variables and instrumentation needed to allow the operator to monitor and maintain the safety of the AP600 throughout operating conditions that include accident and post-accident conditions. SSAR Section 7.5 provides this list of variables and instrumentation. The pressurizer SRVs and the SG SRVs will have a full set of abnormality alarms and status messages in the MCR. The abnormality alarms will appear in the overview of alarms as integrated into the WPIS. For example, alarms alerting the operator that the valve is OPEN when it should be CLOSED or CLOSED when it should be OPEN will exist and will appear in the alarm overview as integrated into the WPIS. Status messages for the expected behavior of these SRVs will exist on the alarm support screens available at the operator's workstation. For example, status messages informing the operator that the valve is OPEN when it should be OPEN or CLOSED when it should be CLOSED will exist and be available on the alarm support screens available at the operator's workstation. The AP600 Alarm System is designed following the HSI design process described in SSAR Section 18.8 as part of the AP600 HFE program.
30	Item B.2 (3)	1vii, Automatic depressurization system (ADS) study	Determination of the optimum ADS for elimination of manual activation should include consideration of the operators' need to monitor the system and an analysis of the time required for operators to perform manual backup if required.	The AP600 ADS has been designed to provide a controlled depressurization of the RCS following small LOCAs. It is automatically actuated on a low core makeup tank (CMT) level, which is indicative of a significant loss of reactor coolant from the primary system. The ADS functions to depressurize the primary system to enable gravity-driven safety injection. The AP600 passive safety systems (including the ADS and the CMTs) actuate automatically to provide core cooling, and to provide the operators sufficient time to take manual actions as prescribed in the AP600 ERGs. The timing of the accident sequences is such that, for small LOCAs, first stage ADS actuation does not occur for at least 20 minutes after actuation of the CMTs. This provides the operators sufficient time to diagnose the event, to properly monitor the actuation of the ADS, and to perform manual backup if necessary, as prescribed in the ERGs.
31	Item B.2 (4)	1viii, Automatic restart of core spray and low-pressure coolant injection	This issue involves allocation-of-function considerations in terms of automatic restart of a system after manual stoppage by the operators. Considerations of whether automatic restart should be available, how it should be implemented, and what alarm and indications are needed in the CR are required.	**NOT APPLICABLE:** This issue is only applicable to BWR plants.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
32	Item B.2 (5)	1xi, Depressurization by means other than ADS	Consideration of depressurization will involve the provisions of alarms and indication in the CR. Some methods may also require operator actions that should be subject to the full design and implementation process.	Manual controlled depressurization of the primary system is employed to mitigate some accident sequences. For instance, in the response to a steam generator tube rupture (SGTR), the ERGs and background documents (Reference 2) instruct the operator to depressurize the primary system to equalize pressure to the secondary system, and thereby stop the release of primary coolant to the secondary system. This can be achieved by use of the pressurizer spray. If normal or auxiliary spray is not available, then a first-stage ADS valve is used to reduce the RCS pressure. Manual ADS is also used as a backup to automatic actuation of the ADS. In these instances, the operator manually actuates ADS on either 1) low CMT water level followed by the failure of the ADS valves to open, 2) low hot-leg level as a result of failure of the ADS and/or subsequent of operator failure to recognize the need for ADS, or 3) high core exit temperatures indicative of a significant degradation in core cooling. These associated parameters will be alarmed by the Alarm System. The ERGs contain optimal recovery guidelines and function restoration guidelines. The ERG background documents contain a description of the accident sequences where the use of alternate or manual depressurization is anticipated.
33	Item B.2 (6)	1xii, Alternate hydrogen control systems	The evaluation of design alternatives for hydrogen control systems should include the information needs of the operators to assess the conditions that would require system initiation and the degree of automation of the systems.	Hydrogen ignitors are provided to address the possibility of a beyond-design-basis event which results in a rapid production of large amounts of hydrogen, such that the containment hydrogen concentration would exceed the capacity of the Passive Autocatalytic Recombiners (PARs), thereby resulting in the flammability limit being exceeded. The ignitors are incorporated in the design to address a low-probability severe accident, and are not relied upon to mitigate design basis events. The ignitors are actuated manually by the operators, as a result of two conditions: 1) when the core exit temperature reaches 1200 °F (alarm), or 2) on receipt of a high hydrogen concentration alarm as detected by the hydrogen monitors. There is no provision in the design to actuate the ignitors automatically.
34	Item B.2 (7)	2iv, Safety Parameter Display System (SPDS)	The selection and display of important safety parameters and their integration into the overall design of the CR is a primary HFE issue.	The regulatory requirements for an SPDS will be met by integrating the requirements into the design requirements for the AP600 M-MIS, specifically into the portions of the system that produce the alarm messages (Alarm System), the Computerized Procedure System (CPS) for emergency procedures and the process displays (plant information system). The integration of the SPDS into the AP600 M-MIS and a description of how the AP600 M-MIS design satisfies the requirements/criteria of a SPDS is found in SSAR 18.8.2.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
35	Item B.2 (8)	2v, Automatic indication of bypassed and inoperable systems	Providing operators with the capability to monitor the status of automatic systems is an important function of the CR information display system and a component important to the maintenance of the operators' situation awareness.	The WPIS provides and maintains situation awareness by presenting plant information on a large screen display and possessing design features to address the elements of situation awareness. (Refer to the response to item 66 of this table for more information on how the AP600 HSI maintains operator situational awareness.) System and equipment availability and status information is presented by the wall panel displays. Also, the status of automatic control systems (nonsafety-related) and automatic protection systems (reactor protection and ESF actuation systems) are provided by the wall panel displays. The wall panel displays include monitoring of the current state of automatic systems (control and protection). For example, an RCS pressure control functional display is included on the wall panel display. This functional display group includes the current status and trend of RCS pressure. Alarm system overviews are incorporated into the wall panel displays. These overviews alert the operator to changes in plant state, including changes in the status of automatic systems (control and protection). Examples: (1) Operators are alerted to the switch from "auto" to "manual" of automatic control systems such as the pressurizer pressure control system; (2) operators are alerted to bypassed protection instrument channels; and (3) operators are alerted to protection system degradation such as an out of service CMT actuation valve. The WPIS provides the means to directly access the most appropriate workstation displays that provide more detailed information about the change that has occurred. These workstation displays include alarm support displays, functional displays, physical displays, and automatic system monitoring displays.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
36	Item B.2 (9)	2vi, Venting of noncondensible gases	Operator monitoring of the status of noncondensible gases in the RCS and having clear, unambiguous indication of the conditions under which gas release must be initiated, should be evaluated for HFE design implications.	SSAR subsection 5.4.12 discusses the AP600 high-point vents including the reactor vessel (RV) head vent. The requirements for high-point vents are met for the AP600 by the RV head vent valves and the ADS valves. The primary function of the RV head vent is for use during plant fill and startup to properly fill the RCS and vessel head. Both RV head vent valves and the ADS valves may be activated and controlled from the MCR. The AP600 does not require use of an RV head vent to provide safety-related core cooling following a postulated accident. The first stage valves of the ADS are attached to the pressurizer and provide the capability of removing noncondensible gases from the pressurizer steam space following an accident. Gas accumulations are removed by remote manual operation of the first stage ADS valves. The discharge of the ADS valves is directed to the in-containment refueling water storage tank (IRWST). Subsection 5.4.6 and Section 6.3 of the SSAR discuss the ADS valves and discharge system. The AP600 ERGs specified in ERG AE-1, Step 17, states that the plant staff be consulted to determine if the vessel head should be vented. Their decision would be based on the specific accident sequence and available systems. Operation of the ADS typically obviates the need for venting of the head to preserve natural circulation cooling. Although not required to provide safety-related core cooling following a postulated accident, the RV head vent valves can remove noncondensible gases or steam from the RV head to mitigate a possible condition of inadequate core cooling or impaired natural circulation through the SGs resulting from the accumulation of noncondensible gases in the RCS. The design of the RV head vent system is in accordance with the requirements of 10 CFR 50.34 (f)(2)(vi). The RV head vent valves could also be used during a severe accident (beyond-design-basis) scenarios where multiple failures in the safety-related systems result in fuel damage and the generation of noncondensible gases that collect in the vessel head. Combinations of multiple failures in the safety-related systems could make venting the head to alleviate the buildup of noncondensible gases desirable.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
37	Item B.2 (10)	2xi, Direct indication of safety relief valves in CR	The alarming and indication of SRV status should be clear and unambiguous and should be evaluated for HFE design implications.	Status indication of the pressurizer SRVs and the SG SRVs are provided in the MCR. The valve position indication for these SRVs is accomplished through "direct" measurement of stem position. The position status of these SRVs is included in the list of variables and instrumentation needed to allow the operator to monitor and maintain the safety of the AP600 throughout operating conditions that include accident and post-accident conditions. SSAR Section 7.5 provides this list of variables and instrumentation. The pressurizer SRVs and the SG SRVs will have a full set of abnormality alarms and status messages in the MCR. The abnormality alarms will appear in the overview of alarms as integrated into the WPIS. For example, alarms alerting the operator that the valve is OPEN when it should be CLOSED, or CLOSED when it should be OPEN will exist and will appear in the alarm overview as integrated into the WPIS. Status messages for the expected behavior of these SRVs will exist on the alarm support screens available at the operator's workstation. For example, status messages informing the operator that the valve is OPEN when it should be OPEN, or CLOSED when it should be CLOSED will exist and be available on the alarm support screens available at the operator's workstation. The AP600 alarm system is designed following the HSI design process described in SSAR Section 18.8 as part of the AP600 HFE program.
38	Item B.2 (11)	2xii, Auxiliary feedwater (AFW) indication and initiation	The HFE aspects of providing indication and initiative for AFW should be evaluated.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The AP600 Passive Residual Heat Removal (PRHR) system functionally replaces the AFW system. Refer to SSAR Section 6.3 for a description of the Passive Core Cooling System (PXS) which includes the PRHR system. The indications needed to monitor the proper operation of the PRHR system are identified and verified through the FBTA process as described in SSAR Section 18.5.
39	Item B.2 (12)	2xvi, 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 HFE design implications.	**THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
40	Item B.2 (13)	2xvii, CR instrumentation for various parameters	The selection and display of important parameters and their integration into the overall design of the CR is a primary HFE issue.	The WPIS provides dynamic displays and mimics that present information to orient the MCR operators and those entering the CR (operator shift turnover, technical staff, plant management, etc.) to the current status of the plant. For each plant mode or significant plant state within an operating mode, the WPIS includes a mimic display that provides a physical overview of the plant's significant systems and respective key components. The wall panel mimic display includes the dynamic display of key plant parameters so that the reactor operator or a person entering the MCR can establish the plant operating status.

TABLE 1 (Continued) OPERATING EXPERIENCE REVIEW FOR THE AP600 Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
41	Item B.2 (14)	2xviii, CR instrumentation for inadequate core cooling	The selection and display of important parameters and their integration into the overall design of the CR is a primary HFE issue.	The regulatory requirements for an SPDS will be met by "integrating" the requirements into the design requirements for the AP600 M-MIS, specifically into the portions of the system that produce the alarm messages (Alarm System), the CPS for emergency procedures, and the process VDU displays (Plant Information System). Refer to SSAR subsection 18.8.2 for a description of the SPDS. Following a reactor trip the CPS provides automatic monitoring of the critical safety functions (CSFs), alerts the operator to a degraded function, and suggests the appropriate function restoration guideline. Core cooling is one of the CSFs. Also, refer to SSAR subsection 1.9.3.
42	Item B.2 (15)	2xix, Instrumentation for post accident monitoring	The selection and display of important parameters and their integration into the overall design of the CR is a primary HFE issue.	The selection and display of the parameters which perform the post-accident monitoring function is part of the design process, analysis, and results presented in SSAR Section 7.5. An analysis is conducted to identify the appropriate variables and to establish the appropriate design basis and qualification criteria for instrumentation employed by the operator for monitoring conditions in the RCS, the secondary heat removal system, the containment, and the systems used for attaining a safe shutdown condition. Three categories of design and qualification criteria are used (SSAR subsection 7.5.2). Category 1 instrumentation has the highest performance requirements and is used for information that can not be lost under any circumstances. The QDPS is the HSI that provides the Class 1E displays to the operators in the MCR. The QDPS displays will include all Category 1 variables and some Category 2 variables (Table 7.5-1 of the SSAR). The specific displays of the QDPS result from the completion of the HSI Design process (Element 7). The HSI design process is described under SSAR Section 18.8.
43	Item B.2 (16)	2xxi, Auxiliary heat removal systems design to facilitate manual/automatic actions	The specification and evaluation of manual and automatic actions should be subject to the function allocation analyses performed as part of the design and implementation process.	SSAR Section 18.4 and WCAP-14644 document the AP600 functional requirements analysis and function allocation, including the function allocation decisions (manual/automatic) made for auxiliary heat removal systems such as the CCS and the SWS. Table 2 of WCAP-14644 includes the identification of when an auxiliary heat removal system is used to support a CSF. Table 4 includes an explanation of the functional allocation for each auxiliary heat removal system.
44	Item B.2 (17)	2xxiv, Recording of RV level	The selection and display of important parameters and their integration into the overall design of the CR is a primary HFE issue.	The requirements for RV-level indication are provided by redundant, safety-related RV-level instrumentation. As shown in SSAR Figure 5.1-5, these instrument channels (LT-160 and LT-170) have one level tap that connects to the bottom of a hot leg, and one level tap that connects to the top of the hot-leg bend that connects to the SG. This instrumentation is used to provide RV water level during an accident, and is also used to provide hot-leg level during shutdown operations including mid-loop. This instrumentation provides indication of RV water level for a range spanning from the bottom of the hot leg to approximately the elevation of the mating surface. This instrumentation is temperature compensated and provides accurate level measurement during all modes of operation. Refer to SSAR subsection 1.9.3.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
45	Item B.2 (18)	2xxv, Technical support center (TSC), operational support center (OSC), and emergency offsite facility (EOF)	The design of the TSC, OSC, and EOF should include HFE considerations to ensure that the personnel located in these facilities can most effectively perform their safety-related functions. Poor HFE design of these facilities may interfere with the performance of operators in a well-designed CR.	The design of the TSC, remote shutdown facility, and the OSC are governed by the same HFE design program as the MCR design. Chapter 18 of the SSAR describes the AP600 HFE program. SSAR subsection 18.8.3 addresses the TSC, remote shutdown facility, and the OSC. The HFE program is designed around the 10 elements of the HFE Program Review model presented in NUREG-0711. The COL applicant shall address the design of the EOF as stated in SSAR subsection 18.2.6.
46	Item B.2 (19)	2xxvii, Monitoring of inplant and airborne radiation	The selection and display of important parameters and their integration into the overall design of the CR is a primary HFE issue.	The radiation monitoring system (RMS) provides plant effluent monitoring, process fluid monitoring, airborne monitoring, and continuous indication of the radiation environment in plant areas where such information is needed. The design bases of the RMS includes providing long-term, post-accident monitoring (using both safety-related and nonsafety-related monitors) and providing equipment to meet the applicable regulatory requirements for both normal operation and transient events. Refer to SSAR Section 11.5 for a description of the RMS. Radiation monitoring data, including alarm status, are integrated into the MCR workstation displays and, where appropriate, into the WPIS displays. The output of the HFE task analysis activities is used as an input to the design of the workstation and wall panel displays. Refer to SSAR Section 18.5 for a description of the task analysis activities.
47	Item B.2 (20)	2xxviii, CR habitability	While potential pathways for radioactivity to affect CR habitability may be identified and design solutions to preclude such problems may be developed, the CR operating crew should be aware of potential pathways. The integrity of the design solutions and the presence of radiation in the pathways should be considered if evaluations of monitoring methods in the CR are warranted.	The nuclear island nonradioactive ventilation system (VBS) is a nonsafety-related system which supplies the MCR. It includes radiation monitors in the supply ducts, with alarms to indicate high radiation levels in the pathway. If the radiation level is above the Hi-Hi setpoint, the normal heating, ventilation and air-conditioning (HVAC) system is automatically stopped and the CR is then isolated. The safety-related emergency habitability system (VES) is initiated on the same signal, and it provides air for respiration of the CR occupants and pressurization of the CR pressure boundary. The air is not delivered through the isolated HVAC duct, but is delivered through dedicated, separate lines which penetrate the CR pressure boundary. The VES is designed to maintain a positive pressure of 1/8" water gauge in the MCR pressure boundary with respect to surrounding rooms. The system incorporates redundant pressure instrumentation with alarms to provide indication that this function is met.
48	Item B.2 (21)	I.A.1.4, Long-term upgrading of operating personnel and staffing	This issue concerns shift staffing with licensed operators and working hours of licensed operators. Updates to 10 CFR 50.54 were approved.	Staffing levels are the responsibility of the COL applicant as stated in SSAR Section 18.6. SSAR Section 16.1, subsection 5.2.2.d also addresses MCR staffing and limits on working hours.
49	Item B.2 (22)	I.A.4.2, Simulator capabilities	This issue involves the improvement of the use of simulators in the training of operators.	Training program development is the responsibility of the COL applicant as documented in SSAR Sections 13.2 and 18.10.
50	Item B.2 (23)	I.C.1, Guidance for the evaluation and development of procedures	This issue addresses normal, transient, and accident conditions to ensure that procedures are technically correct, explicit, and easily understood.	The development of plant procedures are the responsibility of the COL applicant as documented in SSAR Section 13.5. The AP600 ERGs have been developed and provide the technical basis for the development of the emergency operating procedures (EOPs). Refer to SSAR Section 18.9 for more information on "Procedure Development."

TABLE 1 (Continued) OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
51	Item B.2 (24)	I.C.9, Long-term program for upgrading procedures	This issue includes EOPs with particular emphasis on diagnostic aids for off-normal conditions.	The development of plant procedures is the responsibility of the COL applicant as documented in SSAR Section 13.5.
52	Item B.2 (25)	I.D.1, CR design reviews	This issue addresses general CR design issues.	This issue is addressed by SSAR Section 18.2 (HFE Program Management), the HSI design implementation plan (SSAR Section 18.8) and the HFE Verification and Validation (SSAR Section 18.11). Design reviews are used as part of the Element 7 (HSI Design) process as described in Sections 18.2 and 18.8 of the SSAR.
53	Item B.2 (26)	I.D.2, Same as item B.2(7), above	This issue addresses the need for the provision of an SPDS that displays a minimum set of parameters that define the safety status of the plant.	The regulatory requirements for an SPDS will be met by integrating the requirements into the design requirements for the AP600 M-MIS, specifically into the portions of the system that produce the alarm messages (Alarm System), the CPS for emergency procedures and the process VDU displays (Plant Information System). The integration of the SPDS into the AP600 M-MIS and a description of how the AP600 M-MIS design satisfies the requirements/criteria of a SPDS is found in SSAR 18.8.2.
54	Item B.2 (27)	I.D.4, CR design standard	This issue addresses the need for guidance on the design of CRs to incorporate human factors considerations.	This issue is addressed by development and implementation of an integrated HFE Design Process that conforms to NUREG-0711. Refer to Chapter 18 of the AP600 SSAR for a description of the AP600 HFE program.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
55	Item B.2 (28)	I.D.5.1, CR design, improved instrumentation research alarms and displays	This issue involves the MMI in the CR with regard to the use of lights, alarms, and annunciators to reduce the potential for operator error, information overload, unwanted distractions, and insufficient organization of information.	The function of the AP600 Alarm System is to support the MCR operators with the following activities of human decision-making (adopted from Rasmussen's model of human decision-making): 1) The ALERT activity, i.e., alert the operator to off-normal conditions; 2) The OBSERVE WHAT IS ABNORMAL activity, i.e., aid the user in focusing on the important issue(s); 3) Help with the process STATE IDENTIFICATION activity, i.e., aid the user in understanding the abnormal conditions and provide corrective action guidance, as far as to guide the operating crew into that area of the complete Plant Information Display System in which the data/information about the abnormality and its resolution can be found. The AP600 Alarm System addresses the problem of alarm avalanching and operator data overload by managing the presentation of the alarms to the operators in such a manner as to reduce the number of alarms presented simultaneously during major disturbances, while maintaining sensitivity during small disturbances. The Alarm System is robust enough to: a) show multiple major process problems; b) not be overwhelmed by minor alarms that are related to, or are consequence of, the process problems (avalanching); and c) elevate minor alarms to a place of attention-provoking significance, when they are the most significant process abnormalities. However, those active alarm messages which are not currently displayed are accessible and available to the operators, upon request. The Alarm System aids in directing the operator to the area in the informational display system of the CR that contains specific data related to eliminating, diagnosing, and mitigating the process abnormality. The Alarm System also provides a link from a given alarm to its applicable computerized alarm response procedure.
56	Item B.2 (29)	II.F.1 and II.F.2 Same as Item B.2 13 and 14 above	These issues address detailed CR design issues related to instrumentation (II.F.1, "Additional accident monitoring instrumentation," and II.F.2, "Instrumentation for detection of inadequate core cooling").	This is addressed by the response to items 40, 41, and 44.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
57	Item B.2 (30)	II.K.1.5, Safety-related valve position description	This issue addresses direct indication of relief and safety valve position in the CR so that the alarming and indication valve status is clear and unambiguous and should be evaluated for HFE design considerations.	Status indication of the pressurizer SRVs and the SG SRVs are provided in the MCR. The position status of these SRVs is included in the list of variables and instrumentation needed to allow the operator to monitor and maintain the safety of the AP600 throughout operating conditions that include accident and post-accident conditions. SSAR Section 7.5 provides this list of variables and instrumentation. The pressurizer SRVs and the SG SRVs will have a full set of abnormality alarms and status messages in the MCR. The abnormality alarms will appear in the overview of alarms as integrated into the WPIS. For example, alarms alerting the operator that the valve is OPEN when it should be CLOSED, or CLOSED when it should be OPEN will exist and will appear in the alarm overview as integrated into the WPIS. Status messages for the expected behavior of these SRVs will exist on the alarm support screens available at the operator's workstation. For example, status messages informing the operator that the valve is OPEN when it should be OPEN, or CLOSED when it should be CLOSED will exist and be available on the alarm support screens available at the operator's workstation. The AP600 Alarm System is designed following the HSI design process described in SSAR Section 18.8 as part of the AP600 HFE program.
58	Item B.2 (31)	II.K.1.10, Review and modify procedures for removing safety-related systems from service	This issue addresses procedures for ensuring that the operability status of safety-related systems is known.	The development of plant procedures is the responsibility of the COL applicant as documented in SSAR Section 13.5. The AP600 wall panel overview alarm displays, along with the informational system VDU displays, present indications of bypassed or deliberately-induced inoperable safety equipment. This includes the bypassed or deliberately induced inoperability of any auxiliary or supporting system that effectively bypasses or renders inoperable the protection system and the systems actuated or controlled by the protection system. The WPIS mimic displays include the display of high-level derived quantities, e.g., those that depend on a particular logic algorithm. An example of a high-level derived quantity is the availability of a safety system or function.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
59	Item B.3 (1)	Generic Letter 91-06, Resolution on (GI) A-30, Adequacy of safety-related dc power supplies	In this generic letter, the NRC proposes certain monitoring, surveillance, and maintenance provisions for safety-related dc systems.	The following responses are provided to the questions raised in the attachment to Generic Letter 91-06. The responses are numbered to match the question numbers in Generic Letter 91-06. SSAR subsection 8.3.2.1.1 describes the features of the Class 1E dc and UPS system. 1. Unit -- AP600 2.a. The number of independent redundant divisions of Class 1E dc power for this plant is 4. b. The number of functional safety-related divisions of dc power necessary to attain safe shutdown for this unit is 3. 3.a. The following alarms are provided for each division of dc power: 1. Battery test/disconnect switch status and battery open circuit alarm (open circuit alarm provided by the battery monitor system) 2. Battery charger disconnect switch status and battery charger output breaker status 3. dc system ground detection alarm 4. dc bus undervoltage 5. Battery over/under voltage (provided by the battery monitor system) and battery charger output over/under voltage 6. Battery charger ac input power failure and battery charger trouble alarm 7. Battery discharge rate alarm b. The following indications are provided for each division of dc power: 1-3. Battery current -- used for float, charge, and discharge 4. dc bus voltage c. Procedures for response to these alarms and indications are a COL applicant issue.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
59				4. The battery chargers are provided with input undervoltage alarms and the input breakers are provided with breaker trip alarms. In addition, a spare battery and charger are provided for use during maintenance and testing of the batteries and chargers. 5. Not applicable. 6. Maintenance and testing activities and procedures are a COL applicant issue. 7. The AP600 Technical Specifications (TS) are similar to those found in the Westinghouse Standard TS for maintenance and surveillance of Class 1E electrical systems. 8.a. Capability is maintained for ensuring continued and adequate reactor cooling following the loss of one safety-related dc power supply or bus. b. RCS integrity and isolation capability are maintained following the loss of one safety-related dc power supply or bus. c. Operating procedures are a COL applicant issue. 9. Not applicable.
60	Item B.3 (2)	Generic Letter 91-07, GI-23 Reactor Coolant Pump Seal Failures	This generic letter discusses the interaction between GI-23 and A-44, both of which have human factors aspects.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR 5.1.3.3 and 5.4.1
61	Item B.3 (3)	Generic Letter 91-11, Resolution of Generic Issues 48 and 49	This generic letter addresses several issues related to electrical systems, including the reduction of human errors, control of equipment status, and testing.	The three statements below address the three recommended actions of Generic Letter 90-11. 1. The time limitations and surveillance requirements for vital instrument buses are addressed in TS; SSAR Section 16.1, subsections 3.8.5 and 3.8.6. 2. The time limitations and surveillance requirements for Class 1E inverters are addressed in TS; SSAR Section 16.1, subsections 3.8.3 and 3.8.4. 3. The AP600 design does not contain any tie breakers that can connect redundant Class 1E buses. The one-line diagram for the Class 1E dc and UPS systems are shown in SSAR Figures 8.3.2-1 and 8.3.2-2.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
62	Item B.3 (4)	IN 93-47, Unrecognized Loss of CR Annunciators	Unrecognized Loss of CR Annunciators.	The AP600 Alarm System informs the MCR crew about those failures, within the equipment comprising the system, that could degrade to the point where either system performance is reduced or system availability is threatened. The AP600 Alarm System design philosophy is such that the system's preferred failure mode is through a succession of "gracefully degrading" states of operation rather than a "sudden death." The alarm overview displays, integrated into the WPIS displays, include a display of alarm messages that describe failures or degradation of equipment that comprise the Alarm System. Since the alarm overview displays are integrated into the WPIS, a dynamic indication that the WPIS is running is used to illustrate to the CR operators that the system is not "hung" in a frozen condition.
63	Item B.3 (5)	IN 93-81, Implications of Engineering Expertise on Shift	Implications of Engineering Expertise on Shift.	As stated in SSAR Section 18.6, COL applicants will address the staffing levels and qualifications of all plant personnel.
64	Item B.4	CR Organization -- Staffing and Responsibilities	CR staffing levels had impaired crews in performing their emergency functions. CR personnel were overburdened during emergencies. Based upon a review of NUREG-1275, WCAP-14114 (Section 6.2) discusses cases where operators failed to take a required action due to a mental lapse because of a high workload situation.	Workload analysis is part of the task analysis (Element 4) to be performed as part of the AP600 HFE design process. The workload analysis provides an indication of the adequacy of CR staffing assumptions. In cases where the analysis indicates high operator workload values or insufficient time available for performance, we will evaluate alternative CR staffing assumptions or changes to the M-MIS design or task allocation to reduce operator workload. Refer to SSAR Section 18.5 for a description of the task analysis implementation plan which includes workload analysis. As stated in SSAR Section 18.6, staffing levels are the responsibility of the COL applicant.
65	Item B.4	CR Organization -- Shift Technical Advisor (STA)	The use of the "dual-role" STA-impaired crew performance because the other SROs were overloaded when one SRO assumed the STA role. Assignment of other tasks during events detracted from the STAs safety function.	Workload analysis is part of the task analysis (Element 4) to be performed as part of the AP600 HFE design process. The workload analysis provides an indication of the adequacy of CR staffing assumptions. In cases where the analysis indicates high operator workload values or insufficient time available for performance, we will evaluate alternative CR staffing assumptions or changes to the M-MIS design or task allocation to reduce operator workload. Refer to SSAR Section 18.5 for a description of task analysis implementation plan which includes workload analysis. As stated in SSAR Section 18.6, staffing levels are the responsibility of the COL applicant.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
66	Item B.4	CR Organization -- Teamwork Findings	Critical performance in complex systems depends on the coordinated activity of a group of individuals, which includes all factors related to the performance of the operating crew. Based upon a review of NUREG-1275, WCAP-14114 (Section 6.1) discusses cases where there were low levels of task awareness, command, control, and communication. These events illustrate failures to maintain broad awareness of ongoing activities and their implications. Of particular concern are failures of supervisory personnel in maintaining awareness of the activities of the personnel under their direction.	For the AP600 MMI design, the following elements of situation awareness have been adopted: a) the awareness of current plant state; b) awareness of changes in plant state; and c) the links from the wall panel group overview displays to the individual workstation displays. As one of the AP600 M-MIS resources available to the MCR operators, the WPIS provides and maintains situation awareness by presenting plant information on a large screen display and possessing the design features to address each of the three elements. The following provides two examples of design features of the WPIS that address the first element of situation awareness: 1) For each plant mode or each significant plant state within an operating mode, the WPIS includes a mimic display which provides a physical overview of the plant's significant systems and respective key components; and 2) The wall panel mimic display includes the dynamic display of key plant parameters so that a reactor operator, supervisor, or a person entering the MCR can establish the plant operating status. To address awareness of changes in plant state, the Alarm System's overview displays are incorporated into the AP600 WPIS overview and mimic displays. The alarm overview portion of the WPIS performs the "alerting" activity in the human decision-making process. The links that are provided from the wall panel displays to the individual workstation displays are the third element of situation awareness. For systems of workstation displays as large as the one required for AP600, asking operators to find and select the most appropriate displays when unanticipated plant changes occur can impose a large mental burden and can be time consuming when other activities may be time critical. When significant changes to plant parameters occur, operators need to know which workstation displays are appropriate and the most efficient method to locate and select those displays. Operators will not be required to conduct lengthy searches for displays at the point when significant changes in plant state have occurred. Operators need to be able to get to any display quickly and efficiently. Therefore, the WPIS displays provide the ability to identify and access the most appropriate workstation display from the wall panel. Specifically, the WPIS possesses the following design features to address the third element of situation awareness: a) When changes in plant state have occurred as indicated on the WPIS, operators are not required to conduct lengthy searches through the workstation displays for more detailed information. When a change occurs, as indicated on the mimic display (a changing plant parameter) or the wall panel alarm overview display, the WPIS identifies the most appropriate workstation displays. b) The WPIS provides the capability to directly access from the wall panel the most appropriate workstation display that provides more detailed information about the change that is occurring or has occurred.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
67	Item B.4	Procedures -- Procedural Adherence	Operators acted during events without using a procedure. Procedural content, ease of use, and management policy and practices influenced procedure use. Based upon a review of NUREG-1275, WCAP-14114 (Section 4.5) discusses cases where procedures were available but not used.	The development of plant procedures, including administrative procedures such as procedural compliance, are the responsibility of the COL applicant as documented in SSAR Section 13.5.
68	Item B.4	Procedures -- Knowledge-Based Performance During Events	Operators experienced difficulty in applying knowledge to unusual plant conditions that resulted in delays in recognizing and responding to events. Based upon a review of NUREG-1275, WCAP-14114 (Section 4.1) discusses cases where the particular situation was not fully covered by the procedure requiring knowledge-based reasoning to fill in gaps and adapt to the situation.	The development of plant procedures are the responsibility of the COL applicant as documented in SSAR Section 13.5. Completion of Element 7 (HSI Design) of the HFE Program Review Model (NUREG-0711) and the AP600 HFE Design Process helps address this issue. A fundamental tenet of the AP600 HFE/M-MIS design process is that, in addition to ensuring that the M-MIS supports the task of process equipment control and operation, the interface design basis includes consideration of those cognitive tasks that represent how humans reason, assess situations, and make decisions in a real-time process control environment. The premise for this design basis is that errors of intention (incorrect or improper decision-making) can be reduced if the set of tasks that the M-MIS is designed to support includes those cognitive activities experienced while operating the plant. To accomplish this design basis, an input to the task analysis activities is an operator decision-making model. This model is utilized in the M-MIS design process to provide a structure for and to help determine the cognitive needs of the plant operations personnel. The model is used to define the set of questions that are used in the cognitive task analysis part of the FBTA. The definition of I&C requirements that results from answering this set of questions supports operator performance at all three levels in Rasmussen's decision-making model (i.e., skill-based, rule-based, and knowledge-based reasoning). Using the output of the FBTAs as an input to the design of the M-MIS, should result in an MMI that supports the kind of knowledge-based reasoning that is required to handle unanticipated events or events where existing procedures may require knowledge-based reasoning to fill in gaps. The FBTA is based on a fundamental analysis of plant goals and functions and is effective in designing M-MISs to support operator performance in preanalyzed situations (executing a procedure) and unanticipated situations. Refer to SSAR Section 18.5 for the task analysis plan and to 18.8 for the HSI design plan.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
69	Item B.4	Procedures -- Knowledge-Based Performance During Events	Operators experienced difficulty in applying knowledge to unusual plant conditions, which resulted in delays in recognizing and responding to events. Based upon a review of NUREG-1275, WCAP-14114 (Section 4.2) discusses cases where operators had to balance multiple goals in determining a course of action. Situations arise where operators need to consider and balance multiple goals.	The development of plant procedures are the responsibility of the COL applicant as documented in SSAR Section 13.5. Completion of Element 7 (HSI Design) of the HFE Program Review Model (NUREG-0711) and the AP600 HFE Design Process helps address this issue. A fundamental tenet of the AP600 HFE/M-MIS design process is that, in addition to ensuring that the M-MIS supports the task of process equipment control and operation, the interface design basis includes consideration of those cognitive tasks that represent how humans reason, assess situations, and make decisions in a real-time process control environment. The premise for this design basis is that errors of intention (incorrect or improper decision-making) can be reduced if the set of tasks that the M-MIS is designed to support includes those cognitive activities experienced while operating the plant. To accomplish this design basis, an input to the task analysis activities is an operator decision-making model. This model is utilized in the M-MIS design process to provide a structure for and to help determine the cognitive needs of the plant operations personnel. The model is used to define the set of questions that are used in the cognitive task analysis part of the FBTA. The definition of I&C requirements that results from answering this set of questions supports operator performance at all three levels in Rasmussen's decision-making model (i.e., skill-based, rule-based, and knowledge-based reasoning). Using the output of the FBTAs as an input to the design of the M-MIS, should result in an MMI that supports the kind of knowledge-based reasoning that is required to handle unanticipated events. The FBTA is based on a fundamental analysis of plant goals and functions and is effective in designing M-MISs to support operator performance in preanalyzed situations (executing a procedure) and unanticipated situations.
70	Item B.4	Procedures -- Knowledge-Based Performance During Events	Operators experienced difficulty in applying knowledge to unusual plant conditions, which resulted in delays in recognizing and responding to events. Based upon a review of NUREG-1275, WCAP-14114 (Section 5.0) discusses cases where operator actions reflected gaps in knowledge (implying a need for improved training).	Training program development is the responsibility of the COL applicant as stated in Section 13.2 of the AP600 SSAR.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
71	Item B.4	Procedures -- Operator Preconditioning	Preconditions from past experience, training, or management direction strongly affected how operators recognized and responded to events and had led some operators to disbelieve valid indications or take inappropriate actions. Based upon a review of NUREG-1275, WCAP-14114 (Section 4.4) discusses cases where the delay in performing EOP E-0 may negatively impact recovery ability. The inherent fixed linearity of paper-based procedures means that in some cases operators are placed in situations where they have to go through procedural steps that are obviously not relevant to the situation, and as a consequence delay reaching procedural steps that are important to perform in an expeditious manner. The inherent fixed linearity of paper-based procedures has two potential negative consequences. First, in some cases the delays caused by the need to follow each procedure step sequentially will result in conditions becoming more degraded than if operators could reach the relevant procedure steps more quickly. Second, because operators are able to assess the situation more quickly than the procedures allow, and in their experience they are generally correct, the temptation to jump to what they perceive to be the relevant steps for terminating the incident is high. This is likely to be a contributing factor in cases where operators were observed to "wing it" without procedures.	The AP600 HSI/M-MIS includes a CPS that assists the plant operators in monitoring and controlling the execution of plant procedures. For a given procedure, the status of each procedure step is dynamically determined and presented to the operator along with the supporting plant information. To alleviate the inherent fixed linearity of paper-based procedures the CPS performs parallel monitoring activities which are performed by the operator in paper-based procedures. A parallel monitoring activity is a plant condition, state, or parameter that is monitored by the computer in parallel with the activity of guiding the operator through the respective procedure. Types of parallel information monitored by the CPS are the status of CSFs, procedure notes and cautions, foldout page items, initiated actions (continuous action steps), and continuously monitored parameters. With the CPS dynamically determining the status of each procedure step and performing parallel monitoring activities, the delays caused by the inherent fixed linearity of executing paper-based procedures are minimized or eliminated. Therefore, the CPS allows the operator to reach the relevant steps for terminating the incident and stabilizing the plant much quicker and minimizes the temptation to jump to relevant steps or to "wing it" without procedures.
72	Item B.4	Procedures -- Control of Emergency Safety Features	Operators inappropriately defeated the automatic operation of ESFs during valid system demands. Some licensees have not provided sufficient guidance that limits bypassing or disabling ESFs, allowed for by TS and emergency or operating procedures. Based upon a review of NUREG-1275, WCAP-14114 (Section 4.3) discusses cases where operators bypassed safety features.	The AP600 ERGs (Reference 2) provide specific termination criteria for the operator to bypass or override ESF actuations. These are typically provided to terminate safety system operation once an accident sequence has been diagnosed, and the plant has been returned to a stable, safe condition.
73	Item B.4	Human-Machine Interface -- Shutdown Instrumentation	A lack of appropriately ranged, direct-reading, CR instrumentation to monitor reactor pressure, temperature, and level caused operators to have difficulty in recognizing and responding to shutdown events, when operator actions were required to accomplish the safety functions of disabled, automatic safety systems. Based upon a review of NUREG-1275, WCAP-14114 (Section 3.1) discusses cases where there were misleading indicators (failed sensors).	The design of the AP600 has considered shutdown modes extensively as documented in the various licensing submittals: 1) passive safety systems that are designed to mitigate accidents during shutdown modes (SSAR Section 6.3), 2) TS that apply to the passive safety systems during shutdown modes (SSAR Chapter 16), 3) ERGs (Reference 2) for shutdown modes, 4) quantification of the risk of core damage at shutdown (AP600 shutdown PRA), 5) evaluation of design basis initiating events during shutdown modes (AP600 Shutdown Evaluation Report - 6/96). Instrumentation has been designed to appropriately cover all modes of operation including shutdown.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
74	Item B.4	Human-Machine Interface -- Operator Awareness	Operators failed to recognize conditions that were clearly off-normal, but which were not alarmed. Based upon a review of NUREG-1275, WCAP-14114 (Section 2.) discusses cases where the operators failed to detect an abnormal (but not alarmed) condition.	The AP600 WPIS provides and maintains situation awareness by presenting plant information on a large screen display and possessing the design features to address each of the three elements of situation awareness: (1. awareness of current plant state; 2. awareness of changes in plant state; and 3. links from the wall panel group overview displays to the individual workstation displays). The WPIS addresses the first element by providing a dynamic mimic display that presents a physical overview of the plant's significant systems and respective key components, including the display of key plant parameters. This is done for each plant mode or each significant plant state within an operating mode. To address the second element, awareness of changes in plant state, the Alarm System's overview displays are incorporated into the WPIS overview and mimic displays. The alarm overview portion of the WPIS alerts the MCR operators to develop abnormal or emergency conditions by providing appropriate alarms or alarm-like information.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
75	Item B.4	Human-Machine Interface -- Operator Awareness	During transients that result in a reactor trip, a large number of annunciators are activated; their usefulness to the operator is diminished as the number of low priority annunciators increases. Prioritization of annunciators could improve the effectiveness of this system.	The function of the AP600 Alarm System is to support the MCR operators with the following activities of human decision-making: 1) The ALERT activity, i.e., alert the operator to off-normal conditions; 2) The OBSERVE WHAT IS ABNORMAL activity, i.e., aid the user in focusing on the important issue(s); 3) Help with the process STATE IDENTIFICATION activity, i.e., aid the user in understanding the abnormal conditions and provide corrective action guidance, as far as to guide the operating crew into that area of the complete Plant Information Display System in which the data/information about the abnormality and its resolution can be found. The AP600 Alarm System addresses the problem of alarm avalanching and operator data overload by managing the presentation of the alarms to the operators in such a manner as to reduce the number of alarms presented simultaneously during major disturbances, while maintaining sensitivity during small disturbances. The Alarm System is robust enough to: a) show multiple major process problems; b) not be overwhelmed by minor alarms that are related to, or are consequence of, the process problems (avalanching); and c) elevate minor alarms to a place of attention-provoking significance, when they are the most significant process abnormalities. However, those active alarm messages which are not currently displayed are accessible and available to the operators, upon request. Part of the method used to manage the presentation of alarms to the operator is the functional organization of the alarms. The overview alarms are organized by function, such as RCS pressure control, temperature control, and inventory and SG water level control. Within each function, there are goal-related alarms and process-related alarms for the respective function. The alarms within each function are prioritized such that only the highest priority, goal-related alarms and process-related alarms for that function are displayed. This functional organization and prioritization of alarms provides an efficient way of directing and focusing the operators attention to the transient and its source. The overall importance to plant safety or the urgency of operator action is easily determined from this method of alarm presentation. The Alarm System aids in directing the operator to the area in the informational display system of the CR that contains specific data related to eliminating, diagnosing, and mitigating the process abnormality. The Alarm System also provides a link from a given alarm to its applicable computerized alarm response procedure.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
76	Item B.4	Human-Machine Interface -- Instrumentation	Crew response was affected by availability of instrumentation, appropriateness of the instruments to the task, and the relative location of the I&C. Based upon a review of NUREG-1275, WCAP-14114 (Section 2.1) discusses cases where the plant parameter indicators required for monitoring or control were unavailable or inadequate.	Completion of Element 4 of the HFE Program Review Model (NUREG-0711) and the AP600 HFE design process includes an FBTA as part of the overall task analysis. The task analysis implementation plan is described in SSAR Section 18.5. For each Level 4 plant function shown on Figure 18.5.1 of the SSAR, an FBTA is performed. There are four components to an FBTA. First, analysis is done to identify the complete set of goals relevant to the function. Second, a functional decomposition is done. This decomposition identifies all the various processes that have a significant effect on the function. Third, a cognitive process analysis is done by applying the 11 questions derived from Rasmussen's human decision-making model approach. The results of the cognitive process analysis identify the indications, parameters, and controls that the operator needs to make decisions about the respective functions. Finally, there is a verification that the indications parameters and controls identified in the cognitive analysis are all included in the AP600 design. In addition, as part of the background documentation for the AP600 EHGs, the I&Cs needed to execute each step within each of the guidelines (optimal recovery guidelines and function restoration guidelines) is identified. Verification that the needed I&Cs, identified here, are all included in the AP600 design is part of the AP600 design process.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
77	Subsection 2.1.1	MCR -- System Integration	Integration of Information During unplanned transients, the operators are presented with an overwhelming volume of immediate information. A better display integration and increased automation may help them through these evolutions.	The function of the AP600 Alarm System is to support the MCR operators with the following activities of human decision-making: 1) The ALERT activity, i.e., alert the operator to off-normal conditions; 2) The OBSERVE WHAT IS ABNORMAL activity, i.e., aid the user in focusing on the important issue(s); 3) Help with the process STATE IDENTIFICATION activity, i.e., aid the user in understanding the abnormal conditions and provide corrective action guidance, as far as to guide the operating crew into that area of the complete Plant Information Display System in which the data/information about the abnormality and its resolution can be found. The AP600 Alarm System addresses the problem of alarm avalanching and operator data overload by managing the presentation of the alarms to the operators in such a manner as to reduce the number of alarms presented simultaneously during major disturbances, while maintaining sensitivity during small disturbances. The Alarm System is robust enough to: a) show multiple major process problems; b) not be overwhelmed by minor alarms that are related to, or are consequence of, the process problems (avalanching); and c) elevate minor alarms to a place of attention provoking significance, when they are the most significant process abnormalities. However, those active alarm messages which are not currently displayed are accessible and available to the operators, upon request. The Alarm System aids in directing the operator to the area in the informational display system of the CR that contains specific data related to eliminating, diagnosing, and mitigating the process abnormality. The Alarm System also provides a link from a given alarm to its applicable computerized alarm response procedure. The AP600 M-MIS includes a CPS that assists the plant operators in monitoring and controlling the execution of plant procedures. For a given procedure, the status of each procedural step is dynamically determined and presented to the operator along with the supporting plant information. To alleviate the inherent fixed linearity of paper-based procedures, the CPS performs parallel monitoring activities versus the operator in paper-based procedures. A parallel monitoring activity is a plant condition, state or parameter that is monitored by the computer in parallel with the activity of guiding the operator through the respective procedure. Types of parallel information monitored by the CPS are the status of CSF, procedure notes and cautions, foldout page items, initiated actions (continuous action steps) and continuously monitored parameters. With the CPS dynamically determining the status of each procedure step and performing parallel monitoring activities, the delays caused by the inherent fixed linearity of executing paper-based procedures are minimized or eliminated. The CPS provides direct links from steps to the associated Plant Information System Displays (physical process, functional, automatic monitoring logic or soft control displays).

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
78	Subsection 2.1.2	MCR -- System Integration	Change in Control Modes In transient situations, operators often have to take manual control of many of the tasks that were automatically controlled. This change in control modes by itself is a challenge to the operators, and when added in the middle of a significant transient, with its information integration problems, is even more demanding.	The information integration problems are addressed by the AP600 design as described above in item #77. The AP600 I&C System design incorporates automatic functions not available in previous plant designs. This is the result of efforts to minimize the operators manual workload during normal plant transients (such as a startup) and during unanticipated transients (such as a reactor trip). The feedwater control system in the AP600 is one example. The AP600 feedwater control system automatically controls SG water levels from power levels low in the power range (0% to 2% power) to 100% power. In today's plants, operators are required to control feedwater flow and SG water level in manual until they have reached about 20% power. Another example is the use of the AP600 Startup Feedwater System (SFS). Following a reactor trip, the SFS flow is automatically controlled to maintain the desired SG levels. In today's plants, the operators must manually control AFW flow to maintain desired SG levels. The cognitive task analysis portion of the FTBAs, answering a set of questions derived from Rasmussen's human decision-making model, identifies the controls and indications needed to achieve the respective function. This addresses both manual and automatic controls. The output of the FBTAs is used as input to the design of soft control displays and plant information displays. If an automatic control system's input signal validation algorithm switches the control system from automatic to manual, the operator is alerted to this condition through the alarm system. The computerized alarm response procedure will provide the operator prompt access to the associated soft control (soft automatic/manual controller).
79	Subsection 2.1.3	MCR -- System Integration	Memorization Operators have to memorize their initial actions after a reactor trip, and are expected to accomplish them prior to procedural checks. Operator aids may assist in the initial actions.	Following a reactor trip, the AP600 CPS is activated and the operator is directed to the computerized reactor trip response procedure. The CPS dynamically determines and provides the status of each procedural step along with any necessary supporting information. In today's plants, the operator must not only memorize the immediate action steps, but must also search the main control board for the indications and controls to provide the capability of determining the status of the immediate actions.
80	Subsection 2.1.4	MCR -- System Integration	Processed Information Much information has to be calculated by operators that could be provided directly with current technology. Computer-processed and validated data and calculated values can be provided to the operator in an integrated fashion.	The AP600 M-MIS takes advantage of current computer technology and automatically calculates, then presents the needed information to the operators. In today's plants, the operator must manually calculate the needed information. One example of calculated information provided by the AP600 Plant Information System, are trend displays. During a plant heatup or cooldown, the AP600 Plant Information System will provide heatup and cooldown rate trend displays at the operator's workstation.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
81	Subsection 2.1.5	MCR -- System Integration	Test and Maintenance Surveillance testing can create problems such as: number of tests, additional operators required, producing spurious alarms, inadvertent actuations, and potential for a plant trip. The systems should be designed to be tested periodically without creating incidents.	The AP600 Inservice Test (IST) Plan (SSAR subsection 3.9.6) documents the surveillance test requirements for the AP600. In developing this plan, Westinghouse has considered the difficulty of performing each surveillance test. In some instances, ISTs that would be potentially problematic at-power are deferred to either cold shutdown or refueling conditions. In other cases (such as the ADS valves) a special interlock has been developed to preclude the possibility of the operators causing a plant transient due to a misalignment of the ADS valves during testing. Other features which facilitate inservice testing of the PXS are described in SSAR subsection 6.3.6.2. The online testing of the protection system is accomplished by a series of tests with sufficient overlap to test all necessary functions. These tests are designed to be accomplished without generating spurious alarms and inadvertent trips and actuations. When a protection cabinet is being tested, it is placed into a bypassed state or otherwise removed from service to prevent inadvertent actuations and potential for a plant trip. Most of the testing is performed automatically once initiated by the operator. A description of the protection system reliability and fault tolerance during operations, maintenance, test and bypass and a description of the built-in test capabilities are provided in SSAR subsections 7.1.2.10 and 7.1.2.12.
82	Subsection 2.2.1	MCR --Alarms	Avalanche of Alarms The single biggest issue in the design of advanced alarm systems is the need to reduce the avalanche of alarms during plant upset.	The function of the AP600 Alarm System is to support the MCR operators with the following activities of human decision-making: 1) ALERT activity, i.e., alert the operator to off-normal conditions; 2) OBSERVE WHAT IS ABNORMAL activity, i.e., aid the user in focusing on the important issue(s); 3) Help with the process STATE IDENTIFICATION activity, i.e., aid the user in understanding the abnormal conditions and provide corrective action guidance, as far as to guide the operating crew into that area of the complete Plant Information Display System in which the data/information about the abnormality and its resolution can be found. The AP600 Alarm System addresses the problem of alarm avalanching and operator data overload by managing the presentation of the alarms to the operators in such a manner as to reduce the number of alarms presented simultaneously during major disturbances, while maintaining sensitivity during small disturbances. The Alarm System is robust enough to: a) show multiple major process problems; b) not be overwhelmed by minor alarms that are related to, or are a consequence of, the process problems (avalanching); and c) elevate minor alarms to a place of attention-provoking significance, when they are the most significant process abnormalities. However, those active alarm messages which are not currently displayed are accessible and available to the operators, upon request. The Alarm System aids in directing the operator to the area in the informational display system of the CR that contains specific data related to eliminating, diagnosing, and mitigating the process abnormality. The Alarm System also provides a link from a given alarm to its applicable computerized alarm response procedure.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
83	Subsection 2.2.2	MCR --Alarms	Prioritization of Alarms When an operator is presented with an avalanche of alarms, a prioritization scheme should present all the alarms to the operator but code them into priorities such that the overall importance to plant safety or the urgency of the operator action can be determined.	The AP600 Alarm System addresses the problem of alarm avalanching and operator data overload by managing the presentation of the alarms to the operators in such a manner as to reduce the number of alarms presented simultaneously during major disturbances, while maintaining sensitivity during small disturbances. The Alarm System is robust enough to: a) show multiple major process problems; b) not be overwhelmed by minor alarms that are related to, or are a consequence of, the process problems (avalanching); and c) elevate minor alarms to a place of attention-provoking significance, when they are the most significant process abnormalities. However, those active alarm messages which are not currently displayed are accessible and available to the operators, upon request. Part of the method used to manage the presentation of alarms to the operator is the functional organization of the alarms. The overview alarms are organized by function, such as RCS pressure control, RCS temperature control, RCS inventory, and SG water level control. Within each function, there are goal-related alarms and process-related alarms for the respective function. The alarms within each function are prioritized such that only the highest priority, goal-related alarms and process-related alarms for that function are displayed. This functional organization and prioritization of alarms provides an efficient way of directing and focusing the operators attention to the transient and its source. The overall importance to plant safety or the urgency of operator action is easily determined from this method of alarm presentation.
84	Subsection 2.2.3	MCR --Alarms	Loss-of-Power to Annunciator Panels The loss of power to these panels could result in the loss of the operators' ability to respond to plant upsets, particularly if the operators are not aware of the loss.	Power to the alarm system is from a redundant power supply or UPS. The Alarm System also includes a "heartbeat" indication visible to the operator at all times. The "heartbeat" indication alerts the operator to degraded conditions of the Alarm System, including a total loss of the system, experienced as a result of loss of the redundant power sources. The Alarm System is designed such that the system's preferred failure mode is through a succession of "gracefully degrading" states of operation rather than a "sudden death."

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance issue	Human Factors/Human Performance Issue Addressed by AP600 Design
85	Subsection 2.2.4	MCR -- Alarms	Alarm Displays Alarm System research has identified multiple use by operators of the Alarm Systems, namely; for alerting, for status monitoring, and for situation awareness. The selection of a display technology and display methods for the Alarm System can significantly impact these multiple uses of alarm systems by operators. Both conventional fixed-location displays and the newer Cathode Ray Tube (CRT)-based displays have advantages and disadvantages.	The function of the AP600 Alarm System is to support the MCR operators with the following activities of human decision-making: 1) ALERT activity, i.e., alert the operator to off-normal conditions; 2) OBSERVE WHAT IS ABNORMAL activity, i.e., aid the user in focusing on the important issue(s); 3) Help with the process STATE IDENTIFICATION activity, i.e., aid the user in understanding the abnormal conditions and provide corrective action guidance, as far as to guide the operating crew into that area of the complete Plant Information Display System in which the data/information about the abnormality and its resolution can be found. The AP600 Alarm System addresses the problem of alarm avalanching and operator data overload by managing the presentation of the alarms to the operators in such a manner as to reduce the number of alarms presented simultaneously during major disturbances, while maintaining sensitivity during small disturbances. The Alarm System is robust enough to: a) show multiple major process problems; b) not be overwhelmed by minor alarms that are related to, or are a consequence of, the process problems (avalanching); and c) elevate minor alarms to a place of attention-provoking significance, when they are the most significant process abnormalities. However, those active alarm messages which are not currently displayed are accessible and available to the operators, upon request from workstation displays. The Alarm System aids in directing the operator to the area in the informational display system of the CR that contains specific data related to eliminating, diagnosing, and mitigating the process abnormality. The Alarm System also provides a link from a given alarm to its applicable computerized alarm response procedure. The AP600 Alarm System design captures the advantages of both the conventional fixed-location displays and the newer CRT-based displays. The AP600 Alarm System consists of overview alarms and VDU (such as CRT)-based alarms and alarm support information. The overview alarms are functionally organized with each function having goal-related and process-related alarms. The alarm overviews are integrated into and displayed by the WPIS, therefore the presentation of the alarm system overviews is analogous to the conventional fixed position annunciators. All alarms and associated supporting information is available at the operator's workstation VDUs. The presentation of alarms on the workstation VDUs is analogous to CRT-based alarm displays.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
86	Subsection 2.2.5	MCR -- Alarms	Alarm Controls Auditory features of alarm systems have been problematical and separate silence, acknowledge and restart test (SART) controls are recommended. The controls for computer-based alarm systems will become more complex and need attention.	The AP600 Alarm System provides the means for the AP600 CR operator to be alerted, via both visual and audio alerting techniques, to problems in the processes involved in the plant by: a) indicating the abnormality by presenting a precisely worded message or a graphic representation of the condition; b) presenting the abnormality in a context which conveys the impact on plant health; c) separating alarms from other data; and d) generating audible tones corresponding to specific sets of alarms. The controls for the auditory features of the AP600 Alarm System will not add to the workload nor will they be distracting. A design requirement of the Alarm System is that it will not create distractions to the operators, nor will it add to the fatigue of its users, by the addition of noise or visual distortions. Concept testing (part of the HSI design process, SSAR Section 18.8) and the HFE Verification and Validation (SSAR Section 18.11) shall ensure that the alarm system auditory features are acceptable.
87	Subsection 2.2.6	MCR -- 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.	**THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
88	Subsection 2.3.1	MCR -- Controls and Displays	Engineering Units Displays sometimes use engineering units which mean little to the operator, (e.g., "lbs-mass/hour) rather than percentage of full-power flow.	The AP600 Plant Information System presents displays (physical process, functional, trend, and automatic monitoring and logic displays) to the operator. The engineering units used on these displays will be meaningful to the operators. One way that this is ensured is through the detailed display design and implementation process (SSAR Section 18.8, HSI design). The design process includes a check by operational personnel that the displays and the information presented are meaningful. The final HFE verification and validation (Element 10) will validate the usefulness of displays.
89	Subsection 2.3.2	MCR -- Controls and Displays	Push Button Lamp Replacement Push-button lamp replacement is problematic because the removal and replacement of the lens or bulb can sometimes cause inadvertent actuation.	**NOT APPLICABLE:** The use of push button lamps are not part of AP600 CR MMI.
90	Subsection 2.3.3	MCR -- Controls and Displays	CRT-Based Displays On CRT-based displays, the operators are often restricted to the use of "prepackaged" displays and do not have enough capability to select parameters for display and trending.	The AP600 Plant Information System presents displays (physical process, functional, trend and automatic monitoring, and logic displays) to the operator. In addition to these "prepackaged" displays, the Plant Information System provides the capability to the operator of being able to create a desired parameter and trend display. In addition, the operator will have the capability of displaying this created trend display on the WPIS.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
91	Subsection 2.3.4	MCR -- Controls and Displays	Computer Interfaces Complex or poorly designed computer interfaces are supplied, as opposed to interfaces that are simple and "user-friendly".	It is the mission of the AP600 M-MIS to improve the means that are provided to the users of the plant operation and control centers for acquiring and understanding plant data and in executing actions to control the plant's processes and equipment (Reference: 18.8.1 of the SSAR). Therefore, a basic design goal of the AP600 M-MIS is to provide an integrated environment that is "user friendly" and allows the operator to quickly and efficiently maneuver through the MMI resources (Alarm System, Information System, CPS, and Soft Controls) to access needed information and controls.
92	Subsection 2.3.5	MCR -- Controls and Displays	Upgrading of Computer Systems The difficulty of upgrading computer systems can be a problem, even for relatively minor plant modifications.	The distributed nature of the AP600 I&C System architecture includes the robustness and flexibility to upgrade the system in an efficient manner. The distributed I&C architecture is discussed in Section 7.1 of the SSAR.
93	Subsection 2.3.6	MCR -- Controls and Displays	Computer Response Time A common specification for maximum delay time between screens is two seconds. This may be acceptable for routine computer processing, however, during nuclear power plant (NPP) transients it is too long and causes unnecessary operator frustration and delays in information processing.	The issue to be addressed is the amount of time it takes for the operator to locate a desired piece of information. How does the operator locate a desired display? How many displays must the operator navigate through before he locates the desired information? The AP600 Plant Information System addresses this issue through its design process and type of displays presented to the operator. Functional displays are designed and used to complement physical (system) displays. Functional displays are designed to present to the operator associated goal monitoring and process monitoring information for a respective function. The output of the respective FBTA is used as a major input to the design of the functional displays. The FBTA includes a cognitive task analysis that identifies the instrumentation, information, and controls that the operator needs to make operating decisions for the respective function. Since the AP600 Plant Information System includes functional displays (produced from their associated FBTA) rather than just physical system displays, it is more likely that the operator will find all the information that he needs for a given thought process on one display (such as a functional display). Also, the use of denser displays and more meaningful groupings of information on the displays will result in a search within the display rather than movement between displays to find desired information. To support the operator's situational awareness in an efficient and timely manner, the design of the WPIS requires that the operator be able to point to and select in one step (from the workstation), a system, component or major parameter displayed on the wall panel and recall on a workstation VDU, a related functional display or physical display. One step navigation from a functional display to an associated physical display, and from a physical display to its associated functional display, will also be available. To add flexibility to the method of navigation between displays a menu or map of all available displays, will also be available to the operator. This method of navigation to a desired display will involve a maximum of two steps; select the map and then select the display. The actual delay times between screens is driven by the I&C technology and associated hardware. Advances in this technology are allowing faster responses all the time. This issue of how long it takes the operator to access needed information will be evaluated during the man-in-the-loop concept testing. The results of this concept testing will be used to refine the functional and detailed design of the M-MIS. This issue will also be measured and validated by the HFE verification and validation (SSAR Section 18.11).

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
94	Subsection 2.3.7	MCR -- Controls and Displays	Computer-Based Data Points Computer-based data points should have a provision to indicate to the operators when the data for the point is invalid (e.g., point is out of scan).	The information presented to the operators by the AP600 M-MIS includes indication of data quality for the data displayed. The objective is to allow the operator to evaluate the information being displayed to him and, eventually, discard it or look for alternative measures. If a parameter measurement is outside the range of the instrument (note that the data quality would be good) then this "out-of-range" information is indicated on the display to the operator. The data quality of computer calculated points is also addressed and displayed by the AP600 M-MIS. The data quality of calculated points considers the data quality of the input points and the validity of the calculation and its boundary conditions. The data quality conventions used are consistent throughout the M-MIS. For example, the convention used on a workstation display to indicate that a data point such as a hot leg temperature is of "poor" quality is the same as the convention used to present the same information on the WPIS.
95	Subsection 2.3.8	MCR -- Controls and Displays	Trip Status Indication In the CR, the operators need an adequate indication for trip status of important local equipment.	The function of the AP600 Alarm System is to support the MCR operators with the following activities of human decision-making (adopted from Rasmussen's model of human decision-making): 1) The ALERT activity, i.e., alert the operator to off-normal conditions; 2) The OBSERVE WHAT IS ABNORMAL activity, i.e., aid the user in focusing on the important issue(s); 3) Help with the process STATE IDENTIFICATION activity, i.e., aid the user in understanding the abnormal conditions and provide corrective action guidance, as far as to guide the operating crew into that area of the complete Plant Information Display System in which the data/information about the abnormality and its resolution can be found. The Alarm System includes alarms of trip status for important local equipment and it clearly distinguishes between alarms that are conveying to the operator something about a process abnormality vs. advising him of the status of equipment.
96	Subsection 2.4.1.1	MCR -- Communications	Communications Coverage -- Dead Spots Auxiliary operators often cannot be contacted in the plant due to their inability to hear pages from the CR since there are many hard-to-hear or dead spots in the plant.	The plant communication system consists of the following systems: wireless communication system, telephone/page system, private automatic branch exchange (PABX), sound-powered system, emergency response facility communications, and security communication system. The wireless telephone system is the primary means of communication for plant operations and maintenance personnel. The wireless system consists of wireless belt-clip portable handsets, hands-free type portable headsets, a comprehensive antenna system, and a wireless telephone switch. The telephone/page, PABX telephone, and sound-powered communication systems are for general plant communications and serve as backup to the wireless system. The communications system is described in SSAR subsection 9.5.2.
97	Subsection 2.4.1.2	MCR -- Communications	Communications Coverage -- Radio Frequency (RF) Interference RF interferes with communications due to inadequate shielding. Communication radios also cause unintended actuation of equipment.	The communications system complies with applicable codes and standards, minimizing Electro-Magnetic Interference (EMI) and its potential effects to equipment. "Low-powered" type equipment is used, where possible, which has been demonstrated to have a limited potential for causing interference with electronic equipment. Communication equipment and sensitive I&C equipment are shielded, as necessary, from the detrimental effects of EMI.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
98	Subsection 2.4.1.3	MCR -- Communications	Communications Coverage -- Plugs Insufficient locations in the plant to "plug in" communications equipment.	**NOT APPLICABLE:** The wireless telephone system is the primary means of communication for plant operations and maintenance personnel. The wireless system consists of wireless belt-clip portable handsets, hands-free type portable headsets, a comprehensive antenna system, and a wireless telephone switch. No "plug-in" locations are required for this type of equipment.
99	Subsection 2.4.2	MCR -- Communications	Noise Interference -- Ventilation The noise level in the CR can be so high during transients that added stress for the operators is created and communication is difficult due to ESF actuated ventilation (especially 2 trains).	The VBS supplies ventilation flow to the MCR during normal operation, and is a nonsafety-related system. The VBS system serves as a first line of defense if available, and it also performs the safety-related function of isolating the HVAC ducts that penetrate the CR pressure boundary. The AP600 design incorporates a VES to provide the safety-related function of ventilating and pressurizing the MCR. This system uses a supply of air for respiration of the CR occupants as well as for pressurizing the room. The system supplies a lower volumetric flowrate of breathable quality air, than the normal HVAC flowrates. The safety-related ventilation system uses no active components which contribute to noise generation. The issue of noise level is not a major concern for the VES system because of the relatively low air flowrate, even when both trains are in operation. The VBS system is used during normal operation as noted previously. This system has industrial type air handling units and fan assemblies with double-walled panel construction to minimize noise and fan turbulence, while the supply and return ducts are provided with anti-sweat insulation. Centrifugal fans are provided with flexible connections and vibration isolator designs to avoid sound rumble conditions. The MCR main supply and return duct layouts require multiple 90° elbows and several 20-foot straight duct sections before entering the MCR, which means that low-frequency noise transmitted through ductwork is eliminated. This ductwork arrangement is normally used for low noise level HVAC acoustic design for sound studios and theaters. Finally, the MCR HVAC design is a low velocity system designed specifically for a lower noise level, in that the duct air velocities are much lower than the maximum velocities described in American Society of Heating, Refrigeration and Air-Conditioning Engineers (ASHRAE).
100	Subsection 2.4.2	MCR -- Communications	Noise Interference -- Printers The noise level in the CR can be so high during transients that added stress for the operators is created and communication is difficult due to high-speed conventional printers.	High-speed printers used in the AP600 MCR will not significantly contribute to the noise level even during transient situations. Printer technology currently exists such that generated noise is no longer an issue.
101	Subsection 2.4.2	MCR -- Communications	Noise Interference -- Alarms The noise level in the CR can be so high during transients that added stress for the operators is created and communication is difficult due to alarms ringing constantly.	The AP600 Alarm System has a design requirement that specifies the system to be designed is not to distract the operators; nor will it add to the fatigue of its users, by the addition of noise, visual distortions or nuisance alarms. The functional organization, prioritization within each function, and the alarm trigger logics are all design features that manage the presentation of alarms such that only meaningful alarms are presented to the operator.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
102	Subsection 2.5.1	MCR -- Procedures	Space Paper-based or hard-copy procedures in NPP operations can cause the following problem. Space for explanatory information is limited and the level of detail in procedure steps is fixed.	The AP600 CPS is the MMI/HSI that the operator will use to execute procedures. The reactor operator will interface with the CPS through his workstation VDUs. The CPS automatically evaluates the status of each procedure step and presents this evaluation to the operator along with enough supporting information (such as actual parameter values and equipment status) to give the operator an understanding of how and why the system produced its evaluation. The CPS will provide the capability for the operator to request supplemental information on an additional VDU. This will be information such as an associated physical, functional, trend or soft control display or perhaps a supporting graph, curve, or background information. In comparison with the paper-medium of presenting procedures, space for explanatory information and the amount of detail provided in the procedure steps is not an issue with the computerized procedure medium. The full-scale mockup of the AP600 main control area will be used to further evaluate the "space" issue. The full-scale mockup is discussed in SSAR Section 18.8.
103	Subsection 2.5.2	MCR -- Procedures	Non-linear Information Paper-based or hard-copy procedures in NPP operations can cause the following problem: Non-linear information must be presented sequentially.	The AP600 M-MIS includes a CPS that assists the plant operators in monitoring and controlling the execution of plant procedures. For a given procedure, the status of each procedure step is dynamically determined and presented to the operator along with the supporting plant information. To alleviate the inherent fixed linearity of paper-based procedures, the CPS performs parallel monitoring activities versus the operator, as in paper-based procedures. A parallel monitoring activity is a plant condition, state, or parameter that is monitored by the computer in parallel with the activity of guiding the operator through the respective procedure. Types of parallel information monitored by the CPS are the status of CSFs, procedure notes and cautions, foldout page items, initiated actions (continuous action steps), and continuously monitored parameters. With the CPS dynamically determining the status of each procedure step and performing parallel monitoring activities, the delays caused by the inherent fixed linearity of executing paper-based procedures are minimized or eliminated. Therefore, the CPS allows the operator to reach the relevant steps for terminating the incident and stabilizing the plant much quicker than paper-based procedures.
104	Subsection 2.5.3	MCR -- Procedures	Irrelevant Information Paper-based or hard-copy procedures in NPP operations can cause the following problem: Irrelevant information regarding conditions that do not exist during a specific instance of procedure execution must be continuously displayed.	As described in the item above (Item 103), the AP600 CPS performs parallel monitoring activities versus the operator in paper-based procedures. A parallel monitoring activity is a plant condition, state, or parameter that is monitored by the computer in parallel with the activity of guiding the operator through the respective procedure. Types of parallel information monitored by the CPS are the status of CSFs, procedure notes and cautions, foldout page items, initiated actions (continuous action steps), and continuously monitored parameters. A continuously monitored parameter is an example of a condition that may not exist at the moment but requires some action when it does exist. The CPS will automatically monitor this condition as parallel information and only present it to the operator when the condition is met and when the operator needs to execute the respective action. With the CPS dynamically determining the status of each procedure step and performing parallel monitoring activities, the instances of presenting irrelevant information to the operator during a specific moment of procedure execution are minimized or eliminated.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
105	Subsection 2.5.4	MCR -- Procedures	Cross-Referencing Paper-based or hard-copy procedures in NPP operations can cause the following problem: Cross-referencing introduces errors and delays in task performance.	The AP600 CPS automatically evaluates the status of each procedure step and presents this evaluation to the operator along with enough supporting information (such as actual parameter values and equipment status) to give the operator an understanding of how and why the system produced its evaluation. The CPS will provide the capability for the operator to request supplemental information on an additional VDU. This will be information such as an associated physical, functional, trend or soft control display or perhaps a supporting graph, curve, or background information. The CPS will provide the capability for the operator to transition to the appropriate location in other operating procedures as required and to automatically select and display the new procedure when requested, while maintaining a placemark in the original procedure.
106	Subsection 2.5.5	MCR -- Procedures	Multiple Procedures Management Paper-based or hard-copy procedures in NPP operations can cause the following problem: Physical management of multiple procedures and place-keeping during concurrent execution are awkward.	The AP600 CPS will provide the capability for the operator to transition to other operating procedures as required and to automatically select and display the new procedure when requested, while maintaining a placemark in the original procedure. The CPS will provide for the display of a procedure transition map. This display will indicate transitions out of or into the procedures, as well as movements within the procedures. The CPS will also provide the capability for the operator to request supplemental information on an additional VDU. This will be information such as an associated physical, functional, trend or soft control display, or perhaps a supporting graph, curve, or background information.
107	Subsection 2.5.6 & NUREG-0933, I.C.5	MCR -- Procedures	Maintaining Procedures Paper-based or hard-copy procedures in NPP operations can cause the following problem: Maintaining the technical accuracy of procedures is difficult. For example, a design change in a single component can invalidate every procedure that references that component. Similarly, a procedure revision that changes the step number in that procedure can invalidate every step in other procedures that cross-reference that changed procedure.	The AP600 CPS will include the capability to modify or edit the procedures in a straightforward manner. This is accomplished by using an off-line relational database management system.
108	Subsection 2.5.7	MCR -- Procedures	Procedure Integration Paper-based or hard-copy procedures in NPP operations can cause the following problem: Handling and reading a paper procedure while also performing the actions required to perform the task described in a procedure are typically incompatible.	The AP600 CPS will provide the capability for the operator to request supplemental information on an additional VDU. This will be information such as an associated physical, functional, trend or soft control display or perhaps a supporting graph, curve, or background information. If a step within a procedure, as presented by the CPS, requires the user to operate a component or system, then the user will be able to select, in a single action from the CPS, the associated soft control display for the respective component. The soft control displays will appear on a VDU, at the operator's workstation separate from the VDU that presents the CPS. The use of multiple VDUs at the operator's workstation, (CPS main interface VDU, CPS supplemental information VDU, and a soft control display VDU), while executing a procedure through the AP600 CPS, minimizes or eliminates the handling and reading problems associated with the execution of a paper-based procedure while also trying to perform the actions required by the procedure.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
109	Subsection 2.5.8	MCR -- Procedures	Handling/Following Procedures Paper-based or hard-copy procedures in NPP operations can cause the following problem: Due to space limitations and the need for procedural aids for the operators to follow, procedures are difficult to work with, especially in the CR during a transient.	The AP600 M-MIS includes a CPS that assists the plant operators in monitoring and controlling the execution of plant procedures. For a given procedure, the status of each procedure step is dynamically determined and presented to the operator along with the supporting plant information. To alleviate the inherent fixed linearity of paper-based procedures, the CPS performs parallel monitoring activities versus the operator in paper-based procedures. A parallel monitoring activity is a plant condition, state, or parameter that is monitored by the computer in parallel with the activity of guiding the operator through the respective procedure. Types of parallel information monitored by the CPS are the status of the CSF, procedure notes and cautions, foldout page items, initiated actions (continuous action steps), and continuously monitored parameters. With the CPS dynamically determining the status of each procedure step and performing parallel monitoring activities, the delays caused by the inherent fixed linearity of executing paper-based procedures are minimized or eliminated. The CPS provides direct links from steps to the associated Plant Information System Displays (physical process, functional, automatic monitoring logic, or soft control displays). For example, if a step within a computerized procedure requires the user to operate a component or system, then the user will be able to select, in a single action from the CPS, the associated soft control display for the respective component. The soft control displays will appear on a VDU at the operator's workstation separate from the VDU that presents the CPS. The use of multiple VDUs at the operator's workstation (CPS main interface VDU, CPS supplemental information VDU, and a soft control display VDU) while executing a procedure through the AP600 CPS, minimizes or eliminates the handling and reading problems associated with the execution of a paper-based procedure.
110	Section 2.6	MCR -- BWR Shutdown	Reactor Shutdown During a reactor shutdown from an initial power of 6%, that involved low-decay heat levels due to a short operating history, operators allowed cooldown (due to small miscellaneous steam load) to add excessive positive reactivity. Further, by not properly maintaining the power in the mid-range of the Intermediate Range Monitors (IRMs), a reactor trip occurred.	**NOT APPLICABLE:** This issue is only applicable to BWRs.
111	Section 3.1	System-Related Insights -- Flooding Concern	Leakage Areas of NPPs, such as isolated rooms, often contain fluid systems with the potential for leakage and flooding.	Internal plant flooding can be attributed to piping ruptures, tank failures, or the actuation of fire suppression systems. The consequences of these events have been evaluated for the AP600 in accordance with Standard Review Plan (SRP) 3.6.1 and SRP 3.6.2. Water-level (flood) design features and protection mechanisms are described in Sections 3.4 and 3.6 of the SSAR, respectively. The protection mechanisms related to minimize the consequences of internal flooding include the following: • Structural enclosures • Structural barriers • Curbs and elevated thresholds • Leak detection systems • Drain systems In appropriate locations, water-level sensors are provided to transmit water level indications to the MCR and the plant control system. Level alarms alert the operator to take corrective action.

TABLE 1 (Continued) OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
112	Section 3.2	System-Related Insights -- Pressurizer	Spray Valve Stuck Open A PWR pressurizer spray valve stuck open (unknown to the operators at the time) causing a continued drop in RCS pressure to below that required by TS. As a result, a plant shutdown was required in order to isolate the spray line.	The AP600 design has addressed the possibility of a stuck open spray valve. The spray valve is provided with an automatic interlock to close on low RCS pressure that would result from an open spray valve. In addition, the remotely-operated spray block valves can be closed from the CR in the event of a stuck open spray valve. Therefore, a forced plant shutdown can be avoided in the event of a stuck-open spray valve.
113	Subsection 3.3.1	System-Related Insights -- Loss of dc Bus	Offsite Power A consequent problem on loss of a direct current (dc) bus is partial loss of normal offsite power.	dc system reliability -- The dc system is designed for a high level of reliability. A non-Class 1E battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for alternating current (ac) input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a partial loss of offsite power. The breakers in the AP600 are controlled by the PLS. The PLS system normally receives power from the non-Class 1E UPS system. Upon failure of the dc bus powering the UPS, or failure of the UPS itself, the loads are automatically transferred to a regulating transformer supply. Therefore, loss of a dc bus will not result in loss of power to the PLS system. The ac power system breakers use solid-state control which receives control power from a power supply internal to the switchgear; therefore, loss of a dc bus will not result in loss of control power to a breaker.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
114	Subsection 3.3.2	System-Related Insights -- Loss of dc Bus	Control Room Annunciator A consequent problem on loss of a dc bus is loss of CR annunciator power.	dc system reliability -- The dc system is designed for a high level of reliability. A battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for ac input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a loss of alarm system power. Alarm system power normally comes from a UPS; however, upon failure of the dc bus powering the UPS, or failure of the UPS itself, the loads are automatically transferred to a regulating transformer supply. Therefore, loss of a dc bus will not result in loss of alarm system power.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
115	Subsection 3.3.3	System-Related Insights -- Loss of dc Bus	Indicators in Control Room A consequent problem on loss of a dc bus is loss of power to indicators in the CR.	dc system reliability -- The dc system is designed for a high level of reliability. A battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for ac input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a loss of indicator power. Indicator power normally comes from a UPS system. Upon failure of the dc bus powering the UPS, or failure of the UPS itself, the loads are automatically transferred to a regulating transformer supply. Therefore, loss of a dc bus will not result in loss of indicator power.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
116	Subsection 3.3.1	System-Related Insights -- Loss of dc Bus	Power to Circuit Breakers A consequent problem on loss of a dc bus is loss of control power to various circuit breakers.	dc system reliability -- The dc system is designed for a high level of reliability. A non-Class 1E battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for ac input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a loss of circuit breaker control. The breakers in the AP600 are controlled by the PLS. The PLS system normally receives power from the non-Class 1E UPS system. Upon failure of the dc bus powering the UPS, or failure of the UPS itself, the loads are automatically transferred to a regulating transformer supply. Therefore, loss of a dc bus will not result in loss of circuit breaker control. The ac power system breakers use solid-state control which receives control power from a power supply internal to the switchgear; therefore, loss of a dc bus will not result in loss of control power to a breaker.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
117	Subsection 3.3.5	System-Related Insights -- Loss of dc Bus	Power to Computers and Displays A consequent problem on loss of a dc bus is loss of power to computers and video display screens.	dc system reliability -- The dc system is designed for a high level of reliability. A battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for ac input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a loss of power to computers and video display (workstation) screens. Power to computers and video display screens normally comes from a UPS system. Upon failure of the dc bus powering the UPS, or failure of the UPS itself, the loads are automatically transferred to a regulating transformer supply. Therefore, loss of a dc bus will not result in loss of power to computers and video display (workstation) screens.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
118	Subsection 3.3.6	System-Related Insights -- Loss of dc Bus	Power to Automatic Features A consequent problem on loss of a dc bus is loss of some of the plant's automatic features, such as trips and interlocks.	dc system reliability -- The dc system is designed for a high level of reliability. A battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for ac input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a loss of automatic features. The automatic features in the AP600 are controlled by the PMS and PLS. The PMS system normally receives power from the Class 1E UPS system. The PLS system normally receives power from the non-Class 1E UPS system. Upon failure of the dc bus powering any UPS, or failure of the UPS itself, the loads are automatically transferred to a regulating transformer supply. Therefore, loss of a dc bus will not result in loss of automatic features.

TABLE 1 (Continued) OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
119	Subsection 3.3.7	System-Related Insights -- Loss of dc Bus	Circuit Breakers A consequent problem on loss of a dc bus is trip of selected circuit breakers, such as reactor trip breakers.	dc system reliability -- The dc system is designed for a high level of reliability. A battery monitor is provided for each battery to monitor and alarm battery voltage, detect and alarm battery open-circuit condition (including blown fuses), and supervise battery availability. The battery chargers are provided with a trouble alarm for ac input failure, dc output under/over voltage, no charge, input/output breaker trip, and dc high voltage shutdown trip. The dc buses are monitored and alarmed for undervoltage. The dc system currents are monitored and alarmed for overcurrent. A ground detection alarm is provided. The dc bus outage time for maintenance and repair will be minimized with the use of the spare battery and charger. Mitigation of the effects of the loss of a dc bus -- The AP600 is designed to withstand the loss of a single dc bus without placing the plant in an unsafe condition. In the AP600 design, loss of a dc bus will not result in a plant trip. The AP600 has eight reactor trip breakers arranged for two-out-of-four trip logic as shown in SSAR Figure 7.1-7. With this configuration, the complete loss of power to any single train will result in tripping the two breakers associated with that train; however, no single-train pair of breakers can trip the plant if they are the only breakers to trip.
120	Section 3.4	System-Related Insights -- Automatic Trip of Condensate and Condensate Booster Pumps	Vessel Overfill In BWRs during transient situations, reactor vessel overfill can be a problem causing main steamline flooding and possible damage. There is currently no automatic trip on condensate and condensate booster pumps on high reactor vessel level.	**NOT APPLICABLE:** This issue is only applicable to BWR reactors.
121	Section 3.5	System-Related Insights -- System Overpressurization	System Overpressurization During system restoration after maintenance during cold shutdown at a BWR, an incorrect valving sequence resulted in overpressurization of piping and damage to the test return line of the Condensate Storage Tank (CST) and Condensate Return Tank.	**NOT APPLICABLE:** This issue is only applicable to BWR reactors.

TABLE 1 (Continued) OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
122	Section 3.6	System-Related Insights -- Feedwater Control System	<u>Control of Feedwater Control System</u> The control of PWR Feedwater Systems during startup and low-power operations has been problematical. Operators have had difficulty in controlling the feedwater flowrate as necessary to maintain SG water levels due partially to the fact that the feedwater control valves and control systems are not designed to operate in the low flow regions. There has also been difficulty in the switchover from manual to automatic control that occurs in this time frame.	In the AP600 design, SG water level is automatically controlled from no-load conditions to 100% plant-rated thermal power by the startup feedwater control subsystem and the main feedwater control subsystem. The startup feedwater control subsystem maintains a programmed water level in the shell side of the SGs during low-power (below approximately 10% of plant-rated thermal power), no-load, and plant heatup and cooldown modes. Transition between the main and startup feedwater control valves is automatically controlled based on flow measurements within the respective control valves. The startup feedwater control subsystem regulates the flow of feedwater in a manner similar to the way (main) feedwater is controlled in the low-power control mode. Two modes of feedwater control (low-power mode and high-power mode) are incorporated in the (main) feedwater control subsystem. A separate low-range feedwater flow measurement is used in the low-power feedwater control mode. SSAR subsections 7.7.1.8.1 and 7.7.1.8.2 provide a description of the feedwater control and startup feedwater control subsystems.
123	Section 3.7	System-Related Insights -- Scram Discharge Volume	<u>Volume Fills With Water</u> On a BWR, when the scram discharge volume fills with water, insertion of the control rods is inhibited.	**NOT APPLICABLE:** This issue is only applicable to BWR reactors.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
124	Section 3.8	System-Related Insights -- Interfacing Systems LOCA (ISLOCA)	Overpressurization of Low-Pressure Systems Overpressurization of low-pressure systems due to RCS boundary failures may result in rupture of low-pressure piping. Some RCS boundary failures have occurred due to operator error. Important operator errors include valve alignment errors during transitions between operation modes.	The AP600 has incorporated various design features to address ISLOCA challenges. These design features have resulted in very low AP600 core damage frequency compared to currently operating plants. These design features are primarily associated with the normal residual heat removal system (RNS) as discussed in SSAR subsection 5.4.7. A Westinghouse design report, WCAP-14425, has been prepared to document the systematic evaluation of the AP600 design for conformance to NUREG/CR-5102. As a result of the study reported in WCAP-14425, additional design features have been incorporated in the AP600. The following table provides a summary of AP600 design features which satisfy ISLOCA frequency acceptance criteria. **System / Subsystem** — **Major Design Feature** Normal Residual Heat Removal 1. Increased design pressure of the outside of the containment portion of the system, such that the ultimate rupture strength of the piping and components are equal to or greater than the RCS design pressure. Chemical and Volume Control System Makeup Pump Suction 1. Relief valves were added to minimize the consequences of pump suction over-pressurization. 2. High-pressure alarm added to pump suction line to alert operator of over-pressurization. Chemical and Volume Control System Letdown Line 1. Placement of high-pressure purification loop inside containment eliminates high-energy letdown outside of containment. 2. Letdown orifice limits leakage from a letdown line ISLOCA. 3. Automatic isolation of letdown occurs upon safeguards actuation signal. 4. Relief valve added to prevent overpressurization of letdown line. Primary Sampling System 1. Most of the Primary Sampling System is designed for full RCS pressure. 2. Flow restricting orifices limit extent of ISLOCA 3. Automatic isolation of Primary Sampling System occurs upon safeguards actuation signal. Demineralized Water System 1. Relief valve added to prevent overpressurization of the inside of containment portion of the system. 2. Automatic isolation of Demineralized Water System occurs upon safeguards actuation signal.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
125	Section 3.9	System-Related Insights -- Advanced I&C	I&C Systems Problems Conventional I&C in NPPs has been associated with periodic failures, spurious reactor trips and plant transients, operator confusion on instrument failure and loss-of-power, extensive time and effort to accomplish testing, and difficulties in troubleshooting and repair. Advanced I&C is subject to sudden failure and recovery, due partially to high susceptibility to EMI. Interfacing with the new equipment and software programming also afford opportunities for operator problems.	The advanced I&C equipment used in the AP600 design is based on an evolution of previous digital I&C designs. Each evolution step incorporates improvements which are a result of experience gained during the use of the previous design. This minimizes the likelihood that any particular design would have a significant amount of problems that would impact plant operation.
126	Subsection 4.1.1.1	Component-Related Insights -- RCPs -- Seals	Design Alternatives Seal degradation and failures have caused RCP leaks. A design alternative which can mitigate the need for extensive and complicated fixes is the use of canned rotor pumps that do not have seals.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
127	Subsection 4.1.1.2.1	Component-Related Insights -- RCPs -- Seals	Instrumentation - Monitoring Flow, temperature, and pressure data from the seal system should be continuously monitored and should be analyzed for seal performance needs.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
128	Subsection 4.1.1.2.2	Component-Related Insights -- RCPs -- Seals	Instrumentation - Ranges on Flow Measuring Devices Provide increased ranges on flow measuring devices so that off-normal values may be read as well as normal values.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
129	Subsection 4.1.1.2.3	Component-Related Insights -- RCPs -- Seals	Instrumentation - Ranges on Temperature Measuring Devices Provide increased ranges on temperature measuring devices up to RCS temperatures.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
130	Subsection 4.1.1.2.4	Component-Related Insights -- RCPs -- Seals	Instrumentation - Additional Pressure and Temperature Measurements Provide added pressure and temperature measurements, e.g., seal leakoff pressures, CCW return line pressure, seal cavity temperatures, differential stage pressures, and radial bearing temperature.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
131	Subsection 4.1.1.2.5	Component-Related Insights -- RCPs -- Seals	Instrumentation - Additional Flow Measurements Provide added flow measurement, e.g., seal leakoff flows.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
132	Subsection 4.1.1.2.6	Component-Related Insights -- RCPs -- Seals	Instrumentation - Better Alarming Provide better alarming of the need for operator action.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
133	Subsection 4.1.1.3.1	Component-Related Insights -- RCPs -- Seals	Procedures and Operator Aids -- RCP Trending Operator aids should be provided that allow the operator to appropriately trend RCP related parameters relative to seal performance criteria.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
134	Subsection 4.1.1.3.2	Component-Related Insights -- RCPs -- Seals	Procedures and Operator Aids -- Emergency Procedure Guidelines Emergency Procedure Guidelines, procedures, and training should be provided for a reasonable spectrum of seal failure events, such as: high-seal, leak-off flow, high-seal temperature, high vibration, loss-of-seal injection, loss-of-seal cooling, SBO, and reactor coolant pump restart criteria. These procedures should incorporate the recommendations of reactor coolant pump and deal vendors.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
135	Subsection 4.1.1.4	Component-Related Insights -- RCPs -- Seals	Functional Allocation Isolation of seal leakoff lines on high-flow, which has historically required operator action, should be evaluated as a candidate for automation since detection, recognition, and action are time constrained.	**NOT APPLICABLE:** The AP600 design specifies reactor coolant pumps with canned motors that have no seals. Refer to SSAR subsections 5.1.3.3 and 5.4.1.
136	Subsection 4.1.2	Component-Related Insights -- RCP Monitoring	Component Degradation When reactor coolant pumps or motor components degrade, they can eventually result in catastrophic failure of pump or seals, if the pump is not stopped in time. Due to the location of the reactor coolant pumps inside containment, detection of degradation must be accomplished through appropriate instrumentation. Large failures of the pump or seals can potentially result in a primary system LOCA.	The AP600 employs canned motor reactor coolant pumps that do not contain seals whose degradation could lead to a loss of reactor coolant. Reactor coolant pump instrumentation is provided to continuously monitor pump performance including 1) bearing water temperature, 2) pump vibration, 3) stator temperature, 4) pump speed. In addition, RCS loop flow rates are continuously measured.
137	Subsection 4.2.1	Component-Related Insights -- AFW Pumps	Trip Status In a case where the overspeed trip valve for the turbine-driven AFW pump turbine was inadvertently tripped and not properly reset, the CR operators were not aware of the inoperable status of the AFW pump.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.
138	Subsection 4.2.2	Component-Related Insights -- AFW Pumps	Steam Binding AFW pumps have experienced steam binding resulting in pump inoperability. This has typically been caused by feedwater back leakage through the AFW discharge check valves, but also by leakage through complex pathways, working its way back to the AFW pump suction sources.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer SSAR Section 6.3.
139	Subsection 4.2.3.1	Component-Related Insights -- AFW Pumps	Pump Driver Trips: Diesel-Driven Pump -- Minimum Operating Speed The diesel-driven AFW pumps have experienced problems where the pump drivers have tripped because the diesel AFW pump had reached minimum operating speed (about 600 rpm) which closed the speed switch.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.
140	Subsection 4.2.3.2	Component-Related Insights -- AFW Pumps	Pump Driver Trips: Diesel-Driven Pump -- Stop Signal The diesel-driven AFW pumps have experienced problems where the pump drivers have tripped because the stop signal was momentarily generated by the operator and was released before the diesel had come to a full stop.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
141	Subsection 4.2.3.3	Component-Related Insights -- AFW Pumps	Pump Driver Trips: Diesel-Driven Pump -- "Auto After Stop" Position The diesel-driven AFW pumps have experienced problems where the pump drivers have tripped when the control switch was allowed to go to "Auto After Stop," an auto-start signal was present from loss of the main feedwater pump (MFP).	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.
142	Subsection 4.2.3.4	Component-Related Insights -- AFW Pumps	Pump Driver Trips: Diesel-Driven Pump -- Diesel Could Not Restart The diesel-driven AFW pumps have experienced problems where the pump drivers have tripped due to the engine still being at greater than 40 rpm, the diesel starter motors were disabled and the diesel could not try to restart.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.
143	Subsection 4.2.3.5	Component-Related Insights -- AFW Pumps	Pump Driver Trips: Diesel-Drive Pump -- Low Lube Oil Pressure The diesel-driven AFW pumps have experienced problems where the pump drivers have tripped 25 seconds after receiving the second auto-start, the low-lube oil pressure switch trip was enabled. This caused the engine to lockout due to the low oil pressure associated with the engine shutdown.	**NOT APPLICABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.
144	Subsection 4.2.4	Component-Related Insights -- AFW Pumps	Pump Driver Trips: Turbine-Driven Pump -- Erroneous Trip of AFW Pumps The turbine-driven AFW pumps have experienced problems where the pump drivers have tripped, because after an auto-start operators erroneously tripped the AFW pumps. The steam-driven AFW pump had been restarted from the CR using the start valve which opened rapidly (less than 5 seconds) and caused the turbine to overspeed and trip. The auto-start signal opens the trip and throttle valve on the initial auto-start over a period of 20 seconds (by design, slow stroke time prevents the turbine overspeed). Until reset locally, the trip and throttle valve remains open when the pump is shutdown from the CR by shutting the start valve. When the faster acting start valve was used to restart the steam-driven AFW pump, the pump tripped on overspeed since the trip and throttle valve was already open.	**NOT APPLIOABLE:** The AP600 does not have an AFW system. The PRHR system functionally replaces the AFW systems in current PWR designs. The PRHR system does not include pumps. Refer to SSAR Section 6.3.
145	Subsection 4.3.1.1	Component-Related Insights -- IST of Pumps and Valves	Installation of Test Connections for Leak Rate Testing and Check Valve (CV) Testing: CVs in Series Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: When there are two CVs in a series and both are required by safety analysis (e.g., for redundancy and single failure purposes), test connections should be installed between the CVs so that each can be tested separately.	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. Table 3.9-16 in the SSAR lists valves that require ISTs. CVs that have a safety back leak function are provided with individual connections to allow their leak tightness to be measured.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
146	Subsection 4.3.1.2	Component-Related Insights -- IST of Pumps and Valves	Installation of Test Connections for Leak Rate Testing and CV Testing: Category A Valves and Containment Isolation Valves. Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Category A valves (per Section XI) and all containment isolation valves (CIVs) should have adequate test connections such that the valves can be safely leak-rate tested to the requirements of ASME, Section XI and 10 CFR 50, Appendix J, without excessive operator realignment of systems and valves, temporary setups, operator radiation exposure, or potential for contamination.	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. Table 3.9-16 in the SSAR lists valves that require IST. Valves that have a safety seat leak function (ASME Section XI type A valves, including containment isolation valves) are designed with the following considerations: • Valve types that provide reliable low leakage • Process isolation valves and test connections to allow their leak tightness to be measured Note that in many cases temporary connections are used to make connections to pressure supplies and test instruments. Such connections are designed so that the connections can be easily made to portable test equipment with minimum radiation exposure.
147	Subsection 4.3.2.1	Component-Related Insights -- IST of Pumps and Valves	Valve Position Indication: Disk Position Indication. Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Consider external disk position indication for CVs that are required to be full stroke tested per Section XI.	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. Table 3.9-16 in the SSAR lists the CVs that require full stroke IST per ASME Section XI. As described in subsection 3.9.6, such CVs will have nonintrusive disk position sensors to facilitate such testing.
148	Subsection 4.3.2.2	Component-Related Insights -- IST of Pumps and Valves	Valve Position Indication: Local Valve Position Indication. Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Consider external position indication for other types of valves which may not have had such indication in the past, e.g., solenoid valves, and non-rising stem valves. All valves within certain categories should be considered for local valve position indication. (See Section 5.3 for further discussion.)	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. Table 3.9-16 in the SSAR lists the valves that have remote position indication IST per ASME Section XI. This table includes solenoid valves, non-rising stem valves, and squib valves.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
149	Subsection 4.3.3.1	Component-Related Insights -- IST of Pumps and Valves	Capability for Full-Stroke Testing of Valves: Loss of Safety Function Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Ensure that a single failure during stroke testing at power will not cause a loss of safety system function.	There are a few situations where a valve is closed during IST, that if an accident occurred and that valve failed to open, a safety function would be lost. This design approach is appropriate based on the following: • TS limit the time that the valve can be closed • The test valve is provided with 1E power and a confirmatory open signal • Providing redundant parallel valves significantly complicates the plant, increasing the chance of leaks / maintenance / radiation exposure and making the pipe routing difficult. • Probabilistic Risk Assessment (PRA) results show that this design approach does not increase risk.
150	Subsection 4.3.3.2	Component-Related Insights -- IST of Pumps and Valves	Capability for Full-Stroke Testing of Valves: Loss of Containment Integrity Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Ensure that a single failure during stroke testing at-power will not cause a loss of containment integrity.	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. All remotely operated CIVs that are opened at power to perform ISTs have automatic closure signals. As a result, if an accident occurred during such an IST and a single failure occurred the containment would still be isolated.
151	Subsection 4.3.3.3	Component-Related Insights -- IST of Pumps and Valves	Capability for Full-Stroke Testing of Valves: Excessive Pressures Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Ensure that a single failure during stroke testing at-power will not subject a system to pressures in excess of their design pressure.	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. A single failure during an IST will not subject the AP600 systems to pressures beyond their design pressure.
152	Subsection 4.3.4	Component-Related Insights -- IST of Pumps and Valves	Stroke Time Testing Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Provisions should be made in the design to facilitate stroke time testing of Section XI Category A valves while the plant is at-power, including rapid acting valves and control valves.	The AP600 systems are designed so that required plant testing can be performed easily and reliably. Chapter 3.9.6 describes the AP600 IST plan. Remotely operated valves are stroke time tested during their periodic stroke IST. The AP600 facilitates this testing with the following: • Few rapid acting valves are used • Increased margin is provided between the design operating time and the safety limits • Remote position sensors are provided As a result, the valve stroke times can be easily verified remotely.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
153	Subsection 4.3.5.1	Component-Related Insights -- IST of Pumps and Valves	Pump Testing: Testing During Plant Operation Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: Ensure that system design has sufficient flexibility to allow pump testing during plant operation. The system should allow flow to be varied so that a reference value of flow or differential pressure can be established for the test without major system reconfiguration. There should also be adequate, installed instrumentation to run the necessary tests, including suction and discharge pressure, differential pressure, and flow-rate. One means of improving flow instrumentation is to include flow-rate instruments in the minimum flow recirculation line.	**NOT APPLICABLE:** This item does not apply to the AP600 because it has no safety-related active pumps. Chapter 3.9.6 describes the AP600 IST plan. This table shows that there are no pumps in the IST plan.
154	Subsection 4.3.5.2	Component-Related Insights -- IST of Pumps and Valves	Pump Testing: Vibration Monitoring Current plants have had to devise complex test procedures that have often challenged operators and maintenance personnel due to designs that make testing very difficult, if possible at all. One of the areas where the design can be enhanced: There should be installed pump vibration monitoring instrumentation to allow for trending and IST of pumps.	**NOT APPLICABLE:** This item does not apply to the AP600 because it has no safety-related active pumps. Chapter 3.9.6 describes the AP600 IST plan. This table shows that there are no pumps in the IST plan.
155	Section 4.4	Component-Related Insights -- Circuit Breakers	Breaker Lock-Out Under various conditions large circuit breakers may become locked-out due to protection system actions. These lock-outs were not always alarmed or indicated to the operators. An example is the safety injection pump breaker, which had a lock-out when an attempt was made to close the breaker with the hand switch in the presence of a trip signal. In this case there was no indication of the lock-out and the only means of clearing the condition was to remove and reinstall the fuses at the breaker or manually change the state of the relays.	Circuit breaker control signal block or lock-out will generally occur when an attempt is made to close a breaker in the presence of a trip signal. Note that the trip signal can originate from either the PMS or from the electric system protective devices (relays). If an attempt is made to close a breaker from the CR through the soft control in the presence of a protective system trip signal, the control action will be blocked (but not locked-out) and the operator will be provided with an appropriate message to clarify the system response. If an attempt is made to close a breaker locally at the switchgear in the presence of a trip signal, the breaker may be locked-out at the switchgear. All switchgear lock-out conditions are indicated and reset capability provided.
156	Section 4.5	Component-Related Insights -- Spent Fuel Pool Seals	Inflatable Seals Spent fuel pools have inflatable seals which are typically pressurized with instrument air. Loss of air pressure, among other items, can cause leakage or failure of these seals and subsequent draining of the fuel pool.	The AP600 spent fuel pool does not contain any inflatable seals that require the availability of auxiliary systems to maintain spent fuel pool water inventory.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
157	Section 4.6	Component-Related Insights -- Heat Exchanges	Biofouling There have been numerous instances of biofouling in NPP heat exchangers (HXs), where various types of clams and mussels have grown inside of piping and particularly HXs. This occurs in open-cycle cooling water systems and has caused sufficient fouling so that pressure drops have increased and flows have decreased. This in turn limits the ability to adequately cool components. HXs that have been affected include those for Component Cooling Water System (CCS), RHR, and Emergency Diesel Generators.	The RNS HXs transfer heat from the reactor coolant to the closed CCS. The CCS is chemically controlled with corrosion inhibitors and pH adjustment. The makeup water to the CCS is demineralized water. When the CCS water chemistry is maintained as specified, there is no potential for biological fouling of any of the components which are cooled by the CCS, including the RNS heat exchangers. The CCS is in turn cooled by the open service water system which releases its heat into the ultimate heat sink via a cooling tower. The SWS is a relatively small open cooling system which is chemically controlled to maintain appropriate concentrations of biocide, algicide, pH adjustor, corrosion inhibitor, scale inhibitor, and a silt dispersant. Refer to the item 7 response for more information on the SWS. (Subsection 9.2.1.2.2) Flows and temperature instruments on the inlet and outlet of both the process-water side and the cooling-water side of the CCS and RNS HXs, enable the use of thermal performance evaluations to detect degradation. The AP600 diesel generators use a closed cooling system with air-cooled radiators; therefore, biofouling concerns are not applicable to the diesel generators. Procedure development is the responsibility of the COL applicant as stated in Section 13.5 of the SSAR.
158	Section 4.7	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.	**THIS ISSUE INPUT** INTO THE DESIGN ISSUES TRACKING SYSTEM.
159	Section 4.8	Component-Related Insights -- Neutron Monitors	Design Flaw in BWR Intermediate Range Monitors A design flaw was identified in BWR Intermediate Range Monitors whereby the failure of a power supply fuse resulted in inoperability but was not annunciated nor did it create a trip situation from the detector output.	A failed nuclear instrument power supply fuse results in an instrument output that is "out-of-range." If a parameter measurement is outside the range of the instrument (note that the data quality would be good), then this "out-of-range" information is indicated on the workstation display to the operator.
160	Section 4.9	Component-Related Insights -- Instrument Air Dryers	Desiccant Carry-Over Due to a failure in the Instrument Air (IA) system filter, the desiccant from the dryer assembly carried over into the IA system and caused a failure of solenoid valves. This in turn caused a CIV to become inoperable.	The after-filter design differential pressure capability is greater than the maximum differential pressure. Should the filter become plugged, it is designed not to fail. The dryer package will have alarms to identify high differential pressure across the filters.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
161	Subsection 5.1.1	Local Control Stations -- General Considerations	Use of HFE Principles in LCS Design Local control stations (LCSs) serve as interfaces between the operators and the plant, similar to the workstations in the CR. Hence, the approach to their design should reflect the same HFE considerations given to the MCR, i.e., they should be designed using the same methods, standards, guideline, and principles. The design of LCSs should be guided by the function and task analyses used to analyze the human role in the plant. It should be determined that functions to be performed at LCSs will not be compromised by human limitations and that the design of the LCS meets the needs of the operator for process information, means of effecting control, feedback on control actions, and an adequate working environment. In addition, the design of each LCS should be consistent with that of other LCSs and should conform to plant-wide conventions regarding coding, labelling, information display, and operation of controls. Labelling should be well-engineered, consistent, thoroughly applied throughout the plant, and appropriately designed to avoid wrong-unit/wrong-train type errors.	LCSs in the AP600 will be designed using the same HFE design process and considerations as will be used for the MCR and HSI. Refer to SSAR Section 18.8. Each LCS will be analyzed and designed to accommodate the following: (a) expected modes of operation, including maintenance and refueling; (b) function identification and task analysis; and (c) staffing levels needed. The design process will identify the individual tasks necessary to perform the LCS's functions. Any MMI designed for the LCS will follow the same process, principles, guidelines, conventions, and codings as was applied to the MMI in the MCR. Plant-wide conventions regarding equipment coding, labelling, and operations of controls will also be applied to the design and layout of LCSs.
162	Subsection 5.1.2	LCSs -- General Considerations	Functional Allocation Considerations In discussing problems that might be anticipated with future LCSs, Hartley *et al.* (1984) pointed to the allocation of an increasing number of LCSs to automatic or semi-automatic systems (as opposed to human operators). The difficulties they anticipated were the same as those that can arise from increasing automation in the CR, i.e., the potential loss of operators' situation awareness, and hands-on control skills (O'Hara, 1993) as their primary role becomes one of monitoring rather than controlling. A related observation was made during the plant visits undertaken for NUREG/CR-6146.	The LCSs will be designed using the same design process as that used for the MCR and the HSI. Refer to SSAR Section 18.8. One of the design objectives for the AP600 M-MIS is to present information to the operator in such a way that the operator is able to maintain situation awareness. The WPIS displays in the MCR will be designed to accomplish this objective. For LCSs, the respective interface will be designed to allow the local operator to maintain an awareness of the situation; to effectively monitor and verify the status of any automatically controlled local functions; and to properly execute any required local manual actions.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
163	Subsection 5.1.3	LCSs -- General Considerations	HSI Consistency With Main Control Room The reviews undertaken for NUREG/CR-6146 involved 11 site visits to observe LCSs. At all of the plants, operators in the CR had access to computer-based displays in addition to conventional displays. These displays provided high-level information, e.g., indications that represented an integration of several parameters, of the value of a set of parameters plotted over time. However, in only one of the plants were such displays available at the shutdown panel. This issue may become more significant in advanced plant designs, where CRs are computer workstation-based, while the LCSs (such as the remote shutdown panel) are based on conventional HSI. In such a plant, operators at remote shutdown stations might be forced to gather information about the status of the plant and the effectiveness of their actions by unaccustomed means.	The workstation in the AP600 remote shutdown room will be identical to the Reactor Operator's workstation in the MCR. The M-MISs available at the operator's workstation in the MCR will also be available at the remote shutdown room workstation. Therefore, the operator will obtain plant information and control the plant from the remote shutdown workstation in the same manner as he does from the MCR workstation. The MMI and workstation design for an LCS will follow the same process, principles, guidelines, conventions and codings as was applied to the HSI in the MCR.
164	Section 5.2	LCSs -- Functional Centralization	Distribution of Safety Functions Functional Centralization (FC) refers to the manner in which the safety functions of LCSs are distributed throughout the plant. This embodies many of the systems engineering characteristics of LCSs and their functional organization. A plant with low FC has a wide distribution of safety functions on many local panels throughout the plant. Such plants also heavily use local control of individual components. A plant with high FC has all safety functions integrated into a single panel which contains all necessary controls and displays. FC affects human performance through its impact on such factors as communication workload, crew coordination, time to complete actions, and requirements for procedural complexity. In NUREG/CR-5572, it was shown that centralization of functions at multifunction control panels was associated with large potential reductions in risk. When considered at the design stage, the risk reduction benefit would be high.	The AP600 plant design is such that it has a high degree of FC, i.e., it has all safety functions integrated into a single panel which contains all necessary controls and displays. This panel is the reactor operator workstations in the MCR. The AP600 I&C architecture will be such that all process information that is available via the plant control system will be available throughout the plant. Communication ports will be located throughout the plant to allow workstations to be used locally at the equipment for "local control", monitoring activities, maintenance activities, or other functions. Local indication and/or controls will not be used except where required by code, regulatory requirements, URD or for operation of the process where portable interfaces with the plant control system would be a hindrance. Through the use of either portable or permanently installed interfaces and/or displays, plant personnel can access any monitored parameter in any location in the plant. By using this technique, local indicating devices will not generally be required and an auxiliary operator can monitor the whole system from one location.
165	Section 5.3	LCSs -- Valve Position Indication (VPI)	Lack of Local Valve Position Indication NUREG/CR-6146 found that many manual valves, even those found to be the most risk-significant manual valves, lacked local position indication. Without such explicit indication, the position of the valve is inferred from stem position (for rising stem valves) or determined by checking the valve in the closed direction. Both methods have potential problems, as discussed in the NUREG/CR. OER also identified incidents that were caused by poor or missing local VPI. The nature of the position indication should be appropriate to the use of the valve.	Where appropriate for the given manual valve type, the valve design specification will specify a local-reading mechanical position indication as a required design feature. Most valves will show their position by their mechanical properties. For example; a "rising stem" for gate valves may be used, while a 1/4-turn handwheel may be used for ball and butterfly valves.

TABLE 1 (Continued) OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
166	Subsection 5.4.1	LCSs -- Miscellaneous Items	Space at LCSs Often there is not enough room for operators to work at the remote shutdown panel. In particular, sufficient space for handling procedures is needed at the remote shutdown panel as well as at many other local panels.	The workstation in the AP600 remote shutdown room will be identical to the Reactor Operator's workstation in the MCR. The M-MISs available at the operator's workstation in the MCR will also be available at the remote shutdown room workstation. This includes the CPS. Therefore, the operator will obtain plant information, and operate and control the plant from the remote shutdown workstation in the same manner as he does from the MCR workstation. The CPS and its use of multiple VDUs (dynamic roadmap screen, main interface screen and supplemental information) eliminates the need to ensure adequate laydown space is available at the workstation for handling paper procedures. Task analysis will be performed for other LCSs and if laydown space is needed then this need will be addressed.
167	Subsection 5.4.2	LCSs -- Miscellaneous Items	Steam Generator Dump Valves Manual operation of PWR SG atmospheric dump valves is often very difficult because of complicated manual arrangements, very high noise levels, high heat loads, and sometimes inconsistent valve operation with valves in close proximity to each other.	Under normal power operation, the operation of the power-operated relief valves (PORVs) is automatically controlled by steamline pressure during plant operations. The PORVs automatically modulate open and exhaust to atmosphere whenever the steamline pressure exceeds a predetermined setpoint. The setpoint is selected between no-load steam pressure and the set pressure of the lowest set safety valves. For their use during plant cooldown, the power-operated atmospheric relief valves are automatically controlled by steamline pressure, with remote manual adjustment of the pressure setpoint from the CR or the remote shutdown workstation. To effect a plant cooldown, the operator manually adjusts the pressure setpoint downward in a step-wise fashion. Manual control at the valve is not provided for the PORVs. The PORV discharges are on the roof of the auxiliary building and discharges via a silencer to limit noise levels. The SG power-operated atmospheric relief valves provide a nonsafety-related means for plant cooldown by discharging steam to the atmosphere when the turbine bypass system is not available. Under such circumstances, the relief valves (in conjunction with the startup feedwater system) allow the plant to be cooled down at a controlled cooldown rate from the pressure setpoint of the lowest set of safety valves down to the point where the RNS can remove the reactor heat. The safety-related means of decay heat removal and plant cooldown is attained by means of the passive RHR system and independent on the PORVs.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
168	Subsection 5.4.3	LCSs -- Miscellaneous Items	Personnel Overexposure Various areas of the plant have the potential for high radiation fields that could lead to personnel overexposure, therefore all plants have installed radiation detectors and alarms. Additionally, however, the malfunction of certain equipment can lead to very high radiation levels. This equipment includes incore instrument thimbles and traveling incore probes (TIP). There should be appropriate local warning devices (and perhaps also CR alarms) to alert personnel when equipment, such as TIPs and incore thimbles are not shielded and the potential exists for high radiation fields.	The AP600 incore instrumentation does not include TIPs or movable detectors. The incore thimble tubes are installed and not moved during plant operation. They do not present any potential for over-exposure of personnel to radiation while installed. These thimble tubes are withdrawn into the integrated head package prior to head removal in preparation for refueling. After thimble tube withdrawal, the integrated head is lifted and set down onto a thick bottom shielding plate. The shielding plate is attached and the head is then lifted into a shielded vault. The thimble tubes also do not present potential for over-exposure of personnel to radiation during shutdown. Area radiation monitors (ARMs) are provided to supplement the personnel and area radiation survey provisions of the AP600 health physics program described in Section 12.5 and to comply with the personnel radiation protection guidelines of 10 CFR 20, 50, 70, and Regulatory Guides 1.97, 8.2, 8.8, and 8.12. In addition to the installed detectors, periodic plant environmental surveillance is established. AP600 normal and accident plant radiation monitoring is described in SSAR Section 11.5. Additional portable monitoring, including that required to meet NUREG-0737, Item III.D.3.3, is the responsibility of the COL applicant.
169	Subsection 5.4.4	LCSs -- Miscellaneous Items	Emergency Lighting Emergency lighting is required in the plant for personnel safety and for nuclear safety reasons. The two key nuclear safety areas requiring emergency lighting are the scenarios of 10 CFR 50, Appendix R, Section III.J and SBO. Operating experience has shown that NPPs have tended to pay less attention to the lighting requirements during an SBO scenario. A common practice is to depend on auxiliary operator use of flashlights. This can be a problem due to the potential unavailability of flashlights in an emergency and also because the physical use of one while operating equipment and communicating with the CR may be cumbersome.	The AP600 design includes extensive use of plant automation and distributed control. The distributed control system minimizes the need for LCSs to meet the requirements of either 10 CFR 50 Appendix R or 10 CFR 50.63 (SBO). Emergency lighting is provided in the MCR and the remote shutdown workstation to illuminate these areas for emergency operations upon loss of normal lighting. See the AP600 SSAR, Chapter 7 for a description of the plant control system. The emergency lighting system is described in AP600 SSAR subsection 9.5.3.2.2 The AP600 design includes two non-Class 1E diesel generators separated by a fire barrier. Following a fire, at least one of the diesel generators will be available to provide power to normal lighting in areas of the plant not damaged by the fire. During SBO the two non-Class 1E diesel generators are available to provide power to normal plant lighting. The onsite non-Class 1E diesel generators are described in AP600 SSAR, subsection 8.3.1.

TABLE 1 (Continued)				
OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
170	Section 6.1	Shutdown Operations -- Procedures	Outage Management and Planning Due to the importance of outage management and planning to shutdown operations, consideration should be given to the development of scheduling tools (e.g., computer-based outage planning and management aids, see Shore *et al.*) to assist in outage planning, scheduling, and management. Further, an interactive up-to-date PRA, that allows a determination of the risk significance of removing selected pieces of equipment from service, would serve to improve outage risk management.	The Design Reliability Assurance Program, or D-RAP, uses probabilistic (and other) measures to identify risk-significant structures, systems and components (SSCs), then generates maintenance recommendations and other information for use in the plant owner's operational reliability assurance activities. The D-RAP is presented in Chapter 16.2 of the AP600 SSAR. The non-site-specific critical items list represents the plant SSCs that have been flagged as risk-significant based on selected PRA risk important measurement thresholds. For these SSCs, Westinghouse develops maintenance recommendations that will be considered by the COL applicant in his plant maintenance program, including his outage planning activities. The COL applicant is responsible for addressing outage planning. There is no interactive PRA that the COL applicant receives from Westinghouse to calculate risk impacts of SSC removal from service. However, the D-RAP critical items list whose selection basis is risk-increase measures, are those items whose unavailability significantly increases risk including risk during shutdown operations. Thus, they should be given special attention in outage planning.
171	Section 6.2	Shutdown Operations -- Procedures	Operator Training Operators are often confronted with unfamiliar situations during shutdown operations. Training programs should be improved to appropriately consider the safety implications of these conditions. As an example, simulators should be able to model important shutdown operations to a greater extent than they currently do.	Training Program development is the responsibility of the COL applicant as stated in Section 13.2 of the SSAR. The AP600 ERGs (AP600 document number GW-GJR-100) provide the function restoration guidelines for shutdown operations, providing guidance to the operators for emergency situations when the plant is shutdown.
172	Subsection 6.3.1	Shutdown Operations -- Procedures	Loss of RHR Capability Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. A particular area needing clear procedural coverage is: Loss of RHR capability, including alternate means of removing decay heat such as gravity drain from refueling waste tanks, safety injection, accumulators, or core flood tanks. Procedures should also address operator-induced loss of RHR and restoration of RHR upon loss.	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). The AP600 ERGs provide the function restoration guidelines following the loss of the RNS during shutdown. In addition, the AP600 PXS is required to be available (via tech specs) through mode 5. See the response to Item 73.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
173	Subsection 6.3.2	Shutdown Operations -- Procedures	Inadvertent Draining of Reactor Vessel Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Clear procedural coverage should contain adequate guidance for lowering RV level when operating in the RHR cooling mode. Also, there should be precautions against inadvertently draining the RV or draining the RV via multiple pathways at the same time. An example of inadvertent draining is having the RHR isolation valves (from the primary) open at the same time as other RHR valves, which can drain water from the RHR system. (LERs 50-265/87-010, 50-341/87-036, and 50-382/86-015).	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). As described in subsection 5.4.7 of the SSAR, the AP600 RNS has been designed with features that address Generic Letter 88-17 regarding mid-loop operations. These features prevent inadvertent lowering of RV vessel level below that necessary to maintain effective decay heat removal. The operational procedures will rely upon RCS instrumentation to provide sufficient indications and alarms to determine the status at any time. The instrumentation is listed below: **Hot Leg Level Instrumentation** - The AP600 RCS contains level instrumentation in each hot leg with indication in the MCR via an appropriate display. In addition, the wide-range pressurizer level instrumentation used during cold plant operations is available to measure to the bottom of the hot legs. There is continuous level indication in the MCR from the normal level in the pressurizer to the range of the two narrow-range hot leg level instrumentation. Alarms are provided to alert the operator when the RCS hot leg level is approaching a low level. The isolation valves in the line used to drain the RCS close on a low RCS level during shutdown operations. Operations required during mid-loop are performed by the operator in the MCR. The level monitoring and control features significantly improve the reliability of the AP600 during mid-loop operations. **Reactor Vessel Outlet Temperature** - RCS hot leg wide-range temperature instruments are provided in each hot leg. The orientation of the wide-range thermowell-mounted resistance temperature detectors enable measurement of the reactor coolant fluid in the hot leg when in reduced inventory conditions. In addition, at least two incore thermocouple channels are available to measure the core exit temperature during midloop RHR operation. These two thermocouple channels are associated with separate electrical divisions.
174	Subsection 6.3.3	Shutdown Operations -- Procedures	Reduced Inventory Operations Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. A particular area needing clear procedural coverage is: Establishing and maintaining mid-loop (in PWRs) or other reduced inventory operations.	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). SSAR subsection 5.4.7.2.1 provides a description of the AP600 design features that have been incorporated to address mid-loop and reduced inventory operations. See the responses to Items 73 and 172 for more information.

TABLE 1 (Continued)				
OPERATING EXPERIENCE REVIEW FOR THE AP600				
Issues Addressed By NUREG 0711 Appendix B				
Item	**Issue Reference**	**Issue/Scope**	**Human Factors Aspect/Human Performance Issue**	**Human Factors/Human Performance Issue Addressed by AP600 Design**
175	Subsection 6.3.4	Shutdown Operations -- Procedures	Temporary RCS Boundaries Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Clear procedural coverage is needed in the use of temporary RCS boundaries such as freeze seals, nozzle dams, and thimble tube seals, including contingency plans in case of failure.	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). See the response to RAI 440.55 and Items 73, 172 and 174. The following AP600 design features reduce the risks associated with temporary RCS boundaries: • SG nozzle dams - the AP600 SG nozzle dams are classified as AP600 Equipment Class C so that the design, manufacture, installation, and inspection of this boundary (when installed) is controlled by the following requirements: 10 CFR 21; 10 CFR 50, Appendix B; Regulatory Guide 1.26 Quality Group C; and ASME Boiler and Pressure Vessel Code, Section III, Class 3. In addition, this pressure boundary is classified as Seismic Category I so that it is protected from failure following a safe shutdown earthquake (SSE). • Elimination of temporary plugs for nuclear instrumentation - The AP600 does not contain bottom-mounted instrumentation that requires temporary plugging during shutdown and refueling. The AP600 utilizes a fixed incore system. • Current plants remove the excore detectors from above the excore housings through the floor of the refueling cavity. During refueling operations, these holes are plugged to facilitate flooding of the refueling cavity. The AP600 has eliminated these temporary plugs by designing the excore instrumentation to be inserted from below the excore housings. • Reduced reliance on freeze seals - the AP600 has reduced the potential applications for freeze seals by reducing the number of lines that connect to the RCS and by providing the ability to perform operability tests on many valves that connect to the reactor coolant pressure boundary. This improved IST reduces the requirements for disassembly of reactor coolant pressure boundary valves to test their operability. The use of freeze seals during a forced outage will typically occur in cold shutdown (Mode 5), when the PXS is required to be available.
176	Subsection 6.3.5	Shutdown Operations -- Procedures	LOCAs During Shutdown Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. A particular area needing clear procedural coverage is: LOCAs during shutdown, including intersystem LOCAs and operator-induced LOCAs. (Also see item under subsection 6.5.3.)	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). The shutdown PRA has addressed the risk of LOCA during shutdown. SSAR subsection 5.4.7.2.2 provides a description of the AP600 design features that have been incorporated to address inter-system LOCA. See the responses to items 73 and 172 for more information.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
177	Subsection 6.3.6	Shutdown Operations -- Procedures	Boron Dilution Accidents Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Clear procedural coverage is needed during rapid boron dilution accidents, such as the startup of an RCP in an idle loop that has a significantly lower boron concentration than the reactor.	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). Such a scenario has been postulated for current plants. Following an SGTR event, the operators are instructed that if they must restart the RCPs, they must start the RCPs in a loop other than the faulted SG. This also applies to the AP600 and is included in the AP600 ERGs in the guideline used for recovering from an SGTR event. Such a precaution may also be used in recovery procedures where startup of an RCP is required following long-term operation with a stagnant RCS loop that may be at a significantly lower boron concentration.
178	Subsection 6.3.7	Shutdown Operations -- Procedures	Containment Integrity During Shutdown Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Clear procedural coverage is needed for control of containment integrity during shutdown, including expeditious closure of open hatches and penetrations on a loss of RHR.	Procedure development is a COL applicant responsibility, however the AP600 TSs (Section 16.1, subsection 3.6) explicitly define which modes of operation and under which specific conditions containment integrity is required. The "Bases" section of each of the 3.6 TSs discusses the rationale for the requirement and includes consideration of the following aspects of plant design and operation for the bases: • Available time for mitigative actions (including time required for such actions) • Mitigating features available • Potential and severity of potential accidents based on initial conditions
179	Subsection 6.3.8	Shutdown Operations -- Procedures	Fire Protection Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Clear procedural coverage is needed for fire protection during shutdown.	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). The Fire Protection System is described in SSAR subsection 9.5.1 and a fire protection analysis is provided in SSAR Section 9A.
180	Subsection 6.3.9	Shutdown Operations -- Procedures	Spent Fuel Pool Cooling Procedures are an important aspect of shutdown operations. Appropriate HFE in the CR and at LCSs that can assist in the implementation of such procedures should also be considered. Additionally, the effective integration of the various HSIs with the procedures is important. Clear procedural coverage is needed for loss of spent fuel cooling.	Procedure development is a COL applicant responsibility (SSAR 13.5 and 18.9). The AP600 spent fuel pool cooling system is not required to operate to mitigate design basis events. In the event the spent fuel pool cooling system is unavailable, the spent fuel cooling is provided by the heat capacity of the water in the pool. Connections to the spent fuel pool are made at an elevation to preclude the possibility of inadvertently draining the water in the pool to an unacceptable level. Further explanations of the spent fuel pool cooling system during abnormal operations can be found in SSAR subsection 9.1.3.4.3 and accompanying subsections. Pertinent safety evaluation information for the spent fuel pool cooling system can be found in subsection 9.1.3.5.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
181	Subsection 6.4.1	Shutdown Operations -- Instrumentation	Independent Measurements of RCS Level Many current plants do not contain permanently-installed instrumentation to monitor the plant's safety status during shutdown. For new plants, instrumentation that appropriately supports shutdown operations should be considered for installation, for example: two independent measures of RCS level, including permanent instrumentation capable of measuring mid-loop conditions accurately. There should be adequate overlap between the RCS level instrument ranges to ensure complete coverage at all levels and to allow comparison between instruments as level changes ranges. Plants should avoid dependency on temporary, tygon tubing type level indicators, which have caused many problems in the past. Additionally, one should consider the potential inaccuracies of mid-loop level indicators that occur when one leg is vented to atmosphere and a slight pressurization of the RCS occurs. Instances have also occurred where the RCS was under slight vacuum, resulting in level measurement inaccuracies. Additionally, there should be available displays and/or alarms of water level information in the refueling area while the reactor vessel head is removed.	The AP600 has incorporated independent hot leg level instruments in each hot leg. These are permanently installed and are capable of measuring mid-loop conditions at shutdown. Their range overlaps with the cold-calibrated wide range pressurizer level instrumentation to allow for continuous measurement of RCS water level during the transition to reduced inventory operations. SSAR subsection 5.4.7.2.1 provides a description of the AP600 design features that have been incorporated to address mid-loop and reduced inventory operations including the hot leg level instruments. See the responses to Items 73 and 172 for more information.
182	Subsection 6.4.2	Shutdown Operations -- Instrumentation	Independent Measurements of Temperature Many current plants do not contain permanently installed instrumentation to monitor the plant's safety status during shutdown. For new plants, instrumentation that appropriately supports shutdown operations should be considered for installation, for example: two independent measurements of core exit temperature.	The design of the AP600 has considered shutdown modes extensively as documented in the various licensing submittals: 1) passive safety systems that are designed to mitigate accidents during shutdown modes (SSAR Section 6.3), 2) TS that apply to the passive safety systems during shutdown modes (SSAR Chapter 16), 3) ERGs (Reference 2) for shutdown modes, 4) quantification of the risk of core damage at shutdown (AP600 shutdown PRA), 5) evaluation of design-basis-initiating events during shutdown modes (AP600 Shutdown Evaluation Report - 6/96). Instrumentation has been designed to appropriately cover all modes of operation including shutdown. RCS loop instrumentation and core exit thermocouples provide independent measurement of reactor coolant temperature during shutdown operations including mid-loop and reduced inventory operations.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
183	Subsection 6.4.3	Shutdown Operations -- Instrumentation	Monitoring RHR System Performance Many current plants do not contain permanently installed instrumentation to monitor the plant's safety status during shutdown. For new plants, instrumentation that appropriately supports shutdown operations should be considered for installation, for example: capability of continuously monitoring RHR system performance, including adequate alarm capability for out of specification temperatures, pressures, and flows.	The AP600 RNS has no safety-related functions during shutdown cooling except maintenance of the reactor coolant pressure boundary and containment isolation if a design basis event occurs. The RNS contains permanently installed instrumentation to monitor system performance as described in SSAR subsection 5.4.7.7. System parameters and alarms necessary for system operation are monitored in the MCR including the following: • RHR pump flow; • RHR HX inlet and outlet temperatures; and, • RHR pump discharge pressure. In addition, the RCS contains instrumentation to control and monitor the operations of the RNS. These include the following: • RCS wide range pressure • RCS hot leg level. Instrumentation is also provided to enable mid-loop operations to be performed from the MCR.
184	Subsection 6.4.4	Shutdown Operations -- Instrumentation	Instrument Ranges and Accuracy Many current plants do not contain permanently installed instrumentation to monitor the plant's safety status during shutdown. For new plants, instrumentation that appropriately supports shutdown operations should be considered for installation, for example: instrumentation containing appropriate ranges and accuracy to monitor shutdown conditions as well as power operating conditions.	The design of the AP600 has considered shutdown modes extensively as documented in the various licensing submittals: 1) passive safety systems that are designed to mitigate accidents during shutdown modes (SSAR Section 6.3), 2) technical specifications that apply to the passive safety systems during shutdown modes (SSAR Chapter 16), 3) ERGs for shutdown modes, 4) quantification of the risk of core damage at shutdown (AP600 shutdown PRA), 5) evaluation of design-basis-initiating events during shutdown modes (AP600 Shutdown Evaluation Report - 6/96). Instrumentation has been designed (including appropriate ranges) to appropriately cover all modes of operation including shutdown.
185	Subsection 6.4.5	Shutdown Operations -- Instrumentation	Dedicated Shutdown Annunciators Many current plants do not contain permanently installed instrumentation to monitor the plant's safety status during shutdown. For new plants, instrumentation that appropriately supports shutdown operations should be considered for installation, for example: use of dedicated shutdown annunciators for special hazardous conditions that arise during shutdown (e.g., refueling cavity low-level alarm). Also consider the use of trend displays during shutdown, such as RV level.	The design of the AP600 Alarm System includes alarms specific to the special conditions that arise during shutdown conditions. The alarm trigger logics include defining plant conditions under which the alarm applies. Applicable trend displays will be used during shutdown conditions, including reactor vessel level or equivalent. The M-MIS includes trend displays as part of the Plant Information System displays that are available to the operator through his workstation. Also, the WPIS will display significant trends for each plant operating mode or significant plant state, including the shutdown modes.
186	Subsection 6.5.1	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. Similar provisions should be made for other containment penetrations that may be open during shutdown evolutions.	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 will be assigned to follow the resolution of this item. **THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM**. Other containment penetrations including containment purge and personnel airlocks provide the ability for rapid closure independent of nonsafety-related support services including ac power.

TABLE 1 (Continued)

OPERATING EXPERIENCE REVIEW FOR THE AP600

Issues Addressed By NUREG 0711 Appendix B

Item	Issue Reference	Issue/Scope	Human Factors Aspect/Human Performance Issue	Human Factors/Human Performance Issue Addressed by AP600 Design
187	Subsection 6.5.2	Shutdown Operations -- Equipment	Fuel Handling Equipment An equipment upgrade that would improve shutdown safety is: improved human engineering of fuel handling equipment. Poorly-designed equipment, in the past, has led to fuel assembly drops and damage. This equipment should also be addressed by the HFE program.	The AP600 fuel handling equipment design has incorporated industry operating data and experience to develop a design that will improve shutdown safety. The use of the operating experience is intended to eliminate any poor design features that were present in previous designs. In addition, several of the leading fuel handling equipment design and maintenance organizations are involved with the design and review of the AP600 fuel handling equipment. To ensure that operating plants have the ability to provide their input into the AP600 fuel handling equipment designs, many of the fuel handling equipment design documents have been reviewed and commented on by personnel at operating plants. Refer to SSAR Section 9.1 for a description of fuel storage and handling.
188	Subsection 6.5.3	Shutdown Operations -- Equipment	Overpressurization An equipment upgrade that would improve shutdown safety is: use valve interlocks to prevent overpressurization of low-pressure piping and components, (LER 50-341/86-045).	The motor-operated valves in the RNS which are connected to the RCS hot leg are interlocked to prevent them from opening when RCS pressure exceeds 450 psig. These valves are also interlocked to prevent opening unless the isolation valve from the IRWST to the RHR pump suction header is closed. SSAR subsection 7.6.1 describes this interlock. SSAR subsection 5.4.7.1.2.5 describes how the RNS provides a low temperature overpressure protection function for the RCS during refueling, startup, and shutdown operations. The system is designed to limit the RCS pressure within the limits specified in 10 CFR 50, Appendix G. The AP600 has also addressed this issue in the ISLOCA report (WCAP-14425).
189	Subsection 6.5.4	Shutdown Operations -- Equipment	Backup Power Sources An equipment upgrade that would improve shutdown safety is: appropriate use of backup onsite power sources, such as emergency diesel generators, and portable power units.	The ac electrical power is not needed to maintain a plant safe shutdown condition for the AP600. Although the diesel generators are not required, generally, if offsite power is lost, they will be available and will automatically start and sequence loads that will enhance the safety of the plant during shutdown conditions.
190	Section 6.6	Shutdown Operations -- Communications	Communications Between MCR and Plant An important aspect of maintaining normal shutdown conditions is adequate communications between the MCR and the rest of the plant. This includes areas where the following activities may take place: maintenance, testing, local operations, and monitoring activities. Effective communications are also very important during any abnormal events that occur during the shutdown period. When designing plant communications systems, care should be taken to consider shutdown operations.	The plant communication system consists of the following systems: wireless communication system, telephone/page system, PABX, sound-powered system, emergency response facility communications, and security communication system. The wireless telephone system is the primary means of communication for plant operations and maintenance personnel. The wireless system consists of wireless belt-clip portable handsets, hands-free type portable headsets, a comprehensive antenna system, and a wireless telephone switch. The telephone/page, PABX telephone, and sound-powered communication systems are for general plant communications and serve as backup to the wireless system. These systems are designed for effective communication between the MCR and the rest of the plant during all modes of operation, including shutdown. The communications system is described in SSAR subsection 9.5.2.

References To Table 1, Operating Experience Review for the AP600 Design

1. "Programmatic Level Description of the AP600 Human Factors Verification and Validation Plan," (draft dated 4/13/95), WCAP-14401 (Non-Proprietary)

2. AP600 Document No. OCS-T5-001, "AP600 Man-In-The-Loop Test Plan Description," Rev. B, WCAP-14395 (Proprietary), WCAP-14396 (Non-Proprietary)

3. WCAP 14644, "AP600 Functional Requirements Analysis and Function Allocation."

4. Electric Power Research Institute, "Advanced Light Water Reactor Utility Requirements Document," Chapter 3, Revisions 5 and 6, issued 12/93

5. AP600 Standard Safety Analysis Report

6. WCAP-14115, Rev. 0, "Review of Nuclear Plant Operating Experience and the Application to the AP600 Design," July 1994

7. WCAP 14114

8. McIntyre, B., "Completion of Westinghouse Activities Related to NUREG-0711," NSD-NRC-96-4845, OCP/NRC0626, October 17, 1996

TABLE 2

RELATED HSI TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR EXPERIENCE EXISTS

Reference Document	**HFE Issues Applicable to the AP600 Design**	**Human Factors/Human Performance Issue Addressed by the AP600 Design**
Ref. 2.1	Interviews Conducted at Fossil Plants with Soft Controls:	
	1) During a startup on a simulator, operators experienced little problem with soft controls as long as events went as anticipated. When problems arose in the startup (such as equipment failing to start, automated systems failing to work) the operators exhibited considerable difficulty in understanding the cause of the problem and recovering from it.	1) The AP600 M-MIS consists of several resources (subsystems) that will work together to alert the operator to the problem, focus his attention on trouble areas, and provide assistance with diagnostics, planning and recovery. These subsystems include the Alarm System, Control (soft control display) System, the Plant Information System (workstation physical, functional and automatic system monitoring displays) and the CPS. See Table 1, response to item 77.
	2) Importance of having redundant methods of calling up the desired displays – there should be multiple paths for accessing a display or control.	2) See the response to Table 1, items 77 and 93 for a description of several AP600 M-MIS resource integration and navigation features. Execution of the HSI Design Implementation Plan, as described in SSAR 18.8, address this issue.
	3) 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.	3) **THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
	4) Providing guidance or design features on how to configure/coordinate a multiple VDU display space.	4) **THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
	5) Importance of providing critical/overview information in parallel to the task being performed.	5) See Table 1, response to item 66.
	6) Supervisory control of automated systems: it is important to detect what it did, explain why it did it, predict what it will do in the future, and understand why it did not perform as expected.	6) The Plant Information System will present to the operator Automatic System Monitoring displays. Automatic system monitoring displays are designed for automatic control systems and automatic protection (reactor and ESF) systems. Each of these displays contain appropriate information, allowing the MCR operators to monitor and supervise the respective automatic system. This information includes what the system did, why, and what is expected in the future.

TABLE 2 (Continued)

RELATED HSI TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR EXPERIENCE EXISTS

Reference Document	HFE Issues Applicable to the AP600 Design	Human Factors/Human Performance Issue Addressed by the AP600 Design
	7) 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 too thick and inaccurate; b) potential problem of multiple individuals simultaneously controlling the same piece of equipment from VDUs at different locations.	7) **THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
Ref 2.2	Soft Control Lessons Learned From Aircraft Industry:	
	1) Lifting finger off the target area touch logic to actuate is more forgiving than when the finger enters the target area to actuate.	1) **THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
	2) "Soft button" to visually depress	2) See response 1) above.
	3) Auditory feedback on "soft button" activation has merit (i.e., sound equivalent to activating a hardware button)	3) See response 1) above.
	4) Display colors for normal and off-normal conditions	4) See response 1) above.
	5) Computer/display response time	5) See Table 1 Item 93.
	6) Linking of alerts, procedures, and configuration tasks	6) See Table 1 Item 77 and 102.
	7) Navigating through displays	7) See Table 1 Item 77 and 93.

TABLE 2 (Continued)

RELATED HSI TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR EXPERIENCE EXISTS

Reference Document	HFE Issues Applicable to the AP600 Design	Human Factors/Human Performance Issue Addressed by the AP600 Design
Ref 2.3	Lessons Learned From Naval Training and Airline Industry (Human Factors Considerations for Group Overview Display):	
	1) Situation awareness of crew	1) See Table 1 Items 66, 68, 74 and 75.
	2) Communication, coordination, and performance	2) See Table 1 Items 66, 69 and 71.
	3) Error detection and recovery	3) See Table 1 Item 55, 66, 68, 74, and 105.
Ref 2.4	Lessons Learned From Naval and Airline Industry (Role of Advanced CR Features for Enhancing Crew Performance):	
	1) Team performance	1) See Table 1 Items 66 and 68.
	2) Communication	2) See Table 1 Items 66, 66, 96 through 100, and 190.
	3) Crew size	3) See Table 1 Item 63, 64, and 65.
	4) Skill/knowledge	4) See Table 1 Items 67 through 72.
	5) Stress/workload	5) See Table 1 Items 64, 66, and 71.
	6) CR design features to enhance situation awareness, verbal communication, and error identification	6) See Table 1 Item 52, 66, 68, 74, 75, 96 through 100 and 190.
	7) Situation Awareness	7) See Table 1 Items 66, 68, 74 and 75.
	8) Overlap of expertise	8) See Table 1 Items 63, 65 and 70.

TABLE 2 (Continued)

RELATED HSI TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR EXPERIENCE EXISTS

Reference Document	HFE Issues Applicable to the AP600 Design	Human Factors/Human Performance Issue Addressed by the AP600 Design
Ref 2.5	Lessons Learned From Nuclear and Airline Industry (Navigation Through Large Display Networks):	
	1) The large scope of computerized CR applications necessitates large display structures involving thousands of displays. Design errors can result in getting lost in large display networks.	1) See Table 1, Item 77, 91 and 93. SSAR Section 18.8 includes the Implementation Plan for the HSI Design that addresses the criteria of Element 7 of NUREG-0711. For each HSI, including the Plant Information System (workstation displays), an HFE design guidelines document is developed that provides guidelines to the HSI designers on the conventions, symbols, color coding and dynamic characteristics to be used in the design of the respective HSI. Issues such as navigation issues will be addressed by the guidelines document. The HSI Design plan also includes concept testing and design reviews.
	2) Overview displays	2) See Table 1, Items 66, 74 and 93.
Ref 2.6	Lessons Learned From the Space Program:	
	1) Information display issues include structures that constitute a display, organization of those structures, and methods of directing the user's attention to specific display areas.	1) See Table 1, Item 77, 91 and 93. SSAR Section 18.8 includes the Implementation Plan for the HSI Design that addresses the criteria of Element 7 of NUREG-0711. For each HSI, including the Plant Information System (workstation displays), an HFE design guidelines document is developed that provides guidelines to the HSI designers on the conventions, symbols, color coding and dynamic characteristics to be used in the design of the respective HSI. Issues such as navigation issues will be addressed by the guidelines document. The HSI Design plan also includes concept testing and design reviews.
	2) Display response time	2) See Table 1 item 93.
	3) Navigating through displays	3) See Table 1 Item 77, 91, and 93. Also, see response 1) above.
	4) Procedural errors	4) See Table 1 Items 50, 51, 91, 105 and 106.
	5) Errors of confusion occur when one word, function, or command is mistaken for another.	5) See Table 1 Items 55 and 61.
	6) Errors in detection and monitoring	6) See Table 1 Items 55, 66, 68, 74 and 105.

TABLE 2 (Continued)

RELATED HSI TECHNOLOGIES WHERE LITTLE OR NO NUCLEAR EXPERIENCE EXISTS

Reference Document	HFE Issues Applicable to the AP600 Design	Human Factors/Human Performance Issue Addressed by the AP600 Design
Ref 2.7	Lessons Learned From Electrical, Gas, and Oil Industries:	
	1) Performance aids	1) See Table 1 Items 26, 69, 77, 79, 80, and 88.
	2) Integrated displays	2) See Table 1 Items 66, 71, 74, 77, 80, 88 and 102.
	3) Unanticipated situations	3) See Table 1 Items 68 and 70.
	4) "Openness" of work area and shared information	4) See Table 1 Items 66, 74, and 75.
	5) Team interaction	5) See Table 1 Items 66, 69, and 71.

References For Table 2, Related HSI Technologies Where Little Or No Nuclear Experience Exists

2.1 Roth, E. M., and D. G. Hoecker, AP600 Document Number OCS-J1-005 Revision A, "Human Factors Issues Associated with Soft Controls: Design Goals and Available Guidance," Westinghouse Science & Technology Center, dated 2/1/94.

2.2 Degani, A., E. A. Palmer, and K. G. Bauersfeld, "Soft" Controls for Hard Displays: Still a Challenge," from the Proceedings of the Human Factors Society 36th Annual Meeting -- 1992.

2.3 Mumaw, R. J. and E. M. Roth, AP600 Document Number OCS-J1-006 Revision A, "Human Factors Considerations for the Design of a Group Overview Display (aka Wall Panel Information System)," Westinghouse Proprietary Class 2, June 1994.

2.4 Stubler, W. F., E. M. Roth, and R. J. Mumaw, "The Role of Advanced Control Room Features for Enhancing Crew Performance."

2.5 Roth, E. M., W. F. Stubler, and R. J. Mumaw, "Navigating Through Large Display Networks in Dynamic Control Applications," Presented at the 34th Annual Meeting of the Human Factors Society, October 1990, Orlando, Florida.

2.6 "Human Computer Interface Guide -- Space Station Freedom Program Office," document number SSP 30504, National Aeronautics and Space Administration, June 1991.

2.7 Roth, E. M., "Analyzing Decision-Making in Process Control: Multi-disciplinary Approaches to Understanding and Aiding Human Performance in Complex Tasks," Westinghouse Science and Technology (STC) Report, 95-1SW5-CHICH-P1, April 25, 1995.

TABLE 3

OPERATOR INTERVIEW ISSUES

Reference Document	HFE Related Issues	Human Factors/Human Performance Issue Addressed by the AP600 Design
Ref 3.1	Westinghouse-Conducted Operator Interview:	
	1) Simulated accidents in NPPs resulted in cognitively demanding situations where situation assessment enabled operators to handle aspects of the situation that were not covered by procedures.	1) See Table 1 Items 66, 68, 74 and 75.
	2) Cognitive performance in simulated emergencies	2) See Table 1 Items 49, 67 through 72.
	3) Crew interaction in simulated emergencies	3) See Table 1 Items 49, 66, 69, and 71.
	4) Training for unanticipated situations	4) See Table 1 Items 49, 68, and 70.
	5) In cognitively demanding situations, the ability of the operator to form accurate situation assessments and to generate response plans to cover aspects of the situation that are not fully addressed by the procedures is important	5) See Table 1 Item 68.
Ref 3.2	Westinghouse-Conducted Operator Interviews:	
	1) Situation assessment	1) See Table 1 Items 66, 74, and 75.
	2) Cognitive skills are needed in situations where formal procedures may not exist or may not be as prescriptive as they could be	2) See Table 1 Items 68, 69, and 70.
	3) Complex decision-making tasks in NPPs	3) See Table 1 Items 68, 69, and 71.
	4) Cognitive skill training	4) See Table 1 item 70.
	5) Performance under stress (workload)	5) See Table 1 Items 64 and 66.

TABLE 3 (Continued)

OPERATOR INTERVIEW ISSUES

Reference Document	HFE Related Issues	Human Factors/Human Performance Issue Addressed by the AP600 Design
Ref 3.3	Westinghouse-Conducted Operator Interviews: AP600 Soft Controls:	
	1) 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.	1) **THIS ISSUE INPUT INTO THE DESIGN ISSUES TRACKING SYSTEM.**
	2) "Soft slider" vs "soft pushbutton": operators carry out manual control tasks faster with open/close pushbuttons than with the slider.	2) See the response to 1) above.
Ref 3.4	Westinghouse-Conducted Operator Interviews:	
	1) Crew structure: the variations in crew structures and action of crew members (i.e., aggressively seeking information or being passive) indicate that operator training should give more attention to the roles and responsibilities of crew structure.	1) Training Program Development is the responsibility of the COL applicant as stated in SSAR Section 13.2. Insights to the training program will be available, following the HFE verification and validation, for consideration by the COL applicant during training program development.
	2) Procedures: during simulator retraining, operators made use of printed procedures during test trials, however, on a few trials the procedures were executed from memory.	2) See Table 1 Items 67, and 71.
	3) Problem recognition	3) See Table 1 Items 68, 69, 74, and 77.

TABLE 3 (Continued)

OPERATOR INTERVIEW ISSUES

Reference Document	HFE Related Issues	Human Factors/Human Performance Issue Addressed by the AP600 Design
	4) Planning: operator activities in the areas of planning strategy and obtaining feedback about the results of control actions would benefit most from new operator aids or CR improvements.	4) See Table 1 Items 69, and 77.
Ref 3.5	Interviews with operators involved with simultaneous reactor trips at the Diablo Canyon units: Shared CR concerns during a dual reactor trip:	
	1) Noise and confusion existed in the CR. Operators had to listen carefully and verify to and from whom each verbal communication was directed. Since personnel at both units were executing the same procedures, but not exactly at the same rate, they had to be careful that they were responding to the correct procedure step. This event is not modeled in simulator training and presented to operators as a new, unique challenge. This event emphasizes the importance of formal, repeat-back communications.	1) **NOT APPLICABLE:** The AP600 design is a single unit. Even if two units are built on one site, they will be standalone and separate. The dual units will not include a shared CR.
	2) Plant communications: When a single unit trips, people outside the CR are instructed to call the other unit to find out what is going on. With the loss of both units, not everyone is sure who to call. The result is a high volume of phone calls to a unit that is busy trying to proceed through recovery procedures.	2) See the response to 1) above.
	3) Alarms: one source of confusion was from alarms on common systems such as service air. It became confusing as to which unit's personnel should respond.	3) See the response to 1) above.
	4) SPDS positioning	4) See Table 1 Item 34.
	5) Emergency lighting in the turbine building was dark for some minutes causing a concern for personnel.	5) See Table 1 Item 169.

TABLE 3 (Continued)

OPERATOR INTERVIEW ISSUES

Reference Document	HFE Related Issues	Human Factors/Human Performance Issue Addressed by the AP600 Design
	General CR concerns: 6) Procedural problems in AFW flow and charging pump operations not related to the dual trips, was a procedural glitch that impeded the operators in throttling AFW flow early enough to prevent a significant cooldown and drop in pressurizer level. During a trip with the positive displacement charging pump (PDP) running, pressurizer level is lost more rapidly during cooldown than if a centrifugal charging pump is running. Operators at bo\u units felt that they should be instructed in the recovery procedures to start a centrifugal pump if the unit had been operating with the PDP.	6) Procedure development is the responsibility of the COL applicant (SSAR 13.5). The AP600 CVS uses centrifugal pumps only. Following a plant trip in the AP600, an excessive cooldown is avoided by automatically controlling the feedwater flow to the SGs.
	7) Visibility of annunciator screen	7) SSAR Section 18.8 includes the Implementation Plan for the HSI Design that addresses the criteria of Element 7 of NUREG-0711 and for each HSI, including the Alarm System, a functional requirements document. This document specifies functional design requirements such as visibility and legibility.
	8) Multiple annunciator system alarm states: It was complicated and difficult for operators to respond quickly to alarms that were near their setpoint and came in and out rapidly. An operator may not have the time to analyze every alarm to decide what is the actual condition.	8) See Table 1 Item 82, 83, and 86
	9) CR was crowded with little room to walk around freely.	9) A full scale mockup of the MCR will be used to verify the layout. (SSAR 18.8)
	10) The location of phones in CR was not conducive to responding to plant problems.	10) See the response to 9) above.
	11) High noise level from computers.	11) See Table 1 Item 100.

TABLE 3 (Continued)

OPERATOR INTERVIEW ISSUES

Reference Document	HFE Related Issues	Human Factors/Human Performance Issue Addressed by the AP600 Design
Ref 3.6	Westinghouse-Conducted Operator Interviews -- Ongoing Activity	
	NPP Normal Operation:	
	1) Operator performance is influenced by cognitive skills as well as institutional practices.	1) See Table 68, 69, and 70.
	2) CR procedures	2) Procedure development is the responsibility of the COL applicant (SSAR 13.5).
Ref. 3.7 and Ref. 3.8	Westinghouse-Conducted Operator Interviews for Feedwater Control during startup (low power):	
	1) One of the main reasons that the manual control of feedwater is a demanding task in currently operating PWRs is that the control task is inherently difficult. In addition accurate information on critical process variables (i.e., steam flow and feed flow) is lacking.	1) See Table 1 Item 122.
	2) Number of operators in CR	2) See Table 1 Item 48 and 64.
	3) High noise level in CR	3) See Table 1 Item 99, 100, and 101.
	4) Stress / workload	4) See Table 1 Items 48 and 64.
	5) CR displays: A way to facilitate prediction is to provide displays in the CR that give more accurate indications of the process state information needed for prediction, such as, a) better steam generator level (SGL) information, b) low power feedflow and steam flow indicators and c) predictive displays. Two types of predictive displays are proposed: 1. a predictor which displays SGL with the shrink and swell effects removed and 2. a predictor of the maximum/minimum SGL to be reached (due to shrink/swell) before level turns around.	5) See Table 1 Item 88, 90, 91, and 122. SSAR Section 18.8 includes the Implementation Plan for the HSI Design that addresses the criteria of Element 7 of NUREG-0711. For each HSI, including the Plant Information System (workstation displays), an HFE design guidelines document is developed that provides guidelines to the HSI designers on the conventions, symbols, color coding, and dynamic characteristics to be used in the design of the respective HSI. Issues such as navigation issues will be addressed by the guidelines document. The HSI design plan also includes concept testing and design reviews.
	6) Training	6) Training Program development is the responsibility of the COL applicant as stated in SSAR Section 13.2.
	7) Computer-based procedural aids	7) See Table 1 Item 102 through 109.

References To Table 3, Operator Interview Issues

3.1 Roth, E. M., Mumaw, R. J., and P. M. Lewis, "An Empirical Investigation of Operator Performance in Cognitively Demanding Simulated Emergencies," NUREG/CR-6208, U.S. Nuclear Regulatory Commission, Washington D.C., July, 1994

3.2 Mumaw, R. J., D. Swatzler, E. M. Roth, and W. A. Thomas, "Cognitive Skill Training for Nuclear Power Plant Operation Decision Making," NUREG/CR-6126, U.S. Nuclear Regulatory Commission, Washington D. C., June 1994

3.3 Hoecker, D. G. and E. M. Roth, "Effects of Control Lag and Interaction Mode on Operators' Use of Soft Controls," STC REPORT 94-8SW5-APMMI-R1 (or alternate AP600 document number: OCS-J1-008 Rev A) Westinghouse Proprietary Class 2, September 23, 1994

3.4 Woods, D. D., J. A. Wise, and L. F. Hanes, "Evaluation of Safety Parameter Display Concepts" Westinghouse Report NP-2239 Research Project 891-5, Electric Power Research Institute, Final Report February 1982

3.5 PG&E Letter 225537, "Simultaneous Unit Trip - Human Factors," from P. G. Saraflan to D. B. Miklush, dated 1/17/95

3.6 Mumaw, R. J., Roth, E. M., Vicente, K. J., and Burns, C. M., "A Model of Operator Cognition and Performance During Monitoring in Normal Operations," Westinghouse Report, AECB Project No. 2.376.3, September 1996.

3.7 Roth, E. M., and D. D. Woods, "Improving Skill in Feedwater Control During Startup: Results of an Expert Panel Session," WCAP-11135, Westinghouse Nuclear Services Integration Division, February 1986

3.8 Schaefer, W. F., "Low Power S.G. Water Level Control System Improvements," WCAP-11126, Westinghouse Proprietary Class 2, May 1986