Response to

Request for Additional Information No. 240 (2800), Supplement 1, Revision 0

6/05/2009

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 18 - Human Factors Engineering
Application Section: All

QUESTIONS for Operating Licensing and Human Performance Branch
(AP1000/EPR Projects) (COLP)

Question 18-36:

A conference call took place May 7, 2009 between NRC staff and AREVA NP representatives to discuss the EPR Human Factors Engineering (HFE) program. The staff questioned the relationship between AREVA's previously submitted HFE documents, such as the Inheritance document, and the elements of NUREG-0711. AREVA acknowledged that the Inheritance document had evolved as it was being developed. AREVA committed to submit an implementation plan for each NUREG-0711 element, and additionally committed to develop additional items, such as an HFE program management plan, a staffing and qualifications plan, and a mapping of all implementation plans to the Concept of Operations document.

Please identify the documents to be developed, and provide their delivery schedule.

Please also include a mapping of all planned and previously submitted documents to the NUREG-0711 criteria for HFE.

Response to Question 18-36:

The following implementation plans, described in NUREG 0711 Rev. 2, were provided in the Response to RAI 171, Question 18-34:

- Human System Interface (HSI) Design Implementation Plan.
- Human Factors Engineering (HFE) Design Implementation Plan.
- Verification & Validation Implementation Plan.
- Implementation Plan for the Integration of HRA into the HFE Program.
- Human Performance Monitoring Implementation Plan.
- Operating Experience Review Implementation Plan.
- Function Analysis and Allocation Implementation Plan.

The HSI Design Implementation Plan and HFE Program Management Plan describe the iterative nature of the HFE program.

The Response to RAI 171, Question 18-34 also included the following documents, which do not describe a specific HFE program element from NUREG 0711 Rev. 2:

- Inheritance Implementation Plan.
- Initial Staffing Assumptions for the U.S. EPR.
- Concept of Operations for the U.S. EPR Control Room.

The concept of operations and the initial staffing assumptions are based on typical operating practices used in existing U.S. plants. The concept of operations and staffing assumption will be evaluated and modified throughout the HFE design process based on results from the analysis phase, design phase, verification and validation phase, and implementation phase.

The required elements for staffing and qualification are provided in the U.S. EPR Task Analysis Implementation Plan.

The following documents are enclosed and complete the documents that support the HFE program:

- U.S. EPR Human Factors Procedure Implementation Plan.
- U.S. EPR Human Factors Training Implementation Plan.
- U.S. EPR Task Analysis Implementation Plan.
- U.S. EPR HFE Program Management Plan.

AREVA NP has prepared a matrix that shows the U.S. EPR HFE Program compliance with the Standard Review Plan (SRP) NUREG-0800. Mapping to this matrix is more relevant to the HFE program than mapping to the Concept of Operations for the U.S. EPR Control Room because the concept of operations is a subset of the documents needed for the overall program. The matrix, SRP, Chapter 18, Compliance Document, is also enclosed.

Table 18-36-1 shows the U.S. EPR Human Factors Engineering plans that address NUREG 0711 guidance.

Table 18-36-1—NUREG 0711 Cross Reference

NUREG 0711, Rev. 2	Title
Section 2 – HFE Program Management	HFE Program Management Plan
Section 3 – Operating Experience Review	U.S. EPR Human Factors Operating Experience Review (OER) Implementation Plan
Section 4 – Functional Requirements Analysis and Functional Allocation	U.S. EPR Functional Requirements Analysis and Function Allocation Implementation Plan
Section 5 – Task Analysis	U.S. EPR Task Analysis (TA) Implementation Plan
Section 6 – Staffing and Qualification	U.S. EPR Task Analysis (TA) Implementation Plan
Section 7 – Human Reliability Analysis	U.S. EPR Implementation Plan for the Integration of Human Reliability Analysis (HRA) into the Human Factors Engineering (HFE) Program
Section 8 – Human-System Interface Design	U.S. EPR Human System Interface Design Implementation Plan
Section 9 – Procedure Development	U.S. EPR Human Factors Procedure Implementation Plan
Section 10 – Training Program Development	U.S. EPR Human Factors Training Implementation Plan
Section 11 – Task Analysis	U.S. EPR Human Factors Verification and Validation Implementation Plan
Section 12 – Design Implementation	U.S. EPR Human Factors Engineering (HFE) Design Implementation Plan

U.S. EPR Human Factors Engineering Program Topical Report - ANP-10279 will be retracted by AREVA NP letter NRC: 09:079. Safety determinations for the U.S. EPR are provided in the U.S. EPR HFE Program Management Plan, which is supplemented by the other HFE program documents submitted for review. Topical report RAIs have been reevaluated (as shown in Table 18-36-2) as they now relate to the U.S. EPR HFE Program Management Plan rather than the U.S. EPR Human Factors Engineering Program Topical Report - ANP-10279.

Responses to the RAIs listed in Table 18-36-2 have been evaluated to confirm that they remain valid. Superseded RAIs indicate that the response to that RAI is no longer valid because of the U.S. EPR Human Factors Engineering Program Topical Report retraction and U.S. EPR HFE Program Management Plan changes.

Table 18-36-2—Evaluation of Chapter 18 RAIs

RAI	Response Status
18-1	Applicable
18-2	Superseded
18-3	Applicable
18-4	Superseded[1]
18-5	Applicable[1]
18-6	Applicable[1]
18-7	Superseded[1]
18-8	Applicable[1]
18-9	Applicable
18-10	Applicable[1]
18-11	Applicable
18-12	Applicable
18-13	Superseded[1]
18-14	Applicable
18-15	Applicable[1]
18-16	Applicable
18-17	Applicable
18-18	Applicable[1]
18-19	Applicable
18-20	Applicable[1]
18-21	Applicable[1]
18-22	Applicable[1]
18-23	Applicable[1]
18-24	Applicable
18-25	Applicable[1]
18-26	Applicable
18-27	Applicable[1]
18-28	Applicable[1]
18-29	Applicable
18-30	Applicable
18-31	Applicable[1]
18-32	Superseded[1]
18-33	Applicable[1]

Note:

1. The HFE document referenced in the RAI response has been submitted to the NRC.

Information from other EPR projects will be considered for design input to the U.S. EPR HFE Functional Requirements Analysis, Operating Experience Review, and Task Analysis that will be performed for the U.S. EPR.

U.S. EPR FSAR Tier 2, Chapter 18 will be revised to reflect the changes that have been made to the program based on the U.S. EPR HFE Program Management Plan as supplemented by additional HFE program documents submitted for review.

FSAR Impact:

U.S. EPR FSAR Tier 2, Chapter 18 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

Table 1.6-1—Reports Referenced
Sheet 1 of 4

Report No. (See Notes 1, 2, and 3)	Title	Date Submitted to NRC	FSAR Section Number(s)
ANF-89-060P-A ANF-89-060NP-A Supplement 1	Generic Mechanical Design Report High Thermal Performance Spacer and Intermediate Flow Mixer	3/28/91	4.2
ANP-10263P-A ANP-10263NP-A	Codes and Methods Applicability Report for the U.S. EPR	11/06/07	4, 5.1, 15, 16, and 19
ANP-10264NP-A	U.S. EPR Piping Analysis and Pipe Support Design Topical Report	11/07/08	3.6, 3.7, 3.8, 3.9, 3.10, 3.12, App. 3A, and App. 3C
ANP-10266-A	AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR Topical Report	06/18/07	7.1, 17.1, 17.2, 17.3, 17.5, 18.1, 18.7, and 18.11
ANP-10268P-A ANP-10268NP-A	U.S. EPR Severe Accident Evaluation Topical Report	2/26/08	6.2.5, 15.4, 19.1, and 19.2
ANP-10269P-A ANP-10269NP-A	The ACH-2 CHF Correlation for the U.S. EPR Topical Report	3/10/08	4.4, 5, 7, 15, and 19
ANP-10272	Software Program Manual TELEPERM XS™ Safety Systems Topical Report	12/21/06	7.1 and 7.6
ANP-10273P ANP-10273NP	AV42 Priority Actuation and Control Module Topical Report	11/28/06	7 and 16
ANP-10275P-A ANP-10275NP-A	U.S. EPR Instrument Setpoint Methodology Topical Report	2/26/08	7 and 16
ANP-10278P ANP-10278NP	U.S. EPR Realistic Large Break Loss of Coolant Accident Topical Report	3/26/07	6.2 and 15
~~ANP-10279~~	~~U.S. EPR Human Factors Engineering Program Topical Report~~	~~1/29/07~~	~~3.4, 7.1, 13.1, and 18~~
ANP-10281P ANP-10281NP	U.S. EPR Digital Protection System Topical Report	3/27/07	3.1.3, 4.6, 7, and 8.1
ANP-10282P ANP-10282NP	POWERTRAX/E Online Core Monitoring Software for the U.S. EPR Technical Report	11/27/07	4.4
ANP-10283P, Revision 1 ANP-10283NP, Revision 1	U.S. EPR Pressure-Temperature Limits Methodology for RCS Heat-Up and Cool-Down Technical Report	4/30/09	5.3 and 16
~~ANP-10284~~	~~U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology Topical Report~~	~~6/20/07~~	~~7~~

18-36

Table 1.9-2—U.S. EPR Conformance with Regulatory Guides
Sheet 8 of 18

RG / Rev	Description	U.S. EPR Assessment	FSAR Section(s)
1.97, R4	Criteria For Accident Monitoring Instrumentation For Nuclear Power Plants	Y	3.10
			3.11.2
			7.1
			7.5
			11.5
			12.3
			16.B3.3
			18.7
1.98, 03/1976	Assumptions Used for Evaluating the Potential Radiological Consequences of a Radioactive Offgas System Failure in a Boiling Water Reactor	N/A-BWR	N/A
1.99, R2	Radiation Embrittlement of Reactor Vessel Materials	Y	5.3.1
			5.3.2
1.100, R2	Seismic Qualification of Electric and Mechanical Equipment for Nuclear Power Plants	Y	3.10
			3.11
			App 3D, Att. E
1.101, R5	Emergency Planning and Preparedness for Nuclear Power Reactors	N/A-COL	N/A
1.102, R1	Flood Protection for Nuclear Power Plants	Y	3.4
1.105, R3	Setpoints for Safety-Related Instrumentation	Y	15.1
			15.2
			15.3
			15.4
		Y ~~(Per AREVA Topical Report ANP-10279)~~	18.7
		EXCEPTION (As addressed in AREVA Topical Report ANP-10275P)	7.1.2.4.7
1.106, R1	Thermal Overload Protection for Electric Motors on Motor-Operated Valves	Y	8.3.1.1

18-36

Table 1.9-4—U.S. EPR Conformance with Advanced and Evolutionary Light-Water Reactor Design Issues (SECY-93-087)
Sheet 5 of 5

Issue	Description	U.S. EPR Assessment	FSAR Section(s)
III.E	Control Room Habitability Position on appropriate analytical methods (i.e., dose limits and accident duration) to be used in determining the acceptability criteria for control room habitably in accordance with regulatory standards.	Y	15.0.3
III.F	Radionuclide Attenuation: Position on fission product removal processes inside containment by natural effects and holdup by the secondary building and piping systems in addition to commission position on containment spray systems for passive ALWRs.	Y	6.5.5 15.0.3
III.G	Simplification of Offsite Emergency Planning: Position on simplifying off-site emergency planning of passive designs due to the estimated low probability of core damage of such designs.	N/A-PAS	N/A
III.H	Role of the Passive Plant Control Room Operator: Commission position on sufficient man-in-the-loop testing and evaluation be performed and that a fully functional integrated control room prototype is necessary for passive plant control room designs to demonstrate that functions and tasks are integrated properly into the man/machine interface decisions.	18-36 Y ~~(Per AREVA Topical Report ANP-10279)~~	18.2 18.3 18.7

13.0 Conduct of Operations

Conduct of operations provides information relating to the preparations and plans for design, construction, and operation of the U.S. EPR. Conduct of operations provides adequate assurance that a plant will establish and maintain a staff of adequate size and technical competence and that operating plans are adequate to protect public health and safety.

13.1 Organizational Structure of Applicant

A COL applicant that references the U.S. EPR design certification will provide site-specific information for management, technical support and operating organizations. The operating organization describes the structure, functions and responsibilities established to operate and maintain the plant. Additional information for a COL applicant to develop an operating organization is provided in Chapter 18~~ and in ANP-10279NP, "U.S. EPR Human Factors Engineering Program Topical Report" (Reference 1)~~.

18-36

Next File

13.8 References

18-36

1. DELETED~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc., January 2007.~~

2. NUREG-0654/FEMA REP-1, "Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants," Revision 1, U.S. Nuclear Regulatory Commission, November 1980.

3. Letter from Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), "U.S. EPR Vital Equipment List (Safeguards Information)," dated November 30, 2007.

4. Letter OG-1789, Tony Stallard, Chariman, B&WOG Operator Support Committee, to Chief, Reactor Systems Branch (NRC), "Transmittal of B&W Owners Group Emergency Operating Procedures Technical Bases Document, Revision 9," dated April 26, 2000 and attachments (ML003711891).

5. Letter from Richards, Stuart A. (NRC) to Kelly, Michael, Chairman, B&W Owners Group Operator Support Committee, "Completion of Review of the Babcock and Wilcox Emergency Operating Procedures Guidelines (TAC No. M54946)," with attachment, dated November 5, 1999.

6. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S. Nuclear Regulatory Commission, February 2004.

7. NUREG-0737, "Clarification of TMI Action Plan Requirements," U.S. Nuclear Regulatory Commission, November 1980.

8. NUREG-0737, "Clarification of TMI Action Plan Requirements: Supplement 1," U.S. Nuclear Regulatory Commission, January 1983.

9. ANS 3.2-1994, "Administrative Controls and Quality Assurance for the Operational Phase of NPPs," American Nuclear Society, 1994.

10. NUREG-0800, "Standard Review Plan", Section 13.5.2.1, "Operating and Emergency Operating Procedures, Appendix A, Review Procedures for the Evaluation of Procedures Generation Packages," Revision 2, U.S. Nuclear Regulatory Commission, March 2007.

11. NUREG-1358, "Lessons Learned from the Special Inspection Program for Emergency Operating Procedures," Supplement 1, U.S. Nuclear Regulatory Commission, 1992.

12. NUREG-1358, "Lessons Learned From the Special Inspection Program for Emergency Operating Procedures," U.S. Nuclear Regulatory Commission, April 1989.

13. NUREG-0899, "Guidelines for the Preparation of Emergency Operating Procedures," U.S. Nuclear Regulatory Commission, August 1982.

3. For the U.S. EPR, the SICS platform concept involves extensive use of the qualified display system (QDS)—a series of touch-screen capable, seismically qualified, 1E supplied visual display units (VDU). The QDS is an AREVA NP product and development activities have been identified for the QDS to support these needs. Because the QDS will replace many conventional indications and controls and to maintain divisional separation requirements, each control QDS is assigned to manage a respective electrical division or mechanical train. ~~This design creates potential additional burden on the operator when the SICS is used to monitor and control the plant.~~

18-36

4. To minimize differences between HMI platforms in the control rooms, local control stations (LCS) which allow for communication with computer-based HMIs (e.g., turbine-generator and emergency diesel generator controls) will be integrated with the PICS. ~~As discussed in section 2.1.1 of ANP-10279 (Reference 2),~~ LCSs will follow guidelines established by the HFE and Control Room Design Team.

Other assumptions and constraints related to standard features of EPR control rooms, HSI design operating philosophy, and the concept of operations are described in Section 18.7.2 of this FSAR and in Section~~s 3 and 4~~2.2 of Reference 2.

The U.S. EPR HFE design process addresses the applicable review criteria specified in NUREG-0711 (Reference 1).

18.1.1.3 Applicable U.S. EPR Facilities

The HFE program scope includes the design of the MCR, the Technical Support Center (TSC), and the remote shutdown station (RSS). The design of LCSs is typically accomplished concurrent with the applicable system and follows guidelines established by the HFE and Control Room Design Team (see Section 18.1.2). In addition, the Instrumentation and Control Service Center (I&CSC), the central location for maintaining the digital I&C systems for the plant, is included in the application of the HFE program. A COL applicant that references the U.S. EPR design certification will be responsible for HFE design implementation for a new emergency operations facility (EOF) or changes resulting from the addition of the U.S. EPR to an existing EOF. The HFE and Control Room Design Team provides guidance to that design. Execution of the HFE program guidance described herein provides reasonable assurance that HFE principles are both comprehensively and properly applied for the design of the EOF. This HFE guidance also provides a level of consistency for all HSI facilities in the U.S. EPR.

18.1.1.4 Applicable Human System Interfaces, Procedures, and Training

The scope of the HFE program includes HSIs, procedures, and training associated with monitoring and controlling U.S. EPR plant processes and equipment through the system functions. These system functions include those required during the various normal operating modes as well as those required during tests, inspections,

surveillances, and maintenance, and during abnormal, emergency, and accident conditions. HSIs associated with non-I&C systems (e.g., manual valve operators and other LCSs) follow guidelines established by the HFE and Control Room Design Team. See Section 18.1.3.2 for information on implementation of these guidelines.

HSIs for the U.S. EPR design are implemented in the following hardware and software with the following I&C systems:

- Process Information and Control System (PICS).
- Safety Information and Control System (SICS).
- LCSs.

Details of the design and the concept of operations associated with each of these HSIs can be found in Section 18.7 and associated references.

The U.S. EPR HFE program also includes the application of appropriate HFE ~~principals~~principles and techniques to support the development of operating procedures for the applicable interfacing facilities (see Section 18.1.1.3) and the operator training program. A generic set of operational guidelines (i.e., not specific to owner and site requirements or constraints), for the U.S. EPR, is provided for use in the development of site-specific operating procedures. The requisite set of knowledge, skills, ~~and~~ attributes, and training objectives and goals required to operate a U.S. EPR are also provided for use in the development of a site-specific training program based on the Systematic Approach to Training (SAT) development protocol accredited by INPO. The training program and procedure development program are described in Sections 18.9 and 18.8, respectively.

18-36

18.1.1.5 Applicable Plant Personnel

The HFE program is tailored allowing licensed control room operators the capability to attain, view, assimilate, and act on process data in order to maintain plant safety. HFE principles are also applied to the tasks which relate to plant safety that are performed by personnel as listed.

Plant personnel addressed by the AREVA NP HFE program include licensed control room operators as defined in 10 CFR 55 and the following categories of personnel defined by 10 CFR 50.120.

- Non-licensed operators.
- Shift ~~supervisor~~manager.
- Shift technical advisor.
- Instrument and control technicians.

18-36

- Electrical maintenance personnel.
- Mechanical maintenance personnel.
- Radiological protection technicians.
- Chemistry technicians.
- Engineering support personnel.

18.1.1.6 Effects of Modifications on Personnel Performance

The HFE program applies to the equipment supplied for the original configuration of the U.S. EPR. Modifications to the original interface configuration are required to adhere to the guidelines of Reference 1. Adverse effects caused by modifications on the overall system performance and the performance of personnel who use the equipment are minimized as described in Reference 1 and RG 1.174. Throughout the life of the plant, HFE issues resulting from plant modifications are documented and dispositioned as described in Section 18.12 and the human performance monitoring implementation plan (Reference 3).

18.1.2 Human Factors Engineering and Control Room Design Team Organization

The HFE and Control Room Design Team is the multi-disciplinary team responsible for implementing the HFE program. The HFE and Control Room Design Team is responsible for overseeing certain aspects of the design and construction of the nuclear facility in accordance with 10 CFR 50.34(f)(3)(vii), as described in SRP Section 13.1.1, Management and Technical Support Organization. A description of the responsibilities, organizational placement and authority, and composition and qualifications of the HFE and Control Room Design Team is provided in Section ~~5.4.2.1~~3.0 of the ~~Human Factors Topical Report~~U.S. EPR HFE Program Management Plan (Reference 2).

18-36

The HFE and Control Room Design Team is guided by the HFE program described herein for the proper development, execution, oversight, and documentation. The HFE and Control Room Design Team follows the same design processes as other engineering disciplines and is accountable for the quality of the HSI and control room layout to meet the requirements of the AREVA QAP Topical Report (Reference 3).

18.1.3 Human Factors Engineering Processes and Procedures

The HFE and control room design is performed in accordance with the U.S. EPR QAP described in Reference 3. As described in Section ~~5.1~~4.0 of the U.S. EPR HFE Program Management Plan (Reference 2), the AREVA NP generic design control process~~, as described in Section 5.1 of Reference 2,~~ is used to execute the HFE and control room

applicable implementation plans or output reports for the various analyses or design activities. ~~Appendix A of Reference 2 provides a summary and schedule of the documentation associated with the HFE program elements.~~

18-36

The U.S. EPR design process requires cross-discipline reviews of design documentation for systems, structures, or components. System interface documents are produced by system discipline engineers to facilitate communication between disciplines for systems, structures, or components that have boundaries encompassing several engineering disciplines. The design documentation for complex systems is generally rolled up into a governing document (i.e., system description) controlled by the lead discipline engineer. Similarly, the HSI engineering activities are integrated into the overall plant design by use of the cross-discipline review concept and system interface documentation.

18.1.3.3 HFE Program Milestones

HFE milestones are identified to allow evaluations of the effectiveness of the HFE effort to be made at critical checkpoints. Section 18.1.5 also shows the relationship to the integrated plant design sequence. A relative program schedule of HFE tasks showing relationships between HFE elements and activities, products, and reviews and identifying HFE program milestones to allow evaluations of the effectiveness of the HFE effort to be made at critical checkpoints is shown in Figure 18.1-1—HFE Program Milestones.

18.1.3.4 HFE Documentation

Documentation of the HFE and control room design is addressed by procedures that apply to U.S. EPR design activities. The applicable procedures establish requirements, methods, and responsibilities for preparing, reviewing, and approving initial design documents as well as for changing previously released documentation. Section ~~5.3~~4.5 of the U.S. EPR HFE Program Management Plan (Reference 2) provides a discussion of the types of document prepared for HFE design and their usage.

18-36

System descriptions for control rooms and for HSI platforms contain the bases for how design requirements are met; this includes HFE-related design requirements. The documentation of the HFE and control room design is included in the system descriptions, equipment specifications, and implementation plans for the various analyses, or in reports generated as a result of the analyses. ~~Appendix A of Reference 2 provides a summary and schedule of the documentation associated with the HFE program elements.~~

18.1.3.5 Subcontractor HFE Efforts

Subcontractors for the HFE portions of the U.S. EPR design are subject to the requirements of the U.S. EPR QAP described in Reference 3. The QAP identifies the

procedures that apply to subcontractor design organizations. Effective implementation of a subcontract supplier organization QAP is monitored by respective internal audit programs and by individual supplier audits.

18.1.4 Human Factors Engineering Issues Tracking

Section ~~5.5~~5.0 of the U.S. EPR HFE Program Management Plan (Reference 2) describes the method used to track HFE issues throughout the life of the design.

18-36

HFE issues are tracked in a standard corrective action program database and are generated, verified, and implemented as described in Section 16 of Reference 3.

18.1.5 Technical Program

As described in the U.S. EPR HFE Program Management Plan ~~Section 5.3 of~~ (Reference 2), the HFE and control room design program is performed in accordance with the process specified in Reference 1. Figure 18.1-2—HFE Design Control Process illustrates the design control process and how the HFE implementation plans, analyses, and evaluations required as part of the program fit the overall process flow.

18.1.5.1 HFE Program Process Drawing

Figure 18.1-2 illustrates how the HFE aspects of the plant are developed, designed, and evaluated on the basis of a structured analysis using accepted HFE principles. It shows the relationships between:

- The implementation plans for the various analysis and validation activities.
- The HFE design guidelines and the design products.
- ~~The specific design records and output reports or summaries used to document the design.~~

In conjunction withthe U.S. EPR HFE Program Management Plan (Reference 2) and Section 18.1 of this FSAR, Figure 18.1-2 illustrates that the HFE and Control Room Design Team is guided by a plan that is properly developed, executed, overseen, and documented. Specific elements of Figure 18.1-2 include:

18-36

- ~~The U.S. EPR design stages (i.e., conceptual, basic, detailed, and construction).~~
- ~~The four HFE program general activities (Figure 1.1 of Reference 1).~~
- The relationship between the different HFE program elements.
- The input and output documents.
- A general sequence for the different HFE elements.

- ~~The relationship between HFE and other EPR design disciplines.~~
- ~~The relationship between HFE and COL applicant.~~

18-36

~~The U.S. EPR HFE design is based on predecessor designs and is revised to accommodate regulatory requirements, industry HFE codes and standards, and customer requirements. The revised predecessor design is used to design a state-of-the-art HFE program which is iterated as the EPR plant design matures. The HFE program culminates in a design which is verified and validated by acceptable HFE methods.~~

18.1.5.1.1 U.S. EPR Design Phases

The ~~background shading in Figure 18.1-2 illustrates how the~~ U.S. EPR design occurs in four design phases. The milestone schedule shown in Figure 18.1-1 is developed with an understanding of the relationship between design phases.

The conceptual design phase consists of producing high level descriptions (e.g., program plans and the plant technical requirements) and system engineering tasks (e.g., such as design requirements and system descriptions). Initial HSI and control room layout designs are developed during this phase. In the U.S. EPR HFE Program Management Plan (Reference 2), conceptual design phase activities are described in Sections ~~5.3.1 through 5.3.4~~ 4.5.

As described in Section ~~5.3.5~~4.5.8 of the U.S. EPR HFE Program Management Plan (Reference 2), the basic design phase includes preparation of design specifications to support ordering equipment. The HSI and control room layout designs are iterated with the initial input from procedure developers and the training specialists during this phase.

18-36

The detailed design phase involves performing design support and configuration measures. Support measures such as calculations, selection and suitability reviews, and design reviews (as described in Section 4.5.1 of the U.S. EPR HFE Program Management Plan (Reference 2)) are used to validate the design and maintain or manage the design configuration. ~~Certain~~ HFE ~~verification~~design evaluation ~~and validation (V&V)~~ activities are conducted throughout basic and detailed design~~, but summary reports for V&V and other HFE program activities are produced late in the detailed design phase.~~ Verification and validation (V&V) activities are performed after the iterative design/evaluation process in order to develop a design that meets requirements.

The construction and operation phase involves acceptance testing before and after installation, verifying configuration management for design documentation (see Section 18.11), and monitoring system and operator performance throughout the life of the plant (see Section 18.12).

18.1.5.1.2 HFE Program General Activities

The four HFE program general activities (see Figure 1.1 of Reference 1) categorize the twelve HFE program elements. These four general activities roughly coincide with U.S. EPR HFE design phases (see Section 18.1.5.1.1). There is significant overlap between general activities and the HFE design process, which often requires iteration or feedback to activities conducted earlier in the sequence.

HFE activities in planning and analysis are a subset of the conceptual design phase. During planning and analysis, the HFE and Control Room Design Team:

- Studies the details of the predecessor plant designs and compares them against the applicable industry codes, standards, regulatory requirements, and customer requirements.
- Conducts analysis of operating experience and formulates the concept of operations including initial staffing and qualification analyses.
- Writes implementation plans for the applicable HFE program activities.
- ~~Determines the applicability of analysis activities conducted on predecessor designs and the best means to convert those analyses into HSI design input.~~ 18-36
- Completes initial design documentation (i.e., design requirements and system descriptions for control rooms and HSIs).

As in the basic design phase, HFE design activities involve iteration of the HSI based on input from other elements such as procedure development and analysis activities.

During the HFE V&V program activity (coincides with detailed design phase), the HSI and control room design is substantiated (see Section 18.10). Changes may cause revisions in the functions and documentation that were completed during the planning and analysis or design stages.

The implementation and operation activity coincides with the construction and operation phase. Changes to the design at this phase may cause re-engineering and revision of documentation produced in any of the previous stages.

18.1.5.2 Relationship Between HFE and Other Engineering Disciplines

Reference 3 requires that the HFE and Control Room Design Team follow the same design processes as other engineering disciplines. Section ~~5~~4.0 of the U.S. EPR HFE Program Management Plan (Reference 2) describes the relationship between HFE program design documentation and general design documentation. 18-36

18.1.5.3 HFE Program Element Documentation

The U.S. EPR HFE program is described in Section 18.1. Section ~~2.2~~2.0 of the U.S. EPR HFE Program Management Plan (Reference 2) describes the general HFE requirements, standards, and specifications utilized in the design of the U.S. EPR. Section 18.10 of this FSAR and Section ~~6.0~~6.3 of the U.S. EPR HFE Program Management Plan (Reference 2) describe the uses of HFE facilities such as mockups and simulators as well as methods and tools employed for the various testing and validation techniques.

Sections 18.2 through 18.12 provide information on the types of documents generated as part of the U.S. EPR HFE program.

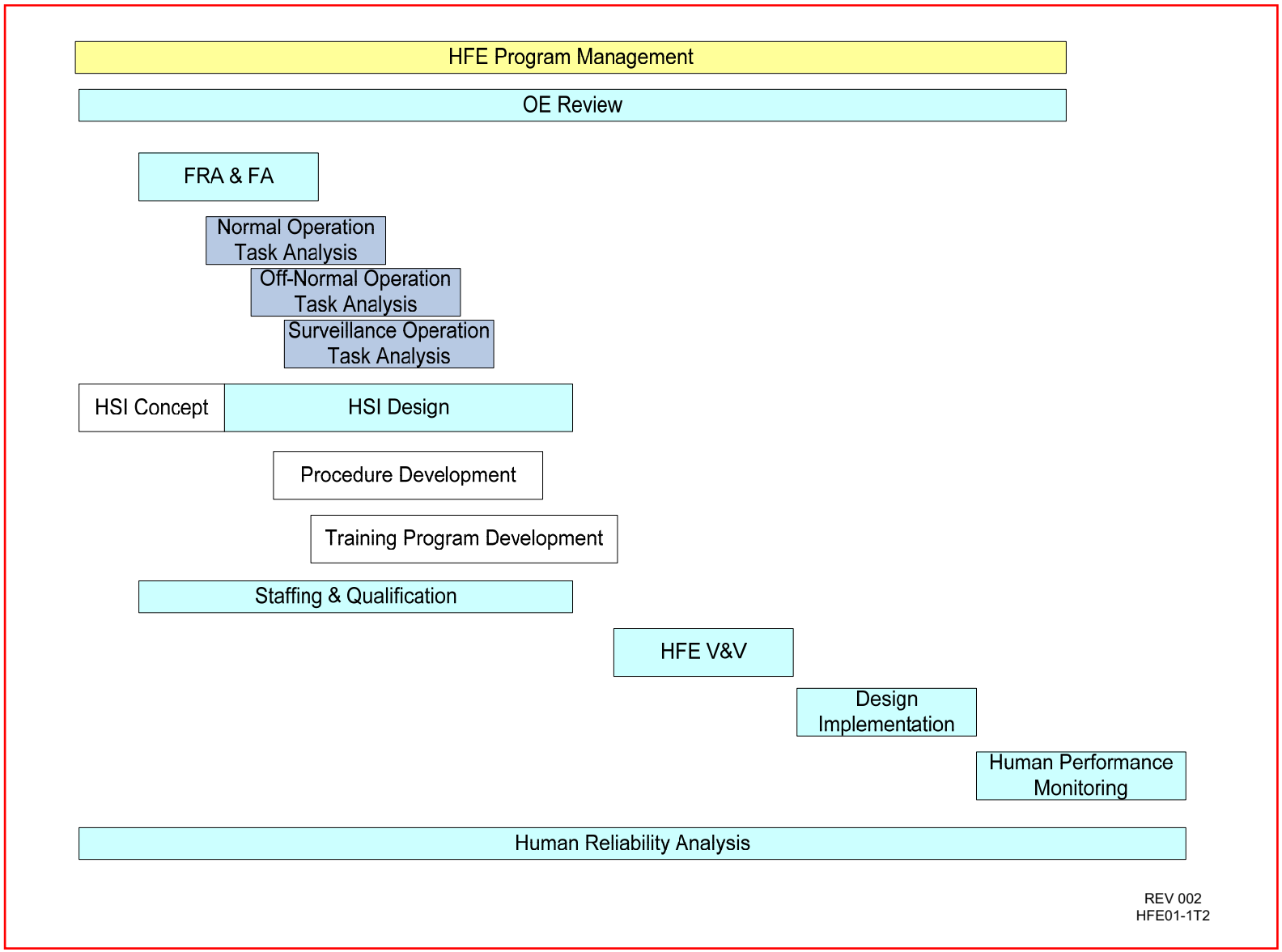
18-36

18.1.6 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S. Nuclear Regulatory Commission, 2004.
2. ~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program Topical Report," AREVA NP Inc., January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.
3. ANP-10266-A, Revision 1, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR," AREVA NP Inc., June 2007.

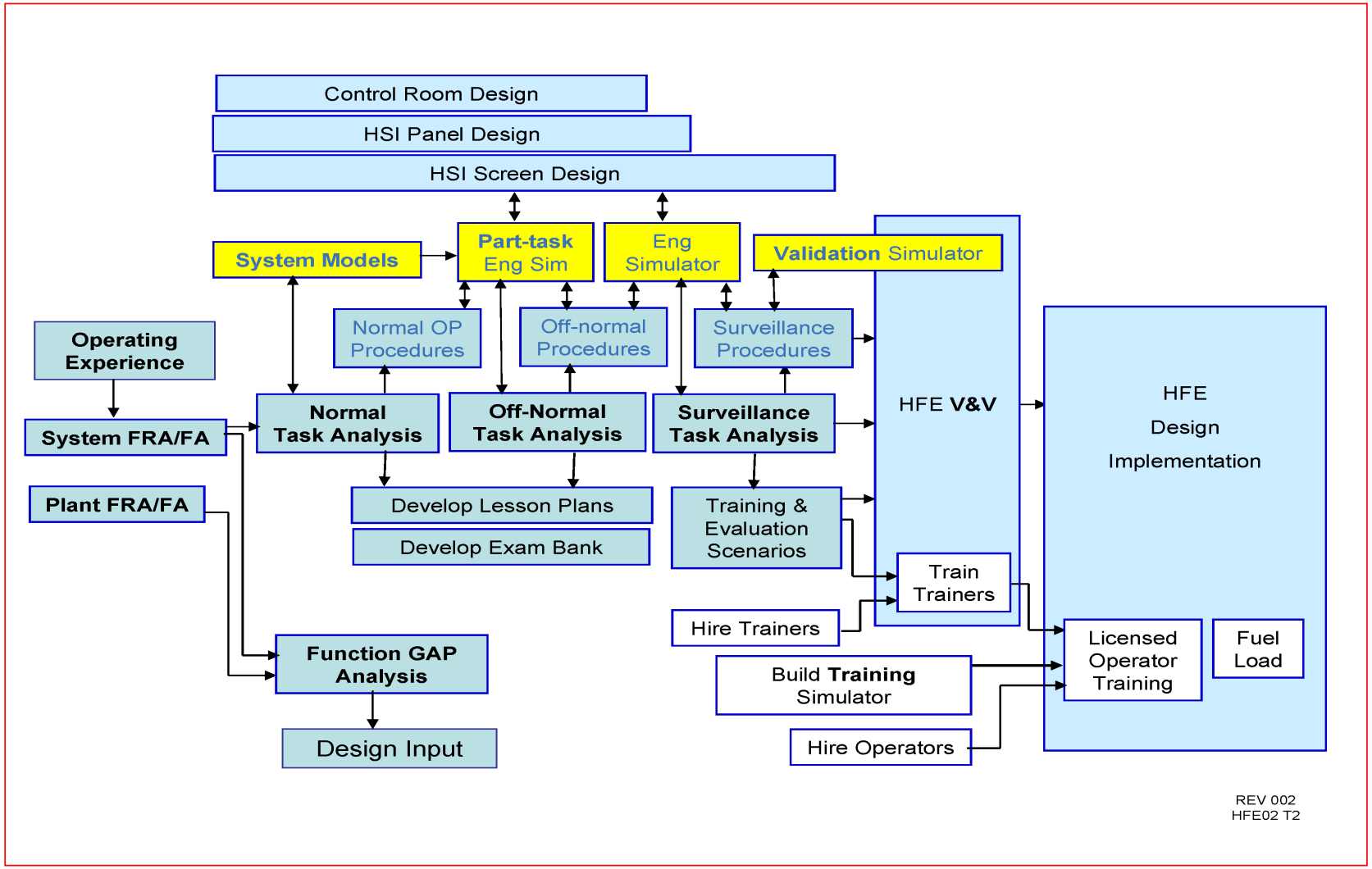
18-36

Figure 18.1-1—HFE Program Milestones



18-36

Figure 18.1-2—HFE Design Control Process



Next File

18.2 Operating Experience Review

Operating experience review (OER) associated with HFE identifies HSI design issues that affect safety. The OER identifies past performance information for predecessor designs (i.e., earlier designs on which the new design is based). The issues and lessons learned from operating experience provide a basis for improving the plant design at the beginning of, and during the design process.

18-36

18.2.1 Objectives and Scope

The OER identifies problems and issues with the HSI. Evaluation and control of the HSI design is promoted when the problems are resolved; operator errors are also reduced. The OER output demonstrates that HFE-related problems and issues in previous designs that are similar to the current design have been identified and analyzed. In this way, negative features associated with predecessor designs are avoided in the current design while retaining the positive features. The OER addresses the predecessor systems of which the design is based, selected technological approaches (e.g., if touch-screen interfaces are planned, associated HFE issues are reviewed), and HFE issues (e.g., generic safety issues defined by the NRC) of the plant.

18.2.2 Methodology

Section ~~5.4.3~~3.0 of Reference 1 describes the process for evaluating operating, design, and construction experience. ~~An~~The OER implementation plan (Reference 1) provides further details, including:

- Sources and means of collecting data.
- Review area focus:
  - Predecessor / related plants and systems.
  - Recognized industry HFE issues.
  - Related HFE technology.
  - Issues identified by plant personnel (including interview topics, questions, and results).
  - Risk-important human actions.
- Information screening.

18-36

- OE Analysis.
- Tracking and maintaining appropriate information.
- Incorporation or utilization of issues by the appropriate design organization.

The multi-disciplinary composition, qualifications and experience level of the HFE and Control Room Design Team provides reasonable assurance that operating experience and the results of research relevant to safety are identified, reviewed and analyzed and that the lessons learned are incorporated into the HSI design.

18.2.3 Evaluation of Results

After an OER issue has been entered into the appropriate tracking database, it is evaluated by a cognizant human factors engineer for applicability. The evaluation includes determining if any lessons learned from the issue have already been incorporated into the design.

Upon completion of the evaluation, the human factors engineer updates the tracking database with appropriate information. Each issue that results in a design change will follow the design change process described in Section ~~5~~4.5.1 of the Human Factors Engineering Program Management Plan ~~Reference 1~~(Reference 2). When the issue has been incorporated into the design, it is closed out in the tracking database. The resolution will remain available for engineers to view.

18-36

OER results are a summary of the data captured and analyzed in the tracking database and the source materials that were evaluated using the methodology described in the implementation plan. The results summary also includes information on how selected issues were captured, maintained, evaluated, and incorporated in the final design.

18.2.4 References

1. ~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc., January 2007.~~Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.

2. Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

Next File

18.3 Functional Requirements Analysis and Function Allocation

Functional requirements analysis (FRA) is the identification and analysis of functions that must be performed in accordance with NUREG-0711 (Reference 1) to satisfy plant safety objectives (i.e., to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public).

Functional allocation (FA) is the analysis of the requirements for plant control and the assignment of control functions in accordance with References 1 and NUREG-0800 (Reference 2) for the following:

- Personnel (e.g., manual control).
- System elements (e.g., automatic control and passive, self-controlling phenomena).
- Combinations of personnel and system elements (e.g., shared control and automatic systems with manual backup).

18.3.1 Objectives and Scope

The purpose of the FRA and FA is to verify that plant safety functions have been defined and that the allocation of those functions to human and system resources has resulted in a role for personnel that takes advantage of human strengths and avoids human limitations (References 1 and 2).

All functions are considered in-scope in that they need to be captured and allocated. Particular significance is placed on functions that satisfy safety objectives (i.e., critical safety functions, as defined by NUREG-0696 (Reference 4)). Section 18.10 describes how procedure verification and validation (V&V) includes an explicit identification of functions to be performed to achieve plant safety objectives.

18.3.2 Functional Requirement Analysis Methodology and Results Summary

18-36

~~The U.S. EPR is an evolutionary PWR design based on years of operation and design experience from the precursor PWR plants (i.e., based on European N4 and Konvoi plants which are in turn based upon Westinghouse-designed PWRs currently operating in the U.S). The U.S. EPR also uses similar control of system functions and instrumentation and control (I&C) concepts as the predecessor PWRs and the Olkiluoto 3 (OL3) EPR.~~

~~Because the U.S. EPR evolved from previous PWR designs, the underlying nuclear and thermodynamic processes and most individual component functions for the U.S. EPR are inherited from the predecessor designs. During the early plant design stages for the OL3 EPR, process functions and their resulting functional requirements were derived from traditional PWR design principles established at the overall plant concept level. For screen-based human system interfaces (HSIs), functional~~

18-36

~~requirements are essentially translated into HSI controls and indications (i.e., screen elements). For the HSIs, applicable conceptual design inputs included:~~

- ~~Concept of operations including the composition, the role of the operating staff, and the role of the control rooms.~~
- ~~Definition of the automation criteria.~~
- ~~Information needs and controls.~~

~~Descriptions of these design inputs are found in ANP-10279NP (Reference 3). HSI design principles, described in Section 18.7.6.1, are used to translate HSI design inputs into the HSI design.~~

~~The OL3 system engineers identified functions and their requirements in the (physical) system design documentation. The design control process procedures governed the detail required for identifying functional requirements. Those requirements initially included, as a minimum:~~

- ~~Safety and design requirements.~~
- ~~Role of the system.~~
- ~~Functions of the system.~~
- ~~Performance data (e.g., capacity, flow).~~
- ~~Interfaces to other systems.~~
- ~~I&C functions used to perform automatic safety functions.~~
- ~~Principle requirements for operation from the main control room (MCR), from the remote shutdown station (RSS), or from a local control station (LCS).~~

~~Initial functional requirements were documented in system descriptions and used to develop successive levels of detail. OL3 system descriptions have organization and content similar to the system description documents developed for the U.S. EPR (see Section 5.3.4 of Reference 3). In order to complete OL3 system design documentation, system engineers performed FRA as they developed and translated the requirements for system performance into requirements for component or functional performance. This OL3 FRA included:~~

- ~~Identification of operating modes:~~
  - ~~Preparation and startup of the system.~~
  - ~~Operation in the various plant states.~~

18-36

- Switchover between operating modes, as applicable.
- Periodic testing, if applicable.
- Shutdown.
- Fault conditions requiring automatic or operator response.

- Identification of:
  - Time criticalities, if any.
  - Parallel functions.
  - Availability of cues indicating the need to perform the task.
  - Availability of cues indicating successful completion of the task.
- Decisions on non-local control of components (e.g., motors, valves) via I&C (manual local operation is adequate if the component is only operated for preparation of startup under non-time-critical conditions or for maintenance such as isolation of sub-circuits).
- Analysis of the variables and check-back signals needed for:
  - Monitoring the operating conditions.
  - Controlling the process variables.
  - Monitoring the availability of the system.
  - Performing tests.
  - Trouble-shooting (diagnostics; evaluation of fault consequences).

Requirements for the design of the HSIs (including those for operation, maintenance, and testing) and for the associated work conditions were then derived from the characteristics of the identified tasks.

For the U.S. EPR, the functional requirements are translated from the OL3 system descriptions into the U.S. EPR system description documents taking into account changes in design principles and design requirements between the two EPR designs. Similarities between the U.S. EPR design and predecessor plants having extensive and successful operating histories provide a valid point of reference for evaluating changes and improvements to functional requirements. The U.S. EPR system description documents also provide the following:

- Safety classification of the function (including indicating critical safety functions).

18-36

- ~~Design basis for the function.~~
- ~~Plant modes or conditions when the function is required to be operable.~~
- ~~Signals and corresponding actuators used to perform the function.~~
- ~~Applicable setpoints for the function.~~

FRA is divided into plant functions and system functions as described in the FRA/FA implementation plan (Reference 3). The plant-level FRA (PFRA) starts with plant-level safety (and power generation goals), continues to safety functions (and power generating functions), and ends with defined system functions. The system-level FRA (SFRA) begins with system functions, continues to train/subsystem functions and ends with component functions and support requirements. Both PFRA and SFRA consider system interdependence, interaction, diversity, and defense-in-depth. The plant-level and system-level FRA can be performed concurrently.

PFRA and SFRA are reconciled into a unified FRA by system function gap analysis (SFGA). During this process, system functions generated independently by PFRA and SFRA are mapped to one another. The functional relationships between plant functions and system functions are then reconciled. The output of SFGA confirms that plant design goals are met by incorporating the differences as design inputs.

Critical safety functions are allocated to systems as guided by generic design criteria. Plant systems configurations or success paths that are responsible for or capable of carrying out the function are defined for all Technical Specification modes. The functional composition addresses the following levels:

- Plant safety functions (maintain fission product barriers).
- Critical safety functions (maintain reactor coolant inventory).
- System functions (control reactivity with boron/control rods).
- Specific plant sub-systems, structures, and components (in-containment refueling water storage tank (IRWST)).

Plant-level function description and mapping include:

- Purpose of the function.
- Conditions that indicate that the function can or should be initiated (loss of subcooling).
- Parameters that confirm system functions (e.g., flow, valve position, pump status).
- Parameters that confirm plant-level functions (e.g., reactor vessel level, core exit temperature).

18-36

- Parameters that indicate that functions can or should be terminated.
- Function diversity.
- Defense-in-depth in safety-related systems.

Plant system and component function description mapping include:

- System design document coordination.
- Review of system functions needed to perform high level goals.
- Parameters required to initiate, monitor, and terminate functions of that system.
- Disclosure of requirements to enable functions.
- Account of conditions that system functions need.
- Evaluation of all mode dependencies.

Plant function documentation is reviewed through the completion of the functional analysis, which includes operating modes as documented in Chapter 16. PRA and HRA analysis combined with OE documentation is used in various steps of the process. Updates and additions to the FRA are implemented during task analysis through the same process.

The FRA report included with the U.S. EPR V&V documentation lists the functions that were considered in-scope for meeting plant safety objectives. The FRA report also includes details of the differences between functional requirements for the predecessor ~~OL3~~ EPRs and the U.S. EPR for the 'safety functions', as well as the technical justification and design basis for each difference.

~~Functional requirements are maintained within the system description documents over the life of the plant as input to modification activities.~~

18.3.3 Functional Allocation Methodology and Results Summary

In the U.S. EPR design process, control of plant process functions is assigned and allocated to humans, automation, or a combination of human and automation using 18-36 ~~the~~a set of automation criteria ~~shown in Section 5.4.4.3 of Reference 3 and in the FA implementation plan~~. U.S. EPR plant process functions and certain control functions are allocated to closed-loop automatic control based on these automation criteria. Generally, functions automated in predecessor PWRs and in the OL3 EPR design are automated in the U.S. EPR design. Functions that are not automated are assigned to operators, either in the MCR or at LCSs. Any changes in automation are weighed against the total responsibilities of the operator to monitor automatic functions and to assume manual control during an automation system failure.

Next File

In addition to tabularizing system and component functions, each applicable system description document lists the type of control to which that function is allocated and the design basis for the allocation. A description of the personnel role with respect to functions and interfacing with automation is provided in the HFE Program Management Plan (Reference 5) concept of operations (see Section 18.7.2).

A specific objective of the V&V is to ~~verify~~validate that the automation design decisions have resulted in an interface that permits accomplishment of the safety functions within human capabilities and identifies as human engineering discrepancies (HEDs) any ineffective function allocation observed. This V&V approach verifies that the FA uses human strengths and avoids human limitations (Reference 2).

18-36

The FA report included in the V&V documentation:

- ~~Details the complete set of automation criteria used for the U.S. EPR including the established control hierarchy between automatic and manual actions.~~List of allocated functions for U.S. EPR
- List~~s the functions that are automated for predecessor EPRs and the differences between the predecessors and the U.S. EPR.~~of differences and similarities between predecessor EPR and the U.S. EPR.
- Explains the technical justification for each difference in functional ~~allocation~~automation.

18.3.4 Changes to Functional Analysis or Allocation

As the U.S. EPR design evolves, functions may be re-allocated in an iterative manner in response to developing design specifics, operating experience, and the outcome of analyses and industry research. As described in Section 18.12, changes and modifications to the initial HSI configuration are required to be evaluated for impact to FRA or FA design documentation. The complete set of automation criteria and other design documentation previously described are considered as part of any proposed change or modification.

18.3.5 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S. Nuclear Regulatory Commission, 2004.

2. NUREG-0800, Chapter 18, "Human Factors Engineering," Revision 2, U.S. Nuclear Regulatory Commission, 2004.

18-36

3. ~~ANP-10279P, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc, January 2007~~Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.

4. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, 1981.

18-36

5. Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

18.4 Task Analysis

The functions allocated to plant personnel define their roles and responsibilities; human actions (HA) accomplish these functions. HAs can be further divided into tasks or groups of related activities which have common objectives or goals. Task analysis (TA) identifies requirements for accomplishing these tasks; specifically, for the displays, data processing, controls, and job support aids needed to accomplish tasks. The results of the TA are identified as inputs in many HFE activities in accordance with NUREG-0711 (Reference 1), such as:

- ~~Staffing, qualifications, j~~Job design, and training.
- Human system interface (HSI), procedure, and training program design.
- Defining task support verification and validation criteria.

The scope and methodology for TA for the U.S. EPR are summarized in the ~~Human Factors Topical Report~~U.S. EPR Task Analysis Implementation Plan (Reference 2).

18.4.1 Task Analysis Objectives and Scope

18-36

The objective of the U.S. EPR TA is to identify the specific tasks needed to accomplish the safety significant functions that are allocated to personnel. The TA also identifies the information, control, and support requirements for those tasks. TA is used to develop the inventory of alarms, displays, and controls necessary for operators to perform tasks.

The TA considers a full range of plant operating modes (i.e., startup, normal power, abnormal and emergency operations, as well as transient, low-power, and shutdown conditions) including selected representative and important tasks from the areas of operations, maintenance, test, inspection, and surveillance. The TA also considers HAs that involve monitoring and backup of automatic functions. Risk important HAs are identified via the probabilistic risk assessment (PRA) Level I and II analyses (see Sections 18.6 and Chapter 19). Also included in the scope of the TA are the analyses of tasks with automated critical functions, including monitoring the automated system and executing backup actions if the system fails.

18.4.2 Task Analysis Methodology

~~The U.S. EPR evolved from predecessor plants and utilizes similar control of system functions and instrumentation and control (I&C) concepts. Similarly, U.S. EPR operating procedures evolved from previously developed procedures. Since all safety significant tasks in scope for TA are driven by procedural requirements, developing the operating procedures drives derivation of (i.e., analyzes) the tasks which operators perform to safely operate the plant. Procedure development (refer to Section 18.8) constitutes an analysis of HAs. U.S. EPR operating procedure guidelines are used to~~

18-36

~~identify the set of information and controls necessary for those tasks to be performed by operating personnel. This TA provides initial input to HSI design and is an iterative process as details of procedure requirements and HSI elements evolve. Plant procedures are verified by a qualified team of operators.~~

~~Section 13.5 describes a basic process for developing emergency operating procedures (EOP) for the U.S. EPR. This process involves the following:~~

- ~~Use of a well refined symptom-based approach and guideline structure.~~
- ~~Use of a generic technical basis document to determine gaps between predecessor designs and the U.S. EPR design with respect to addressing how transients are mitigated.~~
- ~~Incorporation of U.S. EPR specific event analyses.~~
- ~~Development of guidance to account for design differences between the U.S. EPR and predecessor designs.~~

~~Normal and abnormal operating, test, inspection, maintenance, surveillance, and alarm response procedures are similarly developed based on those for predecessor designs. Procedure developers determine gaps between predecessor designs and the U.S. EPR design and determine task requirements for specific procedure requirements. This process is conducted in an iterative manner as the level of detail in the design increases.~~

~~Section 18.5 describes the minimum staffing requirement for operators in the U.S. EPR main control room (MCR). Section 18.7 describes the roles and responsibilities of key operating personnel. The collective set of operator roles and responsibilities is input essential to the development of operating procedures. Validation of operating procedures includes a comparison of tasks with the roles and responsibilities of the operator(s) who may perform the task. Discrepancies discovered during validation activities may result in task reassignment or re-design of the HSI (see Section 18.10). As described in Section 18.7, the design of the HSI may be iterated as necessary to support:~~

- ~~Validation of applicable procedures.~~
- ~~Changes to operator roles and workloads.~~
- ~~Reducing the risk significance of certain HAs.~~

TA is performed on functions identified during the FRA/FA process which includes the automatic actions and operator backup to the automation. A sampling process similar to the operational conditional sampling process described in Section 18.10 (verification and validation) is used to select functions subject to TA. The requirements for accomplishing each task are identified, such as the activity sequence,

18-36

task prerequisites, operational limitations on other trains/systems during task performance, as well as information and controls required to initiate, monitor, terminate, and verify task completion, communication requirements, operator skills, operator qualifications, and job support aids needed.

OER, FRA/FA, HRA, and system data provide input into the TA process. The TA Implementation Plan (Reference 2) provides additional detail on the identification and analysis process for tasks.

The output from TA covers system level and plant level functions for normal, abnormal (including emergency and severe accident events), and surveillance and testing activities performed by licensed and non-licensed operators. The system level TA identifies the tasks required to operate systems during each mode of operation.

The plant level TA identifies the strategy required to accomplish the plant safety and power generation goals. System-level tasks are sequenced based on plant-level strategy and functional requirements.

TA includes workload analysis to evaluate the number of crew members and the skills and qualification in the staffing and qualification assumptions against the sets of concurrent tasks required to implement plant-level operating strategies. Workload values are assigned to tasks allocated to each crew member to determine if changes are required to the initial function allocation among:

- Manual, automatic, group control.
- Shift manager, control room supervisor, licensed operator, non-licensed operator and non-operator plant personnel.
- Control room and local control.

If changes are made to the FA, the TA and workload are reassessed to confirm that the staffing and qualification assumptions remain valid.

The TA process is iterative and progressively more detailed. The results are maintained in a data structure which maps the plant safety objectives to individual operator tasks and plant equipment used to accomplish safety-related functions. This data structure facilitates requirement traceability as well as clearly defined outputs for other HFE activities, such as the design of the HSI, the plant operating procedures, and plant personnel training program.

18.4.3 Results Summary

~~The TA is documented in conjunction with the verification and validation (V&V) results summary by validation of operating procedures containing HAs that the PRA found to be risk significant. The results summary also describes how successive~~

Next File

~~iterations of TA for procedure development, the procedures themselves, and training programs result in an HSI design that supports in-scope information, control, and support requirements.~~A summary report is generated describing the scope of TA and implementation details (e.g., qualification of individuals performing analysis, out of process issues, process outputs).

18.4.4 References

18-36

1. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S. Nuclear Regulatory Commission, February 2004.
2. ~~ANP-10279P, "U.S. EPR Human Factors Engineering Program Topical Report," AREVA NP Inc, January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

18.5 Staffing and Qualifications

18-36

~~10 CFR 50.54 (i) through (m) require a minimum number of main control room (MCR) operators to monitor and control the plant at any given time. The roles and responsibilities of the shift supervisor (SS) are delineated separately from the minimum number of MCR operators. Analysis of the human system interface (HSI) design is necessary to determine the task loading and the margin to and propensity for human error with regard to how the plant normally operates for various abnormal or emergency conditions.~~ Initial staffing assumptions are listed in the Human Factors Engineering (HFE) Program Management Plan (Reference 1). Analysis of actual staffing numbers is an iterative process inherent in task analysis. Initial assumptions are reviewed, validated, and modified as necessary following ~~the~~ analyses ~~associated with other elements of the human factors engineering (HFE) program~~.

~~The analysis described in this section serves as input to aid in the development of an adequate staffing plan for the operating crew. A COL applicant that references the U.S. EPR design will confirm that actual staffing levels and qualifications of plant personnel specified in Section 13.1 of the COL application remain bounded by regulatory requirements and results of the staffing and qualifications analysis. This site-specific information shall be based on corporate staffing philosophy, existing site operations, fleet operations, and plant design. Overall plant staffing plans incorporate organizations including operations, maintenance, engineering, licensing, operations support such as radiological protection, instrumentation and controls, chemistry technicians, security personnel, management, and administration.~~

18-36

18.5.1 Objectives and Scope of Analysis

For developing the conceptual design for HSIs, and considering the minimum staffing requirements established in 10 CFR 50.54 (i) through (m), a U.S. EPR design goal is to design the plant and the HSI so that three licensed operators can safely monitor and control the plant from the MCR under all operating conditions, including normal operation, startup, shutdown, abnormal operation, and accidents. Because of the levels of automation inherent in the instrumentation and controls (I&C) architecture, only one licensed operator is needed at the controls during normal power operations. A second licensed operator is required by law to be on shift to provide defense in depth; the second licensed operator is not required to be continuously at the controls. In addition, a senior reactor operator (SRO) licensed control room supervisor shall remain present or readily available at all times in accordance with 10 CFR 50.54 (m). U.S. EPR design input assumptions also require that each operating crew include an SRO licensed ~~SS~~shift manager (SM)~~, a shift technical advisor (STA) (may be combined with the SS position if the requisite qualifications for each position are fulfilled),~~ and a number of non-licensed operators (NLO)~~., and a maintenance crew consisting of a supervisor and technicians from chemistry, radiation protection, I&C, electrical, and mechanical technicians as noted in the U.S. EPR Human Factors Engineering Program~~

18-36

~~Report (Reference 1). Qualification requirements for operations shift personnel are described in Section 13.1.~~

18-36

The objective of the ~~U.S. EPR staffing and qualifications~~ workload analyses is to demonstrate that the HSI design and the number, roles, and responsibilities of the plant operating staff is able to adequately meet the demands of the processes of the plant. The initial assumption for the roles and responsibilities of operators during a full range of operating conditions is documented in Section ~~4.1~~2.2.2.1 of the HFE Program Management Plan (Reference 1). The initial staffing assumption is based on operational experience from the U.S. EPR predecessor designs (i.e., European N4 and Konvoi pressurized water reactor (PWR) designs which are in turn based upon Westinghouse-designed PWRs currently operating in the U.S.). ~~A higher level of automation exists for the U.S. EPR than for the predecessor plants. This higher level of automation supports fewer operators at the controls even considering additional monitoring requirements for added automation features.~~

To obtain an optimum staffing level for the U.S. EPR, factors associated with other elements of the HFE program are considered. For example:

- The operating experience review (OER), Section 18.2, identifies staffing level related aspects of operating plants of similar design under various conditions and operating modes.

- Functional allocation (FA) decisions, Section 18.3, are evaluated to achieve maximized performance without placing excessive demands upon the operators, and to determine the monitoring tasks required of operators when functions are automated.

- Task analysis (TA), Section 18.4, provides input to the MCR staffing levels by including workload analysis as part of the overall TA process. The objective is to verify that the control room HSI adequately supports operator performance. Workload analysis must carefully consider assumed roles and responsibilities and qualification requirements of operators.

- Human reliability analyses (HRA), Section 18.6, provides input to the consideration of staffing levels on plant safety and reliability. In particular, risk-significant or time critical human actions (HA) are examined during the TA to determine the need for reassignment, changes to operator roles, or the need to change the number of operators required.

- The role of the operator is an important consideration in the HSI design process. Section 18.7 addresses the engineering process of optimizing coordinated operator actions such as the demand on operators during the use of control elements and display elements concurrently and the design of effective support.

18-36

- ~~Because the U.S. EPR uses a computer-based procedure system, concurrent use of multiple procedures has an effect on the role of operators and on staffing demand.~~

18.5.2 Staffing and Qualifications Analysis Methodology

To obtain an optimum staffing level, the initial staffing assumption (Reference 1) may be iterated as a result of task analysis. ~~the other HFE analyses as previously described. The objectives of the staffing analysis are specifically tied to the development of procedures and the associated TA.~~ Initially, tasks are assigned to crew members based on U.S. EPR predecessor operating experience and on established roles and responsibilities as noted in Reference 1. The process then builds on these assumptions. ~~Procedures are developed and integrated with the HSI operational concept. Then, the impact of any new tasks associated with the use of integrated procedures is considered in regard to existing tasks and roles of the crew members. This consideration helps to determine if task allocation adjustments are necessary.~~ Changes in team roles and responsibilities may result from the adjustments to individual crew member responsibilities. Finally, individual team member qualification requirements may evolve with changes in team and individual roles.

18-36

~~A full-scale mockup of the MCR working area, including main control consoles (i.e., workstations) and the plant overview panel is used to verify physical layout aspects such as availability of workspace, physical access, visibility, and related anthropometric and HFE issues. The MCR mockup is also used for walk-through exercises to examine issues such as staffing levels, task allocation, and procedure usage.~~

~~A computer-based procedure system is available to the operators via the HSI. This computer-based system helps achieve the staffing goal for the MCR by reducing the mental burden and workload of the operators. The use of computer monitoring of tasks and automation reduces parallel activities being performed by operators and the probability of human error.~~

~~The integrated system validation conducted as part of the verification and validation (V&V) process includes the following evaluations:~~

- ~~Establishment of HSI adequacy for achieving HFE program goals.~~
- ~~Confirmation of function allocation and task structure assigned to personnel.~~
- ~~Establishment of the adequacy of MCR staffing levels and the adequacy of the various HSIs to support the staff in accomplishing their tasks.~~
- ~~Integration of operating procedures.~~
- ~~Confirmation of the dynamic aspects of the HSI for task accomplishment.~~
- ~~Evaluation and demonstration of error tolerance to human and system failures.~~

18.5.3 Results

18-36

~~If it is determined from the integrated system validation that plant staffing and HSI design goals are not achieved, a decision is made to redesign the appropriate system, modify the roles and responsibilities of effected staff (taking into account the effect on plant safety and reliability), or adjust staffing numbers. A final check is then performed to verify that the staffing numbers and configuration are still in compliance with the requirements of 10 CFR 50.54 (i) through (m).~~ The staffing and qualification analysis is summarized within task analysis. ~~in conjunction with the V&V results (refer to Section 18.10)~~ and includes an evaluation of the number and qualifications of personnel needed to operate~~, maintain,~~ and test the U.S. EPR based on the HSI design features for normal, abnormal, and emergency conditions.

18.5.4 References

1. ~~ANP-10279P, "U.S. EPR Human Factors Engineering Program Topical Report," AREVA NP Inc, January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

Next File

18.6 Human Reliability Analysis

A goal of the HFE program is to establish that plant operators can access the required information and controls to safely and efficiently monitor and control the plant processes and equipment. HRA evaluates the potential for human error that may affect plant safety. Thus, HRA is an essential element in achieving the HFE design goal of providing a design that enhances human performance during plant operation.

18.6.1 Objectives and Scope of HRA / HFE Integration

HRA identifies possible human error mechanisms that may affect plant safety. When these risk-significant HAs are determined, they are incorporated into the HFE design process with the objective of providing robust decision making and support for executing actions to the operator performing the risk-significant HA. A well implemented HRA helps achieve the goal of providing an HSI design that minimizes personnel errors for risk-significant HAs, supports the detection of errors, and provides opportunities to recover from errors. As described in NUREG-0711 (Reference 2), HRA provides inputs to most aspects of the HFE design.

The probabilistic risk assessment (PRA) is described in Chapter 19. Risk-significant HAs are identified in the HRA portion of the PRA and are considered in the HFE design. As described in Chapter 19, risk-important HAs are identified by using selected importance measures, HRA sensitivity analyses, and threshold criteria.

The integration of HRA with HFE helps designers confirm that human-error mechanisms are addressed in the design of the HSI to minimize the likelihood of personnel error, and to verify that errors are detected and recoverable.

18.6.2 Methodology

18-36

~~An~~The ~~i~~Implementation ~~p~~Plan for the Integration of Human Reliability Analysis into the HFE Program (Reference 1) describes the methodology for integrating HRA results with the various HFE program elements, which includes:

- A description of how various portions of the PRA were considered to determine the risk-significant HAs and the importance measures, HRA sensitivity analyses, and threshold criteria used to compile the list of risk-significant HAs.
- A description of how HAs influence operator tasks related to monitoring passive and automated systems.
- A description of how the PRA and HRA results along with the risk-significant HAs are addressed in other aspects of the HFE program with a goal of minimizing the likelihood for operator error and the ability to detect and recover from errors.
- A description of how HRA assumptions are validated during the design process.

- A description of the integration of HRA into the HFE program.

18-36

The HFE design gives special attention to those plant scenarios, risk-important HAs, and HSIs that have been identified by PRA and HRA as being important to plant safety and reliability.

The HRA evaluates and identifies specific HAs based on the impact of potential errors on plant safety. This evaluation is iterative. It begins early in the design process and continues throughout ~~each~~all phases of the design. The initial HRA is defined by a set of scenarios and accident sequences that contribute to core damage frequency or large release frequency. The HRA also considers operating experience, staffing and training, and other engineering assumptions that affect plant operation and human performance. From these inputs, human error probabilities (HEP) are calculated. HEPs are influenced by performance shaping factors (PSF), which are used to adjust the base HEPs to account for conditions such as the complexity of the accident and the stress upon the operators (refer to Chapter 19).

As the EPR design develops, the HRA model is refined to incorporate other HFE elements that will affect human performance. These elements influence the HEP estimates through the PSF values and the PRA evaluates the impact of these errors on accident scenarios. The HRA supports the HFE by providing the HSI design team with feedback that assists in minimizing personnel errors, and improving operator recovery from human errors and plant system failures.

Risk-significant HAs and their associated tasks and scenarios are specifically addressed during function allocation analyses, task analyses, HSI design, procedure development, and training. This process helps verify that these tasks are well supported by the design and are within acceptable human performance capabilities (e.g., within time and workload requirements).

As described in Section 18.10, HRA assumptions such as decision making and diagnosis strategies for dominant sequences are validated by walkthrough analyses with operationally experienced personnel using a plant-specific control room mockup or simulator. Reviews are then incorporated into ~~the final quantification stage of the PRA.~~subsequent iterations of HRA and PRA.

18-36

18.6.3 Results

An output report identifies the list of risk-important HAs and summarizes how those HAs and the associated tasks and scenarios were addressed during the various parts of the HFE design process. The output report addresses the results of the HRA assumption validation.

18.6.4 References

18-36

1. ~~ANP-10279P, "U.S. EPR Human Factors Engineering Program Topical Report," AREVA NP Inc, January 2007.~~Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.

2. NUREG-0711, "Human Factors Engineering Program Review Model," Revision 2, U.S, Nuclear Regulatory Commission, February 2004.

Next File

When a set of OER data is collected, it is classified with respect to its relevance and importance. Classification of OER data is important because it is only useful if it is accessible to members of the design team engaged in the relevant activities. Section ~~5.4.3~~3.3 of the ~~AREVA Human Factors Topical Report (Reference 2)~~ U.S. EPR Human Factors Operating Experience Review Implementation Plan (Reference 14) describes how OER information is screened. ~~OER items classified as highly relevant to the U.S. EPR HSI design are captured in the HFE Issues Tracking Database.~~ Issues not resolved in the current iteration of the HSI design are placed in the HFE issue tracking system to alert the applicable design organization of the relevant OER information. A review of the ~~HSI design implementation plan~~U.S. EPR Human System Interface Design Implementation Plan (Reference 14) and the HSI style guide (see Section 18.7.5) is performed so that the HFE principles cited in the OER event are applied to HSIs in the HSI design process. The HSI style guide documents how HFE principles from OER events are included in the HSI design and justifies the application of those principles.

18-36

18.7.1.1.2 Functional Requirement Analysis and Function Allocation

FRA and FA are performed as described in Section 18.3 and as described in the FRA and FA Implementation Plan (Reference 14). These analyses determine which operational functions are to be performed by automatic systems, by plant personnel, or by some combination of the two. The allocation is made based on the FRA after determining what is required to perform the function. FA evolves from FRA and results in allocating functions for the best overall accomplishment for that function.

A function is a process or activity required to achieve a desired operational goal. The term, function, may refer to those critical to plant safety (e.g., initiation of emergency feedwater) or to non-safety support equipment (e.g., a valve or information display). Functions are essentially hierarchical; for example, pressurized water reactors have evolved a natural hierarchical structure of functions, processes, systems, and components. High-level functions may be accomplished through a combination of lower-level system functions and may require human action (HA). Allocation of functions to humans may be appropriate at any level of the functional structure.

Operational requirements related to a given process function are better defined by breaking the function down into more basic components. At a low level, a function

18-36

~~can and must be~~is explicitly assigned to an available resource (i.e., hardware, software, human, or some combination thereof). The overall goal of FRA and FA is to define the requirements in detail so that the allocation can take advantage of human strengths and avoid human limitations to maximize overall function accomplishment.

Inputs to the FRA include the overall plant design and operational concept, HSI concept definition (i.e., accomplished via the U.S. EPR predecessor designs), and OER identified tasks associated with a high workload that would be more efficient if automated. The FRA inputs lead to the definition of concept of operations (see

Section 18.7.2) with respect to the role of personnel. The inputs define potential changes to functions and allocations, but are to be evaluated against the established automation criteria. Changes to functions and tasks that are inherently expected to be accomplished by humans or those that are required to be automated ~~(refer to Section 5.4.4.3 of Reference 2)~~ either require review by the design review board or are subject to other design change control processes.

18-36

The results of the FRA and FA are used to identify the personnel role in performance of functions to reveal the task requirements and identify the HSI design implications. These HSI design implications include insight into the information that is to be displayed and how that information is presented. This information is used in the HSI procedure and training design to make sure that adequate task support is available to the operators.

18.7.1.1.3 Task Analysis

For the U.S. EPR HSI design, TA is performed for procedure development and is iterated as the HSI design detail evolves as described in Section 18.4.

TA involves determining the requirements for plant personnel to successfully perform complex real-time control actions that stem from functions assigned to them as a result of the FA design effort. Actions performed by plant personnel to accomplish a common-purpose group of activities or functions are called tasks. TA requirements are a primary consideration in design of the HSI.

The TA must select appropriate tasks for analysis. When the tasks are selected, high-level descriptions of the tasks based on basic information can be developed. For example, the purpose, relationship to other tasks, and timing are considered. Using the high-level descriptions, more detailed descriptions of a task are developed to decompose the task into detailed steps. As these details emerge, task resource requirements (i.e., the process data and controls required) become apparent. Resource requirements such as alarms, displays, and controls affect the HSI design requirements. Task resource requirements are also beneficial for determining what should be displayed, how information should be grouped, and the sequences of how users will ~~need~~use the information.

18.7.1.1.4 Staffing and Qualifications and Job Analysis

18-36

As described in Section ~~4.1~~2.2.2.1 of the U.S. EPR HFE Program Management Plan (Reference 2), each member of an operating crew has a unique role and a unique set of responsibilities. The crew members must interact with each other and with the plant in order to fulfill their roles and responsibilities. The number of crew members assigned to an operating shift is based on the need for personnel to accomplish real-time operational goals with a reasonable workload. ~~Staffing and qualification~~Workload analysis considers the allocation of assigned operational

activities, the impact of those activities on crew member roles and responsibilities, and the impact of changes to operational requirements for the operating crew as a whole. The methodology for analysis of staffing and qualifications is described in Section 18.5.

The results of the evaluation of staffing, qualifications, and integrated work design impacts the HSI design in terms of:

- How operational activities are allocated to crew members, including assignments that make operational activities more efficient or reduce workload.
- How teamwork is supported.
- Personnel qualifications.
- Required staffing levels.

18.7.1.2 System Requirements

~~The~~ HSIs are designed to meet several system requirements. The HSI system requirements are documented for use throughout the HSI design process. As described in Section ~~5~~4.5.1 of the U.S. EPR EPR HFE Program Management Plan (Reference 2), the design control process facilitates the translation of high level requirements to lower level requirements, design inputs to design outputs, and high level design features to lower level subsystem and component design features.

18-36

The HSI consists of the controls, alarms, and indications used by the operator for controlling and monitoring the plant. Most plant and system functions are monitored and controlled by the automation system~~, which are continuously~~ supervised by the operations staff. However, some system and functional requirements require manual operator actions and associated monitoring activities.

Details of the HSI system requirements and HSI functions including power requirements, interactions between HSIs (e.g., the alarm system with the plant overview display system; the computerized procedure system with the workstation display system), and interaction between HSIs and instrumentation and controls (I&C) systems are addressed in Section 7.1.

Screen-based HSIs that control safety components that may cause plant transients require two steps to perform an action once the active control window is opened. The first step selects the type of action (e.g., close or throttle valve, stop pump) and the second step executes the action. ~~The active control window is always layered over any other open control windows to avoid initiating incorrect commands. Use of hard-wired HSIs for control of safety components is administratively controlled by incorporating operator self-checking and three-way communication techniques.~~

18-36

For the U.S. EPR, each division of safety-related mechanical and electrical components has its own safety-related screen-based HSI (i.e., qualified display system (QDS)). A minimum of four separate QDSs are used to control the four trains of safety-related components. A dedicated QDS capable of receiving all four trains of data is used to give the operator an overview of the plant. The dedicated overview QDS is for monitoring only, with one way communication, and cannot impact the plant. See Section 7.1.1.2.1 for more information on safety-related HSI.

18.7.1.2.1 Alarm Management Hierarchy

The alarms on the PICS are prioritized into levels. The PICS provides the ability to display, record, and acknowledge alarms and warnings that are necessary for the operators. A color scheme is associated with the prioritization of the alarm to inform the operator of the nature of the alarm and the priority level. The operator uses the alarm text to view alarm details. A direct navigation link associated with the alarm is also available to the operator. Direct navigation links are used along with the alarm management system to allow the operator quick access to related information and controls.

~~For high alarm priority functions, grouped alarm annunciation is also provided on the safety information and control system (SICS).~~

18.7.1.2.2 Loss of Non-Safety Computerized HSIs

18-36

The U.S. EPR is normally controlled from PICS, the non-safety HSI. An independent safety-related HSI back-up, SICS, provides the ability to control and monitor the plant for a limited amount of time to keep it in a safe and steady power condition. If PICS is not available or directly recoverable, the plant is shut down. The SICS consists of QDSs and selected hardwired controls and alarms. The QDS is also safety qualified for controlling and monitoring the plant.

~~Section 4.3.1.1 of Reference 2 describes the criteria to determine PICS availability. The operator verifies PICS data against SICS data when necessary.~~ The PICS also has status ~~lights~~indication to assist the operators in determining availability. ~~The operator is in close physical proximity to both SICS and PICS when seated at a workstation.~~ If the operator begins using the SICS, it has priority for safety-related commands.

18.7.1.2.3 Loss of Plant Automation

No manual actions are required to be taken for 30 minutes from the main control room (MCR) to maintain the plant in a safe condition during design basis events (DBE). During DBEs the trip functions of the protection system (PS) (Section 7.2) and the plant automation of the SAS (Section 7.1) are credited to attain a safe plant state. In the unlikely event that the PS fails, the diverse actuation system (DAS) (Section 7.8) is provided to initiate functions designed to mitigate the effects of DBEs and place the

18.7.1.3.7 10 CFR 50.34(f)(2)(xii) - Auxiliary Feedwater Initiation

The U.S. EPR HSIs enable automatic (protection system) as well as manual system level initiation of the emergency feed water system from the control room, via the SICS. The PICS also displays emergency feed water system flow in the control room. See Section 7.5 for more details.

18.7.1.3.8 10 CFR 50.34(f)(2)(xvii) - Accident Monitoring Instrumentation

The U.S. EPR HSIs provide indication in the control room of containment pressure, containment water level, containment hydrogen concentration, containment radiation intensity, and noble gas effluents at potential accident release points. This indication is provided on the PICS and SICS. See Section 7.5 for more details.

18.7.1.3.9 10 CFR 50.34(f)(2)(xviii) - Inadequate Core Cooling Instrumentation

Indication of inadequate core cooling is provided in the MCR on both PICS and SICS. See Section 7.5 for more details.

18.7.1.3.10 10 CFR 50.34(f)(2)(xix) - Instruments for Monitoring Plant Conditions Following Core Damage

The U.S. EPR HSIs enable the ability to monitor plant conditions following an accident that includes core damage. This indication is provided on the PICS. See Section 7.5 for more details.

18.7.1.3.11 10CFR50 Appendix A GDC 19

18-36

The remote shutdown station (RSS) inventory consists of ~~both~~ PICS ~~and SICS (see Section 18.7.4.5)~~. The ~~SICS and~~ PICS in the RSS ~~have the capability~~provides the HSI for prompt hot shutdown of the reactor, including necessary I&C to maintain the unit in a safe condition. Also, the RSS HSIs provide the capability for subsequent cold shutdown of the reactor through the use of suitable procedures. The RSS is not used for normal operation of the plant.

18.7.1.3.12 10 CFR 50.55a(a)(1)

Structures and components of the safety-related I&C systems that perform safety-related functions are classified as such and are designed, fabricated, erected, constructed, tested, and inspected commensurate with the safety-related function they perform.

10 CFR 52.47(a)8 - Content of Applications (for standard design certification dealing with compliance with TMI requirements)

Information necessary to demonstrate compliance with technically relevant portions of the TMI requirements in 10 CFR 50.34(f) are listed in Section 18.7.1.3.

18.7.1.3.19 NUREG-0737 Supplement 1 Clarification of TMI Action Plan

The U.S. EPR HSIs have indications and control for safety components to meet the Three Mile Island (TMI) action plan requirement. The plant safety parameter display is available in the MCR and in the emergency support facilities.

18.7.1.4 Other Requirements

References 7, 8, 9, and 10 contain industry HFE guidance, which is considered in the design of the U.S. EPR HSIs.

18.7.2 Concept of Operations

The design of the plant I&C platform, the HSI, and the control rooms consider the concept of operations including:

- Physical characteristics and technical abilities of the operating staff.
- Shift staffing and organization.
- Responsibilities of the operational staff.

This section provides a summary description of the concept of operations and assumptions relative to the staffing, personal characteristics, division of team responsibilities, and other related issues that form the basis for the MCR and related HSI design.

The concept of operations is primarily concerned with the MCR operating team. The secondary concern includes system users to be considered in the design of other user interfaces.

18.7.2.1 Crew Composition

Operating crew composition is described in Section 18.5 and in Section ~~4.1~~2.2.2.1 of the EPR HFE Program Management Plan (Reference 2).

18.7.2.2 Roles and Responsibilities of Crew Members

18-36

As described in Section 18.5, a design goal for the U.S. EPR is that three licensed operators can safely monitor and control the plant under operating conditions including normal operation, startup, shutdown, abnormal operation, and accidents. One licensed operator is required to be at the controls, a second licensed operator is required to be on shift but not continuously at the controls, and the control room supervisor (CRS) is required to be present in or readily available to the MCR at all times. In addition, each operating crew includes a shift ~~supervisor~~manager (~~SS~~SM)~~, a shift technical advisor (STA) (may be combined with the SS position),~~ and a number of non-licensed (equipment) operators (NLO), and a maintenance crew. Plant operating

procedures (i.e., normal, abnormal, emergency) are based on roles, functions, and responsibilities of the integrated operating team and are designed so that operators, technicians, and maintenance staff function as an integrated team.

18-36

~~The generic tasks of the operators are described in Section 4.1 of Reference 2.~~

18.7.2.2.1 **DELETED~~Function of Control Room Operators~~**

~~Shift Supervisor~~

~~The SS is the senior person on shift whether in or out of the MCR and is responsible for command and control of site activities for the duration of the shift. The SS holds the highest level of operating license (i.e., senior reactor operator (SRO)) and may also perform the function of the STA as required in NUREG-0737 (Reference 3), if the qualifications are met.~~

~~SS responsibilities include the following:~~

- ~~Coordinate activities site-wide (assuming single unit site).~~
- ~~Make sure plant operations are conducted in accordance with technical specifications and supervise the execution of plant operating procedures during normal, abnormal and emergency conditions.~~
- ~~Determine if equipment is operable.~~
- ~~In order to maintain situational awareness, the SS does not generally directly manipulate plant control. Administrative rules require that the SS avoid direct operations when the CRS and the RO are available.~~
- ~~Review operator logs, condition and event reports, and other documentation from the MCR and provide notification to appropriate operations management when required.~~
- ~~Monitor and direct the actions of the CRS when the site situation warrants.~~
- ~~Manage shift turnover, crew briefs, and coordinate maintenance activities (e.g., work orders, tagouts, and crew interface).~~
- ~~Coordinate refueling operations.~~

~~The SS generally observes plant activities via the plant overview panels or over the shoulder of other MCR operators, but may utilize an auxiliary workstation in the MCR.~~

~~A room is provided within the MCR for the SS to work on administrative tasks. This office provides direct access to the MCR and contains a window with a view of the control room.~~

18-36

Depending on the plant state and the availability of other personnel in the MCR with an SRO level license, the SS may make field observations in the plant.

Shift Technical Advisor

Each operating shift is required to have an individual designated to perform the functions of an STA in accordance with NUREG-0737 (Reference 3). For the U.S. EPR, the STA function is normally performed by the SS, provided that the SS meets the STA training and formal education requirements. The STA is not required to be in the control room areas but is required to be available in the MCR within a short period of time. When in the MCR, the STA uses any available workstation to monitor operational aspects (i.e., high-level plant overview data) for safe operation of the plant. Display hierarchy and navigation design documentation provides an overview of the type of information the STA monitors.

Control Room Supervisor

The CRS is the licensed SRO tasked with monitoring plant processes in accordance with the operating procedures.

CRS responsibilities include the following:

- Report to the SS.
- Coordinate activities plant-wide.
- Command and supervise activities in the MCR including and establishing the priorities of action and designates specific responsibilities to the RO and the additional licensed operator (ALO), where applicable.
- Supervise plant operations for conformance with Technical Specifications and supervise the execution of plant operating procedures during normal, abnormal, and emergency conditions.
- Determine which operating procedures should be implemented at any given time.
- Approve evolutions or testing affecting core reactivity.
- Approve the removal of equipment and systems from service for maintenance, testing, or operational activities and return such equipment and systems to service.
- Determine the mode of operation.
- Evaluate plant performance and make operational judgments based on operating characteristics, reactor behavior, and instrument interpretation.
- Track alarm status.
- Supervise operation surveillances for on-schedule implementation.

18-36

- Supervise the maintenance of primary and secondary chemistry control.
- Maintain awareness of defense-in-depth configuration, thermal margin, containment closure, and equipment hatch status as well as make sure that the safe shutdown configuration controls are satisfied.
- Initiate maintenance or trouble shooting requests for identified equipment problems.
- Supervise members of the operating crew for conformance to approved operational and administrative procedures and maintain awareness of any current short-term information, such as special night orders from the operations superintendents.
- Communicate and inform other control room personnel of abnormal plant conditions and actions taken as well as coordinate operational activities with the RO and the SS.
- Maintain situational awareness.
- Control access to the MCR.
- Supervise shift turnover and conduct shift briefings prior to the start of each shift.
- Act as system manager with respect to the plant processes and their systems and equipment operation.

The CRS is required in the MCR at all times and may leave the MCR only when properly relieved. The CRS is normally seated at an operator workstation, which provides a view of the workstations manned for controls activities. The CRS is expected to not be at the controls operating the plant in order to maintain an overview of the plant situation. Display hierarchy and navigation design documentation describes the type of plant and system overview displays normally monitored by the CRS.

Reactor Operator

The RO is specifically tasked with monitoring and controlling portions of the plant in accordance with the operating procedures and as directed by the CRS. The RO is normally seated at a workstation controlling the plant.

RO responsibilities include the following:

- Report to the CRS.
- Maintain situational awareness.
- Monitor the status of the plant.

18-36

- Execute plant operating procedures under normal, abnormal, and emergency conditions.
- Communicate and inform other control room personnel of plant conditions and actions taken.
- Operate equipment controlled from the MCR.
- Remain cognizance of standing orders or night orders.
- Maintain plant conditions within limitations of plant license and identify Technical Specification action statements when they occur.
- Maintain communications with the load dispatcher to make sure plant load limitations are thoroughly understood.
- Receive, review, and approve control room log readings that are generated automatically.
- Supervise hot license class candidates while they control the plant.
- Interface with maintenance personnel that are conducting periodic tests of plant equipment or systems, and monitor control room responses to test activities.

The RO is required in the MCR at the controls (within sight of the indications of key primary plant parameters) at all times and may leave the MCR (or the RSS) only when properly relieved. The RO is normally seated at a workstation used to operate and monitor plant processes. Display hierarchy and navigation design documentation provides an overview of the type of displays the RO requires.

Additional Licensed Operator

At least one ALO (e.g., SRO or RO) is assigned to each shift and fills roles and functions as directed by the SS or CRS. When required to operate equipment from the control room, the ALO normally operates from a sit-down workstation, relieving the RO from monitoring and controlling the balance of plant (BOP) and auxiliary system functions. Depending on the needs of the shift, typical roles and responsibilities of the ALO may fall into two general categories: administrative and operational.

Administrative responsibilities include the following:

- Assist with administrative functions such as tagouts and work orders.
- Coordinate conduct of surveillance tests.
- Relieve the MCR operators as necessary within the limitations of the ALO's license.

Operations responsibilities include the following:

18-36

- Assist the operators from a sit-down workstation as needed (i.e., specific actions similar to RO during normal operations), during planned high-activity, labor-intensive evolutions such as plant startups and shutdowns.
- Operate the secondary plant or electrical equipment controlled from the MCR during high-activity, labor intense evolutions.
- Operate the primary plant as directed by the CRS.
- Supervise hot license class candidates while they control the plant (in support of the MCR RO).
- Conduct and verify plant component lineups as directed.
- Communicate with RO to remain cognizance of reactor and primary systems.
- Coordinate conduct of plant surveillance tests as directed.
- Receive, review, and approve control room log readings that are generated automatically, as directed.
- Provide temporary relief for the RO as needed.
- Prepare RSS operations to transfer operations to the RSS, when needed.
- Review tagouts and work orders for accuracy and adequacy as directed by the CRS or SS.
- Act as the equipment operator with respect to the plant processes and their systems and equipment operation.

When in the MCR, the ALO is normally seated at the controls in the workstation and is responsible for operating and monitoring plant processes as directed by the CRS. Display hierarchy and navigation design documentation provides an overview of the type of information the ALO requires.

Whether stationed in the MCR or elsewhere, the ALO is required to remain cognizant of plant conditions.

18.7.2.2.2 Non-Licensed Operators

NLOs normally perform operational duties outside the MCR to support plant operation. NLOs are assigned to operate equipment located in specific buildings or in specific trains. This includes performing most operational surveillance procedures for such equipment.

NLOs responsibilities include the following:

- Report to the CRS or SS as applicable.

18-36

- ~~Perform required manual system line-ups and component-level operations required to prepare a plant process system for operation from the MCR.~~
- ~~Execute applicable portions of plant operating procedures (not requiring specific licenses to perform) during normal, abnormal, and emergency conditions.~~
- ~~Make inspection tours of the plant to perform physical verifications of normal operating conditions.~~
- ~~Investigate local alarm situations, assess conditions, and perform diagnostics within their training and authority.~~
- ~~Operate applicable local control stations within their training and authority.~~
- ~~Keep shift personnel informed of actions taken and any operationally significant conditions observed in the plant.~~

~~The SS, on-duty CRS, or RO (as applicable) shall direct operational actions taken by the NLO.~~

~~An NLO is normally assigned the responsibility of executing official communications to agencies outside the plant during a shift. When trained and qualified, an NLO may operate the fire alarm protection system.~~

~~The NLOs on shift are normally in the plant performing assigned duties or training, or awaiting assignments from the SS or CRS in the MCR or the integrated operations area. NLOs normally do not operate the plant from the MCR via the PICS or SICS unless they are participating in hot license instruction.~~

18.7.2.2.3 ~~On-Shift Operations Support Staff~~

~~Instrumentation and Controls Technicians~~

~~I&C technicians and system administrators have distinct areas of responsibility. I&C technician tasks primarily include supervision and maintenance of the I&C systems such as corrective and preventative maintenance, and Technical Specification surveillances. I&C system administrators are experienced staff members who perform approved modifications (i.e., software, hardware, and instrumentation) to plant I&C systems based on the procedures and rules for implementing plant modifications. I&C technicians and system administrators generally perform their roles and responsibilities from the Instrumentation and Control Service Center (I&CSC).~~

~~Users of Miscellaneous Specialized Plant I&C Equipment~~

~~There are specially trained and authorized personnel designated for monitoring and operating specialized systems, such as the loose parts and vibration monitoring systems, leakage monitoring system, the core monitoring systems, and similar special~~

~~purpose systems. These systems have important roles in the operation of the plant and require the users to have access to the I&CSC and the MCR.~~

18.7.2.3 Personnel Supervision of Plant Automation

18-36

In the event of incidents or accidents, functions are automated when analysis shows that immediate action is required sooner than the human response time. Operator action is not required for the first 30 minutes following a design basis event. The operator monitors the automatic operation of the control systems, intervening only in the event of malfunctions of the automatic control system during the initial stages, or to optimize plant parameters or configuration. When the situation is stabilized, the operator function then shifts back to active control. When feasible during abnormal or emergency situations, when conditions are stabilized or under control, the ~~SS~~SM, CRS, and RO physically reviews the appropriate procedure(s) to make sure that all steps were accurately performed.

The role of plant automation and how operators interact with it is described in the concept of operations. ~~Criteria for defining automation are shown in Section 5.4.4.3 of Reference 2. An~~The U.S. EPR Human System Interface Design Implementation Plan ~~HSI design implementation plan~~ (Reference 14) specifies how the automation criteria and the role of operators as supervisors of automation are translated into the design guidance for the HSI.

18.7.2.4 Use of Main Control Room

Use of the MCR during normal operations, during operational occurrences such as loss of PICS or electronic operating procedures, and during emergency or accident scenarios is described in Section~~s 4.2 and 4.3~~2.2.2.2 of the EPR HFE Program Management Plan ~~(~~Reference 2~~)~~.

18-36

18.7.2.5 Crew Member Coordination Methods

The following sections describe how the operations staff interacts within the MCR and other areas. Also included are descriptions detailing how MCR operators communicate and interact with the NLOs and other personnel such as maintenance technicians, engineers, and emergency support staff. A description of the security measures used to control access to control rooms and to the HSI is also provided.

18.7.2.5.1 Forms of Communication and Expected Use

MCR operator communication is essential for the safe operation of the plant. The RO or other MCR operators are required to communicate with operations staff such as NLOs, technicians, engineers, and emergency support staff regarding periodic maintenance, equipment repairs, and abnormal operating conditions. The design of the HSI considers task loading for each individual operator as well as the time it takes

to communicate with others while performing those tasks. To reduce the burden on the operator and validate the minimum staffing requirement assumptions, training the operators to communicate efficiently, effective layout of the control rooms, and a well designed HSI are required. Furthermore, flexibility in the layout of the control rooms and design of the HSI allows for ease of change as communication methods improve with new technology.

18-36

Communication of orders for plant operation is initiated using a chain of command structure. For example, the ~~SS~~SM provides orders to the CRS, the CRS provides orders to the RO, the ALO, or the NLOs, and the RO provides orders to the ALO or NLOs. Verbal communications not directly related to plant operation are minimized in the MCR to avoid interference or disruption. Communicating other types of information, such as authorization and work plans for normal maintenance or testing, is conducted during pre-shift or pre-job briefings if the MCR operators have a need to know. The ~~SS~~SM is generally the point of contact for emergent or non-operational communications.

Face-To-Face Communication

Face-to-face communication is the most effective form of communication because it allows the most information to be conveyed. This form of communication is the preferred method and, when possible, is used for orders related to the operation of the plant safety systems.

Other Forms of Two-Way Communications

Telephones, electronic devices, or other forms of visual two-way communication are used when face-to-face communication is not possible or not efficient. Orders are acknowledged with ~~check~~repeat-backs to confirm the accuracy of the message. Several forms of ~~two~~three-way communication are provided within the MCR of which the plant operators are trained.

18-36

The use of one-way communication (i.e., general public-announcing systems) is limited to emergency situations or when the information is of interest to others not in the audible vicinity of the person conducting the announcement.

18.7.2.5.2 Control Rooms Traffic

Unescorted entry into the control room is only permitted to individuals with proper authorization. Electronic security devices are used to restrict access into the MCR, TSC ~~(when activated during an emergency)~~, RSS, or I&CSC. Permission from the CRS or ~~member of management~~responsible licensed operator is also required to enter these control rooms.

TSC and RSS

18-36

The RSS is generally not occupied except in the event of an MCR evacuation. The ~~SS~~SM or CRS shall authorize access to the RSS as necessary.

The TSC is part of an integrated operations area which is normally in use during power operations. When the TSC is activated during an emergency, all other uses of the integrated operations area are suspended. The emergency coordinator assumes responsibility for controlling access to the TSC when it is activated.

I&CSC

The I&CSC is not continuously occupied. It is staffed by I&C engineers and technicians, I&C system administrators, and trained and authorized personnel designated to operate specialized systems such as the loose parts, vibration monitoring, leakage monitoring, and the Aeroball and PowerTrax core monitoring systems. Several forms of communication are provided in the I&CSC allowing operators immediate communication with the technicians. Access to the I&CSC is controlled by the CRS.

18.7.3 Functional Requirements Specification

18-36

As described in Section ~~5.3~~4.5 of the EPR HFE Program Management Plan (Reference 2), design documents are produced for each of the control rooms (i.e., MCR, TSC, RSS, I&CSC) and HSIs (i.e., PICS and SICS) to track requirements and design specifications. These design documents capture the functional requirements as well as the HFE requirements and provide a uniform philosophy and design consistency among HSIs, including screen style and layout guide, hierarchy of and navigation between screens, alarm system operation, electronic procedure system, plant information system, and hard-wired control integration in panels and workstations.

Section 18.7.4.3 describes how the inventory of alarms, displays, and controls needed to operate the U.S. EPR is determined.

18.7.4 HSI Concept Design

The U.S. EPR implements a modern I&C design based on experience gained internationally in new plant designs and retrofits in existing plants with digital I&C equipment. The HSI concepts are further based on predecessor designs and utilize similar control of system functions and I&C concepts. The concepts for the HSI design for the U.S. EPR are described in Section 7.5, ~~and in~~ Section ~~3.2~~2.2.1.2 of the EPR HFE Program Management Plan (Reference 2), and Section 5.1.2 of the U.S. EPR Human System Interface Design Implementation Plan (Reference 14).

18.7.4.1 Safety Parameter Display System

The parameters required to be displayed as part of the SPDS are made available on the PICS and SICS. For more details refer to Section 7.5.

18.7.4.2 Operation and Control Centers System

The MCR, TSC, RSS, I&CSC and the HSIs (i.e., PICS and SICS) including the bases for layout of the control rooms and organization of the HSIs within them are described in Section ~~3~~2.2 of the EPR HFE Program Management Plan ~~(~~Reference 2~~)~~.

18.7.4.3 Inventory of Alarms, Displays, and Controls

18-36

The process data inventory, setpoints, and equipment layout needed to operate the U.S. EPR is determined by the system engineers for each piping and instrumentation system and documented in various piping and instrumentation diagrams (P&IDs) or one-line diagrams. The corresponding design documents capture the functions and functional requirements as well as the design basis for each function.

The HFE and Control Room Design Team translates the functions from the P&IDs, one-line diagrams, and design documents into the required inventory of alarms, displays, and controls. ~~An~~The ~~HSI design implementation plan~~U.S. EPR Human System Interface Design Implementation Plan ~~(~~Reference 14~~)~~ describes how the HFE and Control Room Design Team organizes and presents the alarms, displays, and controls on the HSIs in an effective context so that the operators can safely and efficiently operate the plant. Hardware and software requirements to implement this inventory and the subsequent HSI designs are verified as described in Section 18.10.

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

Minimum inventory is defined as the credited set of alarms, displays, and controls needed to implement the plant emergency operating procedures (EOP) (refer to Section 15.0), bring the plant to a safe condition, and to carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment.

The MCR minimum inventory includes the readily accessible HSIs that the operator needs to:

- Monitor the status of fission product barriers.
- Perform and confirm a reactor trip.
- Perform and confirm a controlled shutdown of the reactor using the normal or preferred safety means.

- Actuate safety-related systems that have the critical safety function of protecting the fission product barriers.
- Analyze failure conditions of the PICS while maintaining the current plant operating condition and power level until the PICS can be restored in accordance with applicable regulatory requirements.
- Implement the plant emergency operating procedures.
- Bring the plant to a safe condition.
- Carry out those operator actions shown to be risk important by the applicant's probabilistic risk assessment.

The PICS is the primary non-safety-related HSI normally used for plant monitoring and control. Because the PICS is not credited for performance of safety-related functions, the minimum inventory includes alarms, displays, and controls that are required in addition to the PICS. Thus, the minimum inventory is the portion of the SICS inventory credited for EOP actions to bring the plant to a safe condition or to carry out risk-important operator actions that readily accessible to the operators and does not need to be selected from a menu or screen hierarchy. The SICS performs the functions described in Section 7.1 including both hardwired functions and QDS functions.

A list of the minimum inventory on the MCR SICS is included in Table 18.7-1—Minimum Inventory of Main Control Room Fixed Alarms, Displays, and Controls.

18-36

The methodology for selecting the final minimum inventory is described in the ~~HSI design implementation plan~~U.S. EPR Human System Interface Design Implementation Plan (Reference 14) and includes a description of:

- The selection criteria.
- How the functions and tasks that need to be supported by the SICS minimum inventory are identified.
- The technical requirements that apply to the design of the SICS minimum inventory including those imposed by regulatory requirements, and particularly address requirements related to qualification, independence, and accessibility.
- How the plant-specific probabilistic risk assessment is used to identify operator actions or tasks that are risk important.
- How the guidance provided in RG 1.97 relating to defining postaccident monitoring variables is addressed (see Section 7.5).
- The operator actions credited in the safety analysis or plant-specific EOPs for safety and non-safety success paths.

- How the diversity and defense-in-depth evaluation is used to identify any specific operator actions credited for coping with common cause failures of the protection systems.

- The criteria that are used to determine which SICS components need to be spatially dedicated, continuously visible, continuously available, or accessible by taking only one action (i.e., MCR design and concept of operations).

18.7.4.5 Remote Shutdown Workstation Alarms, Displays, and Controls

The MCR provides the capability for safe shutdown, even assuming a safe-shutdown earthquake (SSE), a loss of offsite power, and the most limiting single failure. Localized emergencies which make the environment unsuitable for the operators and require evacuation of the MCR are not postulated concurrent with other design basis events. If evacuation of the MCR is required, the operators can establish and maintain a safe shutdown from outside the MCR through the use of the PICS and SICS (reactor trip only) in the RSS.

18-36

The minimum inventory of alarms, displays, and controls in the RSS meets criteria similar to that in the MCR, but consists of only those functions necessary to attain safe shutdown following an MCR evacuation. The RSS minimum inventory includes the readily accessible HSIs that the operator needs to:

- Perform and confirm a reactor trip.

- Place and maintain the reactor in a safe condition using the normal or preferred safety means.

Section 7.4.1.3 describes safe shutdown from outside the MCR by use of the RSS.

A list of the minimum inventory on the RSS SICS is included in Table 18.7-2—Minimum Inventory of Remote Shutdown Station Fixed Alarms, Displays, and Controls. The methodology for selecting the final minimum inventory for the RSS is ~~similar to that~~ described in Section 18.7.4.4.

18-36

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

A style guide provided by the HFE and Control Room Design Team is used in the design of HSI features. It also provides guidance on such issues as general plant layout design, equipment accessibility requirements, coding and labeling, and environmental issues such as lighting, acoustics, personnel protection equipment, and ambient conditions suitable for personnel. The style guide is a design guideline applicable to engineering disciplines (e.g., structural engineers) who are required to follow the style guide for plant and equipment layout decisions.

~~The Kraftwerk Kennzeichen System (KKS),~~An identification system for power stations, is used to assign codes to structures, systems and components for the U.S. EPR. ~~KKS c~~Coding is used for labeling on screen-based and hardwired HSI applications as well as throughout the plant.

18-36

To increase efficiency and reduce workload, links to and from higher level and lower level displays are provided. Screen navigation may be performed through lists of available display screens (i.e., menus) or navigation icons (i.e., hyperlinks).

18.7.6.1.3 Alarm System Design

The alarms alert and inform the operators when ~~unexpected~~actionable events occur. Alarms require manual actions to correct, mitigate, compensate for a failure, or make repairs.

The operators should not be burdened by multiple alarm signals that demand simultaneous actions; however, ~~operator training~~task analysis establishes the priorities for responding to alarms to maintain a high level of safety. The following principles are applied when designing the logic of alarms and overall alarm processing:

- Alarm signals lead the operator to the true cause of the reported event (i.e., alarm hierarchy minimizes distractions).
- Alarms are integrated with the HSI to assist the operator with situational awareness, alarm response, and any associated troubleshooting.
- Alarm signals include logic so that only operationally relevant conditions are alarmed (e.g., the alarm logic for low discharge pressure downstream of a pump signals an alarm only if the pump is running).
- The overall plant state is considered for the generation of alarms, or at least to inhibit alarms that are not relevant for the actual plant state.
- Pre-alarms are provided before automatic actuation only when an operator has sufficient time to identify and perform mitigative actions to preclude the need for automatic actions.

18.7.6.2 HSI Considerations and Demands on Operators

The HSI design supports operators in their primary role of monitoring and controlling the plant while minimizing physical and mental demands associated with use of HSIs. Reference 6 principles affecting the design of the HSI are incorporated into the style guide (see Section 18.7.6.1). These principles include:

- Basic screen design.
- Principles to increase usability.

- Are complete and operable.
- Conform to standard HFE principles and requirements.
- Are free of safety issues and human performance issues.
- Implement the design accurately in the final design output documentation.

Testing and evaluation is conducted throughout the HSI design at various stages of development so that the complex HSI design functions properly before the design process is resolved and validation occurs (see Figure 18.1-2).

Activities such as concept testing, mock-up activities, trade-off evaluations, and performance-based tests are utilized at various stages of the design. The criteria used to decide which type of testing or evaluation technique is applicable are described in ~~a V&V implementation plan~~the U.S. EPR Human Factors Verification and Validation Implementation Plan (Reference 14).

18-36

18.7.8 HSI Design Results and Documentation

As described in Section ~~5.4.8.7~~4.5 of EPR HFE Program Management Plan (Reference 2), the HSI designs are documented using specific design control process requirements. The various configuration management, design change controls, design verification, and design quality control tools are also described in Reference 1.

18.7.9 References

18-36

1. ANP-10266NPA, Revision ~~1~~0, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR," AREVA NP Inc., ~~April 2007~~December 2008.
2. ~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc., January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.
3. NUREG-0737, "Clarification of TMI Action Plan Requirements," U.S. Nuclear Regulatory Commission, November 1980.
4. NUREG-0711, "Human Factors Engineering Program Review Model," Rev. 2, U.S. Nuclear Regulatory Commission, February 2004.
5. ANP-~~10284~~10304, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology Technical Report," AREVA NP Inc., ~~June 2007~~May 2009.
6. NUREG-0700, "Human-System Interface Design Review Guidelines," Revision 2, U.S. Nuclear Regulatory Commission, May 2002.

7. NUREG/CR-6633, "Advanced Information Systems: Technical Basis and Human Factors Review Guidance," U.S. Nuclear Regulatory Commission, March 2000.

8. NUREG/CR-6634, "Computer-Based Procedure Systems: Technical Basis and Human Factors Review Guidance," U.S. Nuclear Regulatory Commission, March 2000.

9. NUREG/CR-6635, "Soft Controls: Technical Basis and Human Factors Review Guidance," U.S. Nuclear Regulatory Commission, March 2000.

10. NUREG/CR-6636, "Maintainability of Digital Systems: Technical Basis and Human Factors Review Guidance," U.S. Nuclear Regulatory Commission, March 2000.

11. NUREG-0696, "Functional Criteria for Emergency Response Facilities," U.S. Nuclear Regulatory Commission, February 1981.

12. NUREG-0835, "Human Factors Acceptance Criteria for the Safety Parameter Display System," U.S. Nuclear Regulatory Commission, October 1981.

13. NUREG-1342, "A Status Report Regarding Industry Implementation of Safety Parameter Display Systems," U.S. Nuclear Regulatory Commission, April 1989.

18-36

14. Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.

18.8 Procedure Development

Procedures are essential to plant safety because they support and guide personnel interactions with plant systems and personnel responses to plant-related events. Procedures and the human system interfaces (HSI) are designed in parallel using similar processes and incorporating the same accident analyses; the evaluation processes used are also interrelated. Human factors principles are applied to aspects of the interface to verify complete integration and consistency. Refer to Section ~~5.4.9~~3.2 of the AREVA NP ~~Human Factors Topical Report~~U.S. EPR Human Factors Procedure Implementation Plan (Reference 1) for a generic outline of HFE program input to the procedure development process for the U.S. EPR.

18-36

A COL applicant that references the U.S. EPR design certification will describe how HFE principles and criteria are incorporated into the development program for site procedures.

18.8.1 Objectives and Scope

From the perspective of the HFE program, the objectives of procedure development activities are to develop procedures that are technically accurate, comprehensive, explicit, easy to use, and validated (i.e., the user can comply with the requirements of each step).

HFE guidelines are applied to all procedures associated with plant operations~~,~~ and testing~~, and maintenance~~:

- Generic Technical Guidelines (GTG) for emergency operating procedures.
- Plant and system operations (including startup, power, and shutdown operations).
- ~~Maintenance.~~
- Abnormal and emergency operations.
- Alarm response.
- Equipment testing.

18.8.2 Methodology

Procedure development activities consider the following aspects:

- Plant design basis.
- System-based technical requirements and specifications.

18-36

- Results of task analyses (TA)~~ (performed specifically for procedure development)~~.

- Risk-important human actions (HA) identified in the human reliability analysis (HRA), probabilistic risk assessment (PRA), and operating experience review (OER).
- Initiating events to be considered in emergency operating procedures (EOP), including those events in the design bases.
- GTG for EOP.

Operational guidelines are provided to the COL applicant referencing the U.S. EPR standard design to assist in the development of plant-specific normal operating, abnormal operating, alarm response, and EOPs that incorporate the aspects of the HSI design appropriate to the completion of the plant-specific procedure (see Section 13.5.2.1.3). Generic plant operational guidelines are part of procedure development and are a significant contribution to HSI design because they are developed or modified to reflect the characteristics and functions of the screen-based or conventional HSIs, as appropriate.

18-36

~~An~~ The procedure implementation plan (Reference 1) describes:

- The basis or starting point for procedure development (i.e., how the TA (see Section 18.4) and procedure development interrelate).
- The content of procedures.
- How the HSI style guide (see Section 18.7.6.1) integrates with the procedure writer's guide.
- How procedures are verified and validated.
- The justification for using electronic operating procedures instead of paper-based procedures.

18.8.2.1 Procedure Writer's Guide

A procedure writer's guide is a necessary component of the procedure development program to establish consistency in organization, style, and content. This guide specifies which procedures fall within the purview of the guide. The procedure writer's guide and the HSI style guide (Section 18.7.6.1) are used concurrently while developing procedures that will provide consistency with terminology, abbreviations, and the use of component coding.

18.8.2.2 Verification and Validation of Procedures

Both the electronic and paper-based procedures are verified and validated prior to the completion of the HSI design using a high-fidelity simulator and are used as input to the integrated system validation (ISV), see Section 18.10.3.5.

18.8.2.3 Electronic Procedures

Operating procedures are implemented in a screen-based format that provides access to process information by direct links. These electronic procedures also provide access to related information and direct the operator to the appropriate control screens.

18-36

Refer to Section ~~2.2.9~~6.2.9 of the U.S. EPR Human Factors Program Management Plan (Reference 1) for further details on the development of electronic procedures.

Paper-based procedures serve as backup to screen-based (i.e., electronic) procedures and contain the same guidance and format. Hard copy backups of operating procedures are provided in the main control room (MCR), remote shutdown station (RSS), and the Technical Support Center (TSC) in the event that a failure of the operating procedure computer occurs. Aside from differences in how electronic and hard copy procedures are used (i.e., the navigation and layout) as well as the availability of live data, electronic and hard copy procedures contain the same information in the same format. Adequate space is provided at appropriate workstations in the MCR and RSS for operators to display paper-based procedures, when required.

18.8.3 Results

A results summary report addresses the final set of procedures and support equipment developed using the established methodology. The results summary report includes:

- The results of verification and validation (V&V) activities as they relate to procedure development.
- How procedures will be maintained and updates controlled.
- A description of how operators access and use procedures, especially during operational events including:
  - Storage of procedures.
  - Ease of operator access to the correct procedures.

18.8.4 References

18-36

1. ~~ANP-10279, Revision 0,~~ Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.~~"U.S. EPR Human Factors Engineering Program," AREVA NP Inc., January 2007.~~

Next File

18.9 Training Program Development

Training plant personnel is an important factor in promoting the safe and reliable operation of a nuclear power plant. A methodical analysis of job and task requirements and a Systematic Approach to Training (SAT) are used to provide plant personnel with required knowledge, skills, and attributes (KSA) to perform assigned tasks.

A COL applicant that references the U.S. EPR design certification will describe how HFE principles and criteria are incorporated into the development of training program scope, structure, and methodology.

18.9.1 Objectives and Scope

Section ~~5.4.10 of the AREVA NP Human Factors Topical Report~~ 1.5 of the U.S. EPR Human Factors Training Implementation Plan (Reference 1) describes the objectives of the training program development as they relate to the HFE program.

18-36

An implementation plan describes training program scope including:

- Categories of personnel to be trained (similar to the scope of analysis conducted for staffing, see Section 18.5.1).
- Specific plant conditions, operational activities (e.g., operations, maintenance, testing and surveillance), and HSIs which effect training scenarios and methods.

18.9.2 Methodology

Section ~~5.4.10~~3.2.1 of the U.S. EPR Human Factors Training Implementation Plan (Reference 1) provides an outline of the design process used in developing a training program for the U.S. EPR.

Specific training objectives unique to the operation of the U.S. EPR are developed to coordinate with the HSI design process and the development of procedure guidelines. These training objectives are provided to each COL applicant referencing the U.S. EPR standard design for implementation into their site-specific training program.

18.9.3 Results

A results summary report addresses the training program development including:

- The roles of organizations that contributed to the training program.
- How learning objectives were developed and translated into the use of associated KSAs.
- The use of resources (e.g., lectures, simulators, computer-based training, schedule) for training.

- Methods used to evaluate effectiveness of the program.

18.9.4 References

18-36

1. ~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc., January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

Next File

18.10 Verification and Validation

Human factors engineering (HFE) verification and validation (V&V) consists of techniques used to establish that the design of the HSI meets HFE design requirements and supports the performance of personnel tasks. V&V also establishes that the HSI design adheres to established human factors practices and meets all operational requirements.

18-36

HFE V&V consists of a variety of activities, many of which are ~~not~~ executed ~~in a single step~~ at the end of design activities~~.~~, Evaluations ~~but~~ are performed at various points throughout the design process~~. Some activities are performed iteratively as the level of detail of the design progresses~~to minimize the number of deviations revealed during HFE V&V.

18.10.1 Objectives

The first objective of HFE V&V is to establish that the design of the HSI meets design requirements. To verify the HSI design requirements, V&V demonstrates that:

- Required control capabilities and displayed quantities are provided.
- Each part of the HSI is configured as intended, as required by design-specific HFE guidance, and as described in the style guide (see Section 18.7.6.1) and industry standard practices.
- Conflicts between the various requirements and specifications have been addressed and resolved.

The second objective of HFE V&V is to establish that the HSI is effective in supporting the performance of personnel tasks. To validate that the HSI supports task performance, the entire system is tested to establish that the integrated functionality of individual requirements provides the functions and achieves the performance needed. HFE validation considers the HSI and the operators as a single system (i.e., a team type human-machine environment).

18.10.2 Scope

18-36

The HFE V&V process applies to HSIs (i.e., controls, displays, and alarms) in the MCR, the RSS, ~~and~~ appropriate local control stations (LCS)~~.~~ and ~~F~~functions considered critical to plant safety (i.e., risk-important HAs are specific targets to require sample V&V activities).

HFE V&V is also applied to the following features of the design or changes to the design:

- Procedures (hard copy and computer-based).

- Crew coordination and communication.
- Display navigation, information retrieval, and access to controls.
- Automation and the features of automation including monitoring and control.
- Layout, configuration, and anthropometrics of workplaces and workstations and the features and equipment required for those spaces (e.g., laydown areas, access and egress, radios, phones, and hard copies of procedures and drawings).
- Workplace environment (e.g., lighting, temperature, noise).
- Provisions for routine tests and maintenance.

18-36

- Effectiveness of training materials.

The techniques for HFE V&V are described in Section 18.10.3. Application of the various techniques to different aspects of the HFE design is included in the description of the technique.

18.10.3 Methodology

The first step in verification is to identify the HSI components that are subject to verification. The HSI inventory and characterization activity describes the HSI displays, controls, and related equipment within the scope of the HSI design to be verified. HSI inventory and characterization is described in Section 18.10.3.1.

The second step in verification is the HSI task support verification (TSV) used to establish that the HSI provides the alarms, information, and control capabilities required as a result of the functional requirements analysis (FRA) and TA activities. TSV is also used to establish that the characteristics of those alarms, information, and controls conform to the requirements developed during the TA. HSI TSV is described in Section 18.10.3.2.

HFE design verification (DV) (see Section 18.10.3.3) verifies that the characteristics of the HSI and the environment in which it is used conform to the established design-

18-36

specific state-of-the-art HFE guidelines, as described in the style guide (see Section 18.7.6.1) and the industry standard practices in accordance with NUREG-0700 (Reference 1).

There are a large number of HSI components used in the U.S. EPR. Each HSI component represents at least one personnel task; therefore, a large number of events could be encountered during operation of the plant. It is neither practical nor appropriate to evaluate every scenario to confirm the adequacy and effectiveness of the HSI and establish that the performance requirements are met for each operating condition. Operational condition sampling (OCS) (see Section 18.10.3.4) is used to choose a representative set of scenarios for validation.

Performance-based tests are used to evaluate an integrated system design to determine if the HSI supports safe operations of the plant. This ISV evaluates those aspects of design that can not be assessed analytically. The goal is to test the integration of personnel and plant systems and to validate the integration of the design with personnel actions, plant response, HSIs, and procedures. ISV is performed using a high-fidelity simulator. Generally, ISV participants are operators with training and qualifications consistent with the description in Section 13.2. Multiple groups of operators are used for ISV scenarios so that results are not biased towards well-qualified crews. Details on ISV are provided in Section 18.10.3.5.

Human engineering discrepancy (HED) resolution is performed iteratively throughout the HSI design process so that issues are identified and corrected early. Some HEDs identified during verification are resolved prior to proceeding with validation of the HSI design. HEDs are not considered in isolation and, to the extent possible, their potential interactions are considered when developing and implementing solutions. More details on HED resolution are provided in Section 18.10.3.6.

The final step in verification is the design implementation activity, which confirms that the design description and documentation match the installed configuration and completes any V&V activities that could not be performed prior to installation. Any discrepancies identified at this stage are resolved by updating the appropriate documentation before the design is ready for operation. Design implementation is described in Section 18.11.

18.10.3.1 HSI Inventory and Characterization

The HSI inventory and characterization activity describes HSI components and related equipment associated with personnel tasks that are within the scope of the HSI design to be verified. The complete inventory is created by filtering certain portions of the instrumentation and controls (I&C) input/output (I/O) database which receives information from sources such as system description documents, design specifications, equipments lists, and process and instrumentation drawings. The accuracy of the inventory is confirmed by comparing it with ~~the~~similar data from predecessor designs and HSI elements described in the design specifications for the HSIs. The inventory includes aspects of the HSI that are used for interface management such as navigation and display retrieval in addition to those that control the plant.

18-36

The inventory provides an accurate and complete description of the HSI components and includes the following information:

- A unique component identification code, which includes the associated plant system and subsystem.
- Associated personnel function/subfunction.

The DV consists of comparing the characteristics of the HSI components with the design requirements. An HED is generated when an HSI component does not conform to the operational requirements as defined in the validated procedure guidelines (i.e., derived in TA), HFE design specifications, or the style guide.

HEDs are also identified for:

- Failure to meet crew-identified functionality in addition to that specified by system designers.
- Poor integration with the rest of the HSI.
- Poor integration with procedures and training.
- Failure to meet guidance in the HSI style guide and the HSI Design Implementation Plan (Reference 3).

18-36

HEDs are documented and evaluated to determine the extent of the condition. For example, if the elements of a particular display screen are not in compliance with the required color coding scheme, other similar display screens are evaluated to establish that there are no generic implications. HEDs identified during DV do not always warrant a design change; if, for example, an HSI layout is not consistent with the style guide but is consistent with the physical plant, changing the HSI layout to meet the style guide requirement could adversely effect operator acceptance of that HSI layout and lead to errors in usage. It is also possible for HFE DV to uncover limitations in the style guide requirements if the DV is well documented and reasonable designer decisions conflict with the guidance. HED resolution in this case could involve a revision to the style guide. For an explanation of the HED resolution process, see Section 18.10.3.6.

~~HFE DV is performed throughout the design process as soon as design elements such as individual screen layouts are complete. HFE DV is performed on each HSI element prior to the initial ISV.~~

18.10.3.4 Operational Conditions Sampling

The U.S. EPR has a large number of HSI components. Hundreds of personnel tasks will be encountered during operation of the plant. Sampling of the operational conditions is used to choose a representative set of scenarios for validation. There are three sampling dimensions addressed in the identification of scenarios for the ISV:

- Personnel tasks.
- Plant conditions.
- Situational factors known to challenge personnel performance.

The sample also includes error-forcing context situations specifically designed to create human errors in order to assess the error tolerance of the system and the capability of operators to recover from random errors.

18.10.3.4.4 Identification of Scenarios

When the complete set of operational condition samples is developed, the results are combined to identify a set of scenarios for ISV. The following criteria are used to fully define the scenarios to be validated.

- A given scenario identified for ISV that combines multiple characteristics of each dimension.
- A scenario defined to allow, where practicable, repetition with multiple ISV participants to establish consistency of results. The scenario definition includes, as a minimum:
  - A description of the scenario mission and any pertinent situational history necessary for operators to understand the state of the plant upon scenario startup.
  - Specific start conditions.
  - Events (e.g., failures) that will occur and their initiating condition(s).
  - Precise definition of workspace factors such as environmental conditions.
  - Communication requirements with remote personnel.
  - Crew behavior requirements.
  - Data to be collected by the ~~operators~~observers including how they were collected and where they were captured and stored.
  - Criteria required for terminating the scenario.
  - Task support needs.
  - Staffing objectives.
- The scenarios selected are not biased towards:
  - Positive outcomes.
  - ISV that is administratively easy to conduct scenarios.
  - ISV that is familiar and well-structured scenarios (i.e., textbook design basis accidents).

18-36

- Random scenario selection and sequencing is used to keep the testing unbiased. The easy scenarios are not always conducted first and testing participants get random assignments.

18.10.3.5 Integrated System Validation

ISV is a performance-based evaluation of integrated system design and human task performance to establish that the HSI is operable within performance requirements and supports safe operation of the plant. The ISV addresses the following:

- Adequacy of the entire HSI configuration for achievement of the HFE program goals.
- Confirmation of allocation of functions and the structure of tasks assigned to personnel and machine.
- Adequacy of staffing and HSI that support tasks.
- Adequacy of procedures and operating instructions.
- Validation of the dynamic aspect of HSI for task accomplishment.
- Identification of aspects of the integrated system that may negatively affect integrated system performance. (18-36)

The goals of ISV are to:

- Test the integration of personnel and plant systems.
- Validate the integration of the design with:
  - Personnel actions.
  - Plant response.
  - HSIs.
  - Procedures.

ISV is performed using a high-fidelity simulator. ISV seeks to confirm the adequacy of the HSI and the human performance assumptions, so appropriate performance measures are selected to include both HSI and human performance issues. ISV performance measurement is complex and addresses the following areas:

- Operational safety and task performance (e.g., avoidance of errors, alarm conditions, technical specification violations, response time, task completion time, and procedure compliance).
- Human error.

Section 18.9, the HFE and Control Room Design Team provides input to the training program to identify useful areas of focus for HFE V&V activities. As issues develop they are evaluated so that decisions can be made to proceed with ISV or consider design changes based on preliminary results.

18-36

~~The full-scope simulator cannot evaluate every performance shaping factor such as ambient temperature and noise. See Section 18.11 for a description of how some of the aspects of the ISV that can not be performed by simulator are validated.~~

18.10.3.5.1 Validation Team

The Validation Team for ISV is an independent, multi-discipline team which includes significant involvement of the HFE and Control Room Design Team. To minimize the potential for bias, evaluations are performed independently. The Validation Team includes personnel with expertise in test and evaluation, test design, test procedure development, performance measures, and data analysis.

18.10.3.5.2 Scope

ISV considers actions required to be performed by operators to safely operate the plant during each plant operation mode and actions required to respond to a design basis event or an ATWS condition. Before performing any evaluations, HEDs identified during previous V&V efforts are resolved or retained for consideration after the ISV operational assessment.

18.10.3.5.3 Pilot Study

A pilot study is conducted prior to validation testing. The pilot study provides an opportunity to assess the adequacy of the test design, performance measures, and data collection method. The participants who will operate~~or~~ the integrated system in the validation test will not be used in the pilot study.

18-36

18.10.3.5.4 ISV Test Objectives

Detailed test objectives are developed prior to validation testing and define a systematic approach that relates scenario characteristics and performance measurement criteria. The objectives are developed to provide evidence that the integrated system adequately supports plant personnel in the safe operation of the plant. The objectives include the following:

- Validate the role of plant personnel.
- ~~Validate that the shift staffing, assignment of tasks to crew members, and crew coordination is acceptable. This includes validation of nominal and minimal shift levels.~~

- Validate that for each human function, the design provides adequate alerting, information, control, and feedback capabilities during normal plant evolutions, transients, design basis accidents (DBA), and select risk-significant events that are beyond design basis.

- Validate that the shift staffing, assignment of tasks to crew members, and crew coordination (both within the control room as well as between the control room and local control stations and support centers) is acceptable. This includes validation of the nominal shift levels, minimal shift levels, and shift turnover.

- Validate that specific personnel tasks can be accomplished within time and performance criteria, with a high degree of operating crew situation awareness, and with acceptable workload levels that provide a balance between a minimum level of vigilance and operator burden. Validate that the operator interfaces minimize operator error and provide for error detection and recovery capability when errors occur.

- Validate that the functional requirements are met for the major HSI features such as group-view displays, alarm systems, safety parameter display system functions, general display systems, procedures, controls, communication system, and EOP-related LCSs.

- Validate that the control room operators can make effective transitions between the HSI features (e.g., group-view display, alarm systems, SICS, PICS, procedures, controls, communication systems) in the accomplishment of their task and that interface management tasks such as display configuration and navigation are not a distraction or cause undue burden.

- Validate that the integrated system performance is tolerant of failures of individual HSI features.

- Identify aspects of the integrated system (e.g., staffing, communication, and training) that may negatively impact integrated system performance.

18-36

- Validate the adequacy of the HSI configuration to achieve the HFE V&V objectives.

- Confirm that HSI task verification has been properly performed including, FRA, FA, and partial-scope TA.

- Validate the ability of the HSI to support the staff in accomplishing their tasks.

- Validate staffing goals.

- Validate the adequacy of procedures and operating instructions.

- Validate the dynamic aspect of HSI for task accomplishment.

- Validate HRA assumptions.

18-36

- Evaluate and demonstrate that systems are error-tolerant to human and system failures.
- Validate that normal and minimum staff configurations are considered.

18.10.3.5.5 Strategy

ISV is performed on a high-fidelity simulator and includes the following steps:

- Develop detailed test objectives.
- Verify that the test bed meets the requirements in 10 CFR 50.34(f)(2)(i).
- Verify that previously generated HEDs have been addressed or are tracked for further consideration.
- Select participants:
  - Test participants are qualified operators that represent plant personnel who will interact with the HSI (e.g., operators currently licensed on similar plant designs rather than training or engineering personnel).
  - Test conductors are trained and qualified in the usage of test procedures, error introduction by inaccurate testing procedures, and importance of testing documentation.
  - Normal crew configuration is present for the test (see Section 18.7.2).
  - Sample participants for the validation test are randomly chosen to avoid significant overlap with regard to:
    - Operator license and qualification.
    - Age.
    - Skill and experience.
    - General demographics.
    - Test participants:
      - Are not a part of the design organization.
      - Have not been involved in prior evaluations.
      - Were not selected based on a specific characteristic.
- Select and define scenarios from OCS.
- Develop test procedures.

- Other - HEDs that do not fit Priority 1 or Priority 2. These HEDs may not require correction.

18.10.3.6.2 HED Design Solution Development

For each HED that requires correction, a design solution is developed. The design solution follows the design process steps (i.e., OER, FRA, TA, and HSI design) from the original design. Changes to the original design may not cause deviations from design requirements.

18.10.3.6.3 HED Design Solution Evaluation

The proposed design solution is evaluated to establish that it:

- Adequately corrects the HED.
- Does not adversely impact other aspects of the design.
- Is consistent with HFE guidelines and that ISV can be conducted to evaluate its usability.

18.10.3.7 Results

Procedures and expected documentation requirements for various V&V activities are summarized in the preceding sections. A results summary report addresses the following:

- Demonstrates that V&V was performed in accordance with the prescribed process described in the V&V ~~i~~Implementation ~~p~~Plan (Reference 3).
- Demonstrates that the design conforms to the HFE design principles.
- Demonstrates that the design enables plant personnel to successfully perform ther task to achieve plant safety and other operation goals.
- Provides results of V&V activites and conclusions from those activities.

18.10.4 References

1. NUREG-0700, "Human-System Interface Design Review Guidelines," Revision 2, U.S. Nuclear Regulatory Commission, May 2002.
2. NUREG-6393, "Integrated System Validation: Methodology and Review Criteria," U.S. Nuclear Regulatory Commission, September 1995.
3. Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.

18.11 Design Implementation

Design implementation of the human factors engineering (HFE) aspects of the plant verifies that the as-built design conforms to the standard U.S. EPR design resulting from the HFE verification and validation (V&V) process. Design implementation also verifies that issues and discrepancies defined as human engineering discrepancies (HED) identified in the HFE Issues Tracking Database are addressed. V&V of the HFE program is addressed in Section 18.10.

18.11.1 Objectives and Scope

The verification associated with the design implementation process includes design of the main control room (MCR), remote shutdown station (RSS), Technical Support Center (TSC), local control stations (LCS), the human system interfaces (HSI) important to plant safety which are located within these facilities, and plant-specific procedures and training. The U.S. EPR design implementation is completed after construction is complete, but before plant startup. The implementation phase is defined by a structured plan as noted in the Quality Assurance Plan (QAP) for Design Certification of the AREVA QAP Topical Report (Reference 3) and monitored using the HFE Issues Tracking Database.

Design implementation verifies the following:

- Aspects of the design that were not verified during the V&V process.
- Modifications to the standard U.S. EPR design conform to the HFE principles and design guidance expressed in the HFE style guide and meets the HFE review criteria in NUREG-0711 (Reference 1) and NUREG-0700 (Reference 4).
- As-built HSIs, plant-specific procedures, and training conform to the design that resulted from the V&V process.
- Items in the HFE Issues Tracking Database have been adequately addressed.

Design implementation involves comparing engineering design data with documentation of the as-built design (owned by the U.S. EPR operator).

18.11.2 Methodology

Each area of design implementation is verified using a structured process. This process uses guidance from the V&V (see Section 18.10) to develop methods and verification criteria. The methods for HFE design implementation are described further in the HFE design implementation plan (Reference 5).

18-36

Design implementation relies on the accuracy of the detailed design documents resulting from the standard U.S. EPR design as well as the as-built and plant-specific documents. These documents are produced using the generic design control process as

18-36

described in Section ~~5.1~~4.4 of the ~~Human Factors Topical Report~~U.S. EPR HFE program mangement plan (Reference 2). Modifications made after the design has been verified must follow a design control process similar to that described in Reference 2 to maintain design documentation accuracy.

The HFE Issues Tracking Database is used throughout the process to capture, track, and address HEDs found during design implementation. Each HED follows the same resolution process as outlined for V&V (see Section 18.10). If an HED requires a design change, the AREVA NP design control process is used. When the design change has been implemented, verified, validated, and documented, the HED is closed. If an HED does not require a design change, the HED may be closed with sufficient documented evidence for that decision. HFE-related modifications by U.S. EPR owners after the design is complete are governed by a human performance monitoring (HPM) program similar to that described in Section 18.12.

18.11.2.1 Aspects of the Design Not Verified During the V&V Process

Design implementation addresses features of the design that are not verifiable using a full-scope simulator (e.g., control room lighting, communication systems, background noise levels, ventilation and climate control). Verification that these features conform to the design that resulted from the V&V process is confirmed by matching the design requirements to the actual as-built design documentation.

Other aspects that are not verified during V&V include customer-specific modifications made to the standard U.S. EPR design. These modifications are verified for conformance to the design that resulted from the V&V process. This is accomplished by comparing the HFE aspects of the modification documentation to the standard HFE design documentation.

18.11.2.2 Verification of the As-Built HSIs

A review and audit of the as-built documentation is performed to verify conformance of the as-built design to the standard design resulting from the V&V process. This verification confirms that the as-built documentation is current for the plant, that it conforms to the design requirements, and that it matches the design documentation.

18.11.3 Verification of the Plant-Specific Procedures and Training

AREVA NP supplies guidance for developing procedures and training. Verification that the plant-specific procedures and training are developed using that guidance and that they conform to the design resulting from the V&V effort is performed as described in Section 18.10.

18.11.3.1 Verification that HFE Issues Tracking Database Items Have Been Addressed

This verification process confirms that HEDs being tracked are adequately addressed. This is accomplished by reviewing the database, verifying that HEDs have been addressed, and addressing any remaining HEDs as necessary. In some cases, there are HEDs that require a design change, but are not implemented by the time design implementation is finished and closed. Those HEDs are turned over to the U.S. EPR operator for implementation or closure at a later date.

18.11.4 Results Summary

Throughout the design implementation, the HFE Issues Tracking Database is updated as new HEDs are discovered during the process. Resolution for these HEDs is also updated in the HFE Issues Tracking Database. A results summary report is generated detailing the status of HEDs tracked including any that remain unresolved and concludes HFE issues have been adequately addressed. The results summary report concludes the design implementation was performed in accordance with the prescribed process for validating that the as built design conforms to the standard design resulting from the HFE V&V process. Also included are the methods and criteria used during the design implementation process and the results of the verification. This report becomes part of the final design documentation owned by the U.S. EPR operator.

18.11.5 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," U.S. Nuclear Regulatory Commission, 1994.

2. ~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc, January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

3. ANP-10266A, Revision 1, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR," AREVA NP Inc., April 2007.

4. NUREG-0700, "Human-System Interface Design Review Guidelines," Revision 2, U.S. Nuclear Regulatory Commission, May 2002.

5. Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.

18-36

Next File

18.12 Human Performance Monitoring

Monitoring human performance is performed throughout the life of the plant so that:

- The results of the integrated system validation are maintained.
- Operator performance does not degrade over time.
- Issues discovered by operating and maintenance personnel are noted, tracked, and corrected before plant safety is compromised.
- Changes made to the design do not result in a degradation of human performance.

The U.S. EPR human performance monitoring (HPM) strategy, as described in the HPM Implementation Plan (Reference 3), provides a method to accomplish this goal. A COL applicant that references the U.S. EPR design certification will implement an HPM program similar to that which is described in this section.

18.12.1 Objectives and Scope

The objectives for HPM are:

18-36

- To confirm that the design can be effectively used by personnel.
- To confirm that human actions (HA) are accomplished within an acceptable time and meet performance criteria.
- To confirm that design changes do not adversely affect personnel performance.
- To confirm that the acceptable level of performance established during the integrated system validation remains valid.
- To detect degrading human performance before plant safety is compromised.
- To confirm identified errors in the design are resolved in a timely manner.

To verify that the objectives are met, HPM is conducted in areas of the plant requiring HAs, including:

- Main control room (MCR).
- Remote shutdown station (RSS).
- Technical support center (TSC).
- Local control stations (LCS) important to plant safety.

Operation, testing, and maintenance actions during each plant mode are also monitored for human performance.

against the existing trend of human performance to determine if the performance was degraded by the design change.

Any degradation in performance resulting from the design change is entered into the corrective action program to be analyzed for possible areas of improvement and used as input to human performance trending. Significant impacts to human performance require that the design change be modified. If no degradation in performance is observed, the design is implemented and results of the HPM are entered into the current trend.

When an approved design change has been implemented into the plant, performance is observed and users are interviewed. Interviews with users are performed to determine any operator workarounds, HSI inefficiencies, or design errors that resulted from the design change. Interview questions are centered on tasks that have been affected by the design change. Particular attention is given to user actions during their initial use of the new design to note any adverse affect on performance, confirm the design change is performing its intended function, and to view any operator workarounds. The significance of the design change impact determines the amount of monitoring effort required.

18.12.2.5 Operational Focus Index

An operational focus index is used to trend performance of operator's day to day activities. Indicators are used to exhibit the level of performance and risk associated with different operational activities. The level of the indicator is based on operator performance for that activity (e.g., Red = Bad, Yellow = Caution, Normal = White, and Green = Good).

Operational activities include:

- Operator workarounds.
- Operator burdens.
- Control room correctives.
- Control room annunciations.
- Worker and maintenance tagouts greater than 90 days.
- Caution tagout greater than 90 days.
- Active fire protection impairment due to problem component.
- Corrective maintenance inventory.
- Plant elective maintenance inventory.

18-36

- Temporary modifications.

Indicators are updated periodically with a rolling average used to show trend. Adverse trends are entered into the corrective action program. Further analysis (e.g., root cause or operator interviews) may be required to understand the adverse trend and identify effective corrective actions.

18.12.2.6 Probabilistic Risk Assessment

Probabilistic risk assessment (PRA) models are used when plant or personnel performance can not be simulated, monitored, or measured. Performance data from modeled risk-significant HAs are used to evaluate the risk of the proposed design change on human performance during different operation modes. The U.S. EPR operator maintains the PRA model. After a design change, the PRA model is updated to reflect the new design.

18.12.2.7 Overall Design Control Process

18-36

A design control process described in Section ~~5~~4.5.1 of the ~~Human Factors Topical Report~~U.S. EPR HFE Program Management Plan (Reference 2) controls the design, design changes, design verification, and analysis activities. A similar process is used by the U.S. EPR operator to control design changes. The process confirms that changes made to the design are adequate and accomplish the goal of the design change. The process also confirms that the design change does not result in adverse effects on personnel performance.

A substantial HSI design change is simulated on the simulator. Evaluation of human performance determines the anticipated impact of the design change, verifies that the performance level has been maintained, and verifies that the design change can be effectively used by personnel. If the design change demonstrates performance enhancements and does not show an adverse impact, it may be implemented into the plant.

18.12.2.8 Existing Plant Programs

Additional plant programs are used to support human performance. Barriers, including the inservice inspection and inservice testing program and the maintenance rule, are used to prevent a negative impact on human performance. To maintain acceptable human performance, structures, systems, and components (SSC) must be maintained in proper working order. Routine testing and inspection of SSC is performed so that deficiencies are corrected before the SSC become ineffective or inoperable.

Operators require proper notification when an SSC is out of commission for maintenance or repair in order to maintain sufficient human performance. Use of an

inoperable SSC could potentially be tracked as an error in human performance and indicate a false trend.

18.12.3 Results Summary

HPM is continued throughout the life of the plant. Reports summarizing human performance-related issues, resolution of those issues, implementation status, and operating experience results are maintained for trending purposes. Operating conditions determine the necessary frequency of these summary reports.

A U.S. EPR operator shall maintain an HPM program which meets the intent given in this section. Documentation of HPM summarizes the following:

- Baseline human performance criteria established during V&V.
- HPM implementation strategy.
- Any trends in human performance.
- Operator focus index.
- Human performance-related issues, resolution, implementation status, and operating results.
- Specific human performance issues that can be applied to the standard U.S. EPR plant.

18.12.4 References

1. NUREG-0711, "Human Factors Engineering Program Review Model," U.S. Nuclear Regulatory Commission, 2004.

18-36

2. ~~ANP-10279, Revision 0, "U.S. EPR Human Factors Engineering Program," AREVA NP Inc, January 2007.~~Letter, Sandra M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 240, Supplement 1," NRC:09:080, July 31, 2009.

3. Letter, Sandra. M. Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Response to U.S. EPR Design Certification Application RAI No. 171, Supplement 1," NRC:09:019, March 13, 2009.