## 18.7 Human System Interface Design

The human system interface (HSI) design process translates function and task requirements into HSI characteristics and functions. The HSI uses a structured methodology that guides designers in identifying and selecting candidate HSI approaches, defining the detailed design, and performing HSI tests and evaluations. The HSI promotes the development and use of human factors engineering (HFE) guidelines that are tailored to the unique aspects of the design (e.g., an HSI style guide that defines design-specific conventions). The HSI also promotes standardization and consistency in applying HFE principles. The process and the rationale for the HSI design is documented and controlled under the design control process described in the AREVA Quality Assurance Program (QAP) Topical Report (Reference 1).

This section describes how HFE activities and analyses described in Sections 18.2, 18.3, 18.4, 18.5, and 18.6 are performed as part of the overall HSI design process.

### 18.7.1 Human System Interface Design Inputs

The HSI design is developed based on various design inputs. The HFE program element design inputs (i.e., operating experience review (OER), functional requirements analysis (FRA) and functional allocation (FA), task analysis (TA) human reliability analysis (HRA), and staffing analysis) are used by the HSI design team to make design decisions. Additionally, the HSI design team considers applicable regulatory documents and codes as well as generic HFE standards and industry guidelines.

#### 18.7.1.1 Analysis of Personnel Task Requirements

Several analyses are performed in the early stages of the design process to identify HSI design requirements.

##### 18.7.1.1.1 Operating Experience Review

An OER is performed as described in Section 18.2 to identify any HFE-related safety issues as well as any positive HFE experiences with HSIs and control rooms. The goal of the OER is to compare the analysis of current work practices, operational problems and issues in current designs, and industry experience with candidate technological approaches to system and HSI technology and specific supplier solutions.

At the onset of OER activities, the first HFE task is to identify how candidate functions, tasks, and HSIs are different from predecessor designs. Plant specific and industry experience is sought from a variety of data sources, including: available operating experience databases (documentation), interviews, talkthroughs and walkthroughs with personnel, and interactions with other facilities and organizations.

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 3.3 of the U.S. EPR Human Factors Operating Experience Review Implementation Plan (Reference 14) describes how OER information is screened. 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 U.S. EPR Human System Interface Design Implementation Plan (Reference 15) 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.

#### 18.7.1.1.2 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 16). 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 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 either require review by the design review board or are subject to other design change control processes.

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) are identified. 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 use the information.

#### 18.7.1.1.4 Staffing and Qualifications and Job Analysis

As described in Section 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. 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

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 4.5.1 of the U.S. 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.

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 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 a minimum of two steps to perform an action once the active control window is opened. The first step requires taking the active control window from the automatic or blocked mode and putting it into manual mode. Typically this would require selecting two separate icons on the control window. The second step selects the type of action (e.g., close or throttle valve, stop pump). This step requires selection of a second icon to confirm and execute the action for non-throttling control actions.

Dedicated displays capable of receiving all four trains of data are used to give the operator an overview of the plant on the SICS. The dedicated overview displays are

for monitoring only, with one way communication, and cannot impact the plant. See Section 7.1.1.3.1 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.

#### 18.7.1.2.2 Loss of Non-Safety Computerized HSIs

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 displays and selected hardwired controls and alarms.

SICS is safety-related and is designed and qualified in accordance with IEEE Class 1E standards. The PICS is a non-safety-related system. The main difference between achieving safe shutdown from the different HSI systems is that more non-safety-related plant equipment can be operated from the PICS. The SICS includes the basic functional capabilities for the operator to monitor plant conditions and control appropriate plant systems to perform the credited safe shutdown path. However, more flexibility in the path to safe shutdown is available from the PICS due to the increase in HSI for both safety-related and non-safety-related systems.

Failures in PAS will be indicated on PICS. PAS failures resulting in the unavailability of the PICS need not be distinguished from failures in PICS resulting in the unavailability of PICS. The PICS will be used in all plant conditions, as long as it is available. The PICS is declared unavailable if less than two of the four operator workstations are in an available condition. A PICS workstation is declared unavailable if one or more of the following conditions exist:

- Three or more monitors at a workstation are unusable. The workstation in the Shift Manager office is not considered an operator workstation.
- Data communication is not working satisfactorily (i.e., expected feedback not received in the expected timeframe or inputs do not respond in the expected manner).

- Correlating information on PICS displays at the different workstations is not consistent.

- Information on PICS displays and relevant SICS indications are not consistent (i.e., data on PICS differs significantly from data on SICS).

Operators will respond to these issues by procedure and training and will also be alerted to perform the above verifications by the features on PICS that:

- Inform an operator through alarms or status indicators when individual or multiple data is not valid.

- Inform an operator through alarms or status indicators that critical I&C hardware is not working properly.

- Inform an operator through alarms or status indicators when system logic has not produced the expected results.

The PICS is normally used by the operator to monitor and control process systems, and SICS is used in the unlikely event that the PICS is not available and to perform some of the safety-related permissives and resets. During normal operating conditions, the status of plant operation is displayed on both the PICS and SICS, which allows for verification that the information displayed is consistent.

There are two mechanisms that prompt a manual comparison of PICS and SICS to verify consistency.

- A periodic verification will be performed as part of normal operating procedures to verify consistency between PICS and SICS.

- If, while performing operations from PICS, an operator detects a potential error in data displayed by PICS, the operator will perform a comparison of data between PICS and SICS. This comparison will be performed by employing the same procedure used for periodic verification of consistency. If an acceptable deviation value is exceeded, then operators will discontinue use of the PICS and a transfer to SICS will be initiated. The acceptable deviation value is specified in the procedure.

The PICS also has status indication to assist the operators in determining availability. 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

plant in a safe condition. If a DAS function initiates a plant shutdown, an alarm annunciates in the control room to alert the operators that manual actions may be necessary. The SICS provides the HSI for DAS.

#### 18.7.1.3 Regulatory Requirements

The HSIs are designed to meet the following regulatory requirements as described in Chapter 7.

##### 18.7.1.3.1 10 CFR 50.34(f)(2)(i) - Simulator

The U.S. EPR MCR is modeled by a simulator which provides the capability to simulate a small break loss of cooling accident. The simulator is a close replica of the U.S. EPR MCR and includes the equipment and functionality of the U.S. EPR HSI.

##### 18.7.1.3.2 10 CFR 50.34(f)(2)(iii) - State-of-the-Art Human Factors Principles

The U.S. EPR HSIs are designed using state-of-the-art human factors principles. The HFE style guide provides human factors principles which are applied consistently throughout the U.S. EPR design process.

##### 18.7.1.3.3 10 CFR 50.34(f)(2)(iv) - Safety Parameter Display System

The U.S. EPR HSIs meet the requirements for a safety parameter display system (SPDS) as required by NUREG-0696 (Reference 11). The parameters required to be displayed as part of the SPDS are made available on the PICS and SICS in the MCR, the Technical Support Center (TSC), and the Emergency Operations Facility. The guidance provided by NUREG-0835 and NUREG-1342 is considered when designing the SPDS and HSI. See Section 7.5 for more details.

##### 18.7.1.3.4 10 CFR 50.34(f)(2)(v) - Bypassed and Inoperable Status

The U.S. EPR HSIs provide indication to the operator with regards to bypassed and operable status of safety-related systems. This indication is provided on the PICS. See Section 7.5 for more details.

##### 18.7.1.3.5 10 CFR 50.34(f)(2)(vi) - High Point Venting

Control of the high point venting of non-condensable gases from the reactor coolant system (RCS) is provided in the MCR. This capability is provided on both PICS and SICS.

##### 18.7.1.3.6 10 CFR 50.34(f)(2)(xi) - Relief and Safety Valve Indication

The position of the pressurizer (PZR) safety relief valve and the main steam safety relief valve is indicated in the MCR. Both indication and alarm are provided on the PICS and the SICS. See Section 7.5 for more details.

#### 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

The remote shutdown station (RSS) inventory consists of PICS and SICS. The HSI in the RSS provides for the 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.

For further information on the U.S. EPR QAP, refer to Chapter 17.

#### 18.7.1.3.13 Regulatory Guide 1.22

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance from RG 1.22. The measures for continuous self testing and periodic testing of the PS actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

#### 18.7.1.3.14 Regulatory Guide 1.47

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance from RG 1.47. The PICS automatically indicates the bypassed and inoperable status of the safety-related I&C systems and safety-related process systems in the MCR. The bypassed and inoperable status of electrical auxiliary support features are described in Section 8.3.

#### 18.7.1.3.15 Regulatory Guide 1.62

The U.S. EPR HSIs permit manual initiation of protective actions which include initiation of a reactor trip and engineered safety feature actuation system (ESFAS) safety functions. For more information on reactor trip manual functions, refer to Section 7.2. For more information on ESFAS functions, refer to Section 7.3. For more information on diverse safety functions, refer to Section 7.8.

#### 18.7.1.3.16 Regulatory Guide 1.97

Plant parameters are available to the operator on both PICS and SICS. Plant parameters required for plant status identification (i.e., Type A and B variables) are continually displayed to the operator during an accident response as described in IEEE Std 497-2002 (see Section 18.7.4.4). For more details on I&C requirements related to this RG, refer to Section 7.5.

#### 18.7.1.3.17 Regulatory Guide 1.105

See Section 7.1.3.4.9.

#### 18.7.1.3.18 NUREG-0696

The U.S. EPR design includes emergency response facilities similar to those described in NUREG-0696. When activated, the emergency response facilities provide SPDS information to various outside monitoring agencies. The integration of these facilities is independently verified prior to power operation.

#### 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 2.2.2.1 of the EPR HFE Program Management Plan (Reference 2).

### 18.7.2.2 Roles and Responsibilities of Crew Members

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 manager (SM) 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.

### 18.7.2.3 Personnel Supervision of Plant Automation

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 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. The U.S. EPR Human System Interface Design Implementation Plan (Reference 15) 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 computer-based procedures (CBP), and during emergency or accident scenarios is described in Section 2.2.2.2 of the EPR HFE Program Management Plan (Reference 2).

### 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.

Communication of orders for plant operation is initiated using a chain of command structure. For example, the 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 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 repeat-backs to confirm the accuracy of the message. Several forms of two-way communication are provided within the MCR of which the plant operators are trained.

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, RSS, or I&CSC. Permission from the CRS or responsible licensed operator is also required to enter these control rooms.

#### TSC and RSS

The RSS is generally not occupied except in the event of an MCR evacuation. Electronic measures are used to restrict access to the RSS to only authorized personnel. Access to the RSS will be in accordance with the emergency plan.

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

As described in Section 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, CBP, 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, Section 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 15).

#### 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 2.2 of the EPR HFE Program Management Plan (Reference 2).

### 18.7.4.3 Inventory of Alarms, Displays, and Controls

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. These design documents are then used as inputs to the FRA and TA processes.

Through the FRA/FA and TA processes, the required inventory of alarms, displays, and controls are identified and documented. The U.S. EPR Human System Interface Design Implementation Plan (Reference 15) 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 Alarms, Displays, and Controls

Minimum inventory is defined as the 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.
- 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 methodology for selecting the minimum inventory is described in the U.S. EPR Human System Interface Design Implementation Plan (Reference 15) and includes a description of:

- The selection criteria.
- How the functions and tasks that need to be supported by the minimum inventory are identified.
- The technical requirements that apply to the design of the 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.
- The criteria that are used to determine which components need to be spatially dedicated, continuously visible or accessible by taking only one action (i.e., MCR design and concept of operations).

### 18.7.4.5 Remote Shutdown Station 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 HSIs in the RSS.

The minimum inventory of alarms, displays, and controls in the RSS 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.

The methodology for selecting the minimum inventory for the RSS is described in the U.S. EPR HSI Design Implementation Plan (Reference 15).

#### 18.7.4.6 Computer-Based Procedures

Operating procedures can be implemented in a screen-based format on the Process Information and Control System (PICS) that provides access to process information by direct links. These computer based procedures (CBP) also provide access to related information and direct the operator to the appropriate control screens. Refer to Section 6.2.9 of the U.S. EPR Human Factors Program Management Plan (Reference 2) for further details on the development of CBPs.

Safety Information and Control System (SICS) paper-based procedures are provided in the control rooms in the event that a failure of the PICS occurs. Paper-based procedures contain similar guidance and format as the CBPs. Paper-based operating procedures are provided in the main control room (MCR), remote shutdown station (RSS), and the Technical Support Center (TSC). Aside from differences in how CBPs and paper-based procedures are used (e.g., the navigation and layout) as well as the availability of live data, paper-based procedures shall be as consistent to the CBPs as possible. Adequate space is provided in close vicinity to the workstations in the MCR and RSS for operators to lay out paper-based procedures, when required.

### 18.7.5 Guidance for Local Control Station Design

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.

#### 18.7.5.1 Plant Layout Design and Equipment Accessibility

System engineers specify space requirements for their equipment during the plant layout phase taking into account maintenance, testing, and component replacement. The HFE style guide provides guidance for these space requirements. Location of interfaces also considers the general physical layout of the system. LCSs (local control stations) are placed in easy to access locations (e.g., manual valve operators will not be located where access requires the use of a portable ladder or scaffold).

#### 18.7.5.2 Coding, Language, and Information Presentation

Rules for coding, labeling, and presenting information on HSIs, local control stations, and on most equipment are specified in the LCS style guide. The nomenclature and

terminology used in operating procedures and design documentation (e.g., system manuals and plant drawings) shall be consistent with those used for operator interfaces.

Unique equipment identifiers shall be established in the equipment database early in the design phase, and those identifiers shall be maintained throughout the design, manufacture, construction, testing, procedure development, and operational staff training. In conformance with NUREG-0711 (Reference 4) and consistent with NUREG-0700 (Reference 6), the LCS style guide specifies requirements for the use of symbols, abbreviations, syntax, and color schemes.

### 18.7.5.3 Lighting of the Control Rooms and Workspaces

The lighting in the control rooms and workstations, including local control stations, provides suitable working conditions for personnel by:

- Providing adequate lighting for performance of their tasks (e.g., good contrast for easy discrimination of required information, good minimum lighting level for the preservation of alertness).
- Avoiding glare and reflection.

### 18.7.5.4 Acoustic Environment

The acoustic environment and the mean noise level in the MCR and RSS aids operator alertness so that the monitoring and controlling of processes and the associated mental activities are performed in comfort, and communication between the members of the operating staff is not disrupted.

### 18.7.5.5 Personnel Protection Equipment

Though the use of personnel protection equipment such as hearing, eye, and head protection, anticontamination clothing, and self-contained air breathing apparatus is not postulated in the MCR; it is placed in locations providing easy access. The placement of this equipment is considered in the plant layout design.

### 18.7.5.6 Ambient Conditions

During normal operation at basic atmospheric conditions, the temperature and humidity in the MCR and associated control rooms are controlled to normal comfort levels. During some design basis events, the temperature in the MCR may exceed comfort levels, but the control room air conditioning system maintains temperature and humidity within the range specified in Section 9.4.

## 18.7.6 HSI Detailed Design and Integration

### 18.7.6.1 HSI Style Guide

An HSI style guide is used in the design of the HSI features, layout, and environment. The style guide supports the interpretation and comprehension of design guidance and helps to maintain consistency in the design across the HSIs. The primary topics addressed by the style guide include:

- Data presentation.
- Screen-based data presentation, hierarchy, and navigation.
- Presentation and operation of controls.
- Presentation and interpretation of alarms.

#### 18.7.6.1.1 Information Presentation

The HSI style guide specifies rules for the arrangement of information on screens and conventional control boards and for coding and labeling of information of different types of HSIs. The style guide promotes consistency between nomenclature and terminology used in operating procedures and those used on operator interfaces. Also, if screen elements are derived from design documentation in a structured manner, the style guide creates consistency between HSIs and plant documentation.

#### 18.7.6.1.2 Screen-Based Information Presentation, Hierarchy, and Navigation

Operators are provided with an overview of the plant state and immediate access to specific information and specific controls. This is accomplished by grouping the indicators, alarms and status displays in functional groupings which provide clear, plant design-driven relationships or links between associated indicators and controls. For screen-based controls, the organizational hierarchy of operating displays and navigation methods accounts for the limitations of display areas and the serial character of information access to provide an overall vision of the plant state as well as access to details.

Design goals for the presentation format of information include:

- Allow operators to evaluate the priority, gravity, and impact on safety and availability of an event in the context of overall plant state.
- Direct the operators to the information and controls that are needed to plan and execute any necessary action(s) repeatedly.
- Guide the operator from summary information (e.g., from a fault flag or an alarm) to the detailed fault information (e.g., circuit diagrams) or to the associated procedure or alarm sheet.

- Reduce HSI display screen complexity (i.e., complex P&ID system functions) with more information-rich function oriented displays.

The organization of the display hierarchy reflects logic based on task requirements so as to be readily understood by the operators. The HSI screens used for control and indication are organized in a hierarchical structure and the design guidance found in the style guide provides consistency for navigation techniques applied. The following criteria apply to the design of the hierarchy for screen-based HSIs:

- The information hierarchy at the top levels contains a few overview displays showing essential plant state information while the lower level displays progress through increasing levels of detail.

- Multiple monitors and windowing capability within monitors allow several different types and levels of information to be displayed simultaneously.

- Task-oriented presentation of the same information is displayed in different arrangements to adapt to various operator processes.

- Calculated, preprocessed, and condensed information is used for immediate understanding of the state of a complex system (e.g., core average axial power shape monitoring, departure from nucleate boiling ratio and critical heat flux monitoring, plant calorimetric calculation, saturation temperature, saturation pressure, and curves and limits for heat up and cool down).

Screen navigation refers to the operation of finding, within the screen hierarchy, the correct display for the information or control capability being sought. The most common navigation method involves selecting a new display to open and windowing it over the old one on the active monitor. This is done with menus or display-to-display navigation buttons.

To ease navigation, each display is labeled with a unique title and identification number which indicates its relationship in the hierarchy. This helps the operator stay oriented within the hierarchy, increases the efficiency of navigation, and improves operator situational awareness.

An identification system for power stations, is used to assign codes to structures, systems and components for the U.S. EPR. Coding is used for labeling on screen-based and hardwired HSI applications as well as throughout the plant.

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 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, 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.
- Display formats and elements.
- Use of the alarm system.
- Use of the operating procedure system.
- User interface interaction and management:
  - Display management.
  - Display hierarchy.

  - Navigating between displays.

- Workstation configuration:
  - Anthropometric data for equipment dimensions.
- Workplace environment:
  - Temperature and humidity.
  - Ventilation.
  - Illumination.
  - Sound levels.

The HSI design takes into account the use of HSIs over the duration of a shift where decrements in human performance due to fatigue may occur. Physical layout of the control room and workstations considers the distances operators are required to move to initiate manual actions. Excessive amounts of movement, including arm and hand movement, for long durations can impact the performance of the operator.

#### 18.7.6.3 HSI Modifications

As described in Section 18.12, HSI modifications should be consistent with the U.S. EPR utility operator's existing strategies for gathering and processing information and executing actions identified in the TA. Consistency reduces the need for retraining associated with a lack of proficiency because of modifications. Modifications to the HSIs should be done in accordance with the design change process of the operating utility. A check list of HSI technical considerations should be included in the design change work package for consistency with the U.S. EPR HSI standard design.

### 18.7.7 HSI Verification and Validation (Tests and Evaluations)

Verification and validation (V&V) (see Section 18.10) of the HSI design is performed so that the as-built HSIs:

- 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 the U.S. EPR Human Factors Verification and Validation Implementation Plan (Reference 17).

### 18.7.8 HSI Design Results and Documentation

As described in Section 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


1. ANP-10266, Revision 4, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR," AREVA NP Inc., December 2012.

2. [*ANP-10327P, Revision 0, "U.S. EPR HFE Program Management Plan Technical Report," AREVA NP Inc., April 2013.*]*

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-10304, Revision 6, "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," AREVA NP Inc., May 2013.

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.

14. [*U.S. EPR Human Factors Operating Experience Review Implementation Plan, AREVA NP Inc., 2010.*

15. *ANP-10328P, Revision 0, "U.S. EPR Human System Interface Design Implementation Plan Technical Report," AREVA NP Inc., April 2013.*

16. *U.S. EPR Functional Requirements Analysis and Functional Allocation Implementation Plan, AREVA NP Inc., 2010.*

17. *U.S. EPR Human Factors Verification and Validation Implementation Plan, AREVA NP Inc., 2011.*]*

Next File