AREVA

U.S. EPR HFE Program Management Plan

ANP-10327NP
Revision 0

Technical Report

April 2013

AREVA NP Inc.

(c) 2013 AREVA NP Inc.

Copyright © 2013

AREVA NP Inc.
All Rights Reserved

Nature of Changes

Item	Section(s) or Page(s)	Description and Justification
0	All	Initial Issue

Contents

List of Figures

1.0 INTRODUCTION

1.1 *Applicability*

This Human Factors Engineering (HFE) Program Management Plan applies to the U.S. EPR™ design activities.

1.2 *Owner*

HFE Responsible Technical Manager (RTM) is responsible for providing this plan.

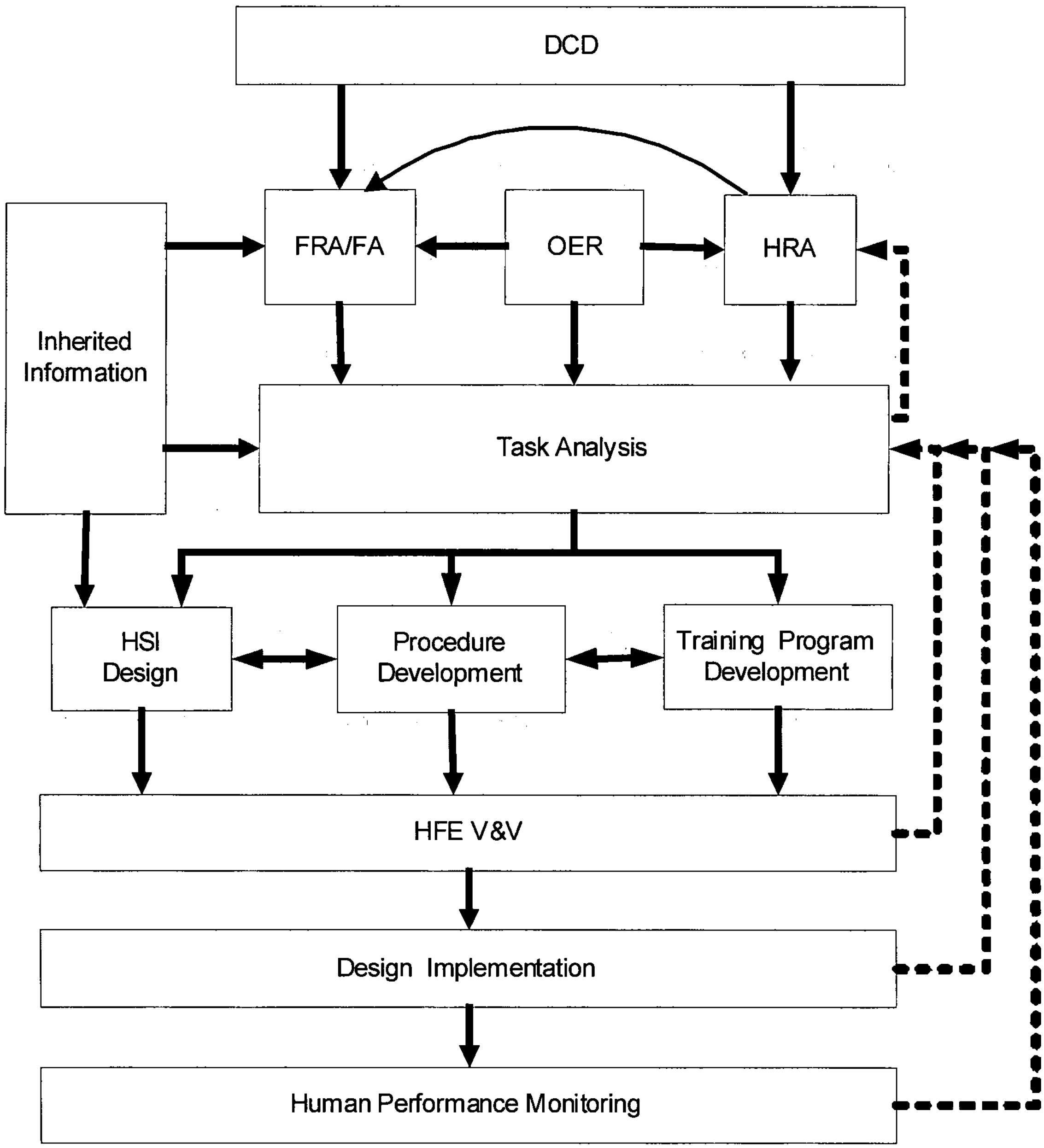
1.3 *Purpose*

The purpose of this plan is to provide guidance to the development, execution, oversight, and documentation of the HFE program.

1.4 *Objectives and Scope*

HFE Program Management coordinates the elements of the HFE program. The HFE program directs an HFE design team with the responsibility, authority, placement within the organization, and composition to verify that the design commitment to HFE is met. The HFE team is guided by this plan to provide reasonable assurance that the HFE program is properly developed, executed, overseen, and documented. This plan describes the technical program elements verifying that all aspects of the HSI are developed, designed, evaluated, and verified on the basis of accepted HFE principles. In addition, the HFE program as a whole appropriately considers and addresses the deterministic aspects of design, as discussed in RG 1.174 (Reference 1). The HFE process and sequence is shown in Figure 1-1 below.

Figure 1-1: HFE Process



1.5 *Definition of Terms*

Term	Definition
Design Certification Document (DCD)	Design document which is part of the licensing basis for the U.S. EPR.
ECS	EDF Coding System – Plant breakdown and identification system.
Flamanville 3 (FA3)	EPR nuclear reactor; currently being built in France.
Functional Requirements Analysis (FRA)	The examination of system goals to determine what functions are needed to achieve them.
Function Allocation (FA)	The process of assigning responsibility for function accomplishment to human or machine resources, or to a combination of human and machine resources.
Human System Interface (HSI)	A human-system interface (HSI) is that part of the system through which personnel interact to perform their functions and tasks. In this document, "system" refers to a nuclear power plant. Major HSIs include alarms, information displays, controls, and procedures.
Human Reliability Analysis (HRA)	Evaluation of the potential for, and mechanisms of, human error that may affect plant safety.
Olkiluoto 3 (OL3)	EPR nuclear reactor; currently being built in Finland.
Operating Experience Review (OER)	A review of relevant history from the plant's on-going collection, analysis, and documentation of operating experiences and from interviews with plant staff.
Precursor Plant	A precursor plant is defined as the large 4-loop nuclear plants from with the EPR design evolved such as the French N4 plants and the German Konvoi plants.
Predecessor Plant	A predecessor plant is defined as the EPR designs (Olkiluoto 3 and Flamanville 3) whose conceptual design was complete prior to the beginning of the U.S. EPR design and are also considered sources of operating experience.
Probabilistic Risk Assessment (PRA)	A systematic evaluation which demonstrates that the design poses acceptably low risk of core damage accidents and consequences.
Process Information and Control System (PICS)	The non-safety-related I&C system that provides the human-system interface (HSI) to control and monitor the plant during all modes of operation.

Term	Definition
Safety Information and Control System (SICS)	The SICS is provided as a safety-related HSI and is specifically designed to provide the operator the necessary inventory and indications for the following: • Mitigation of anticipated operational occurrences (MCR). • Mitigation of postulated accidents (MCR). • Reach and maintain safe shutdown (MCR and RSS). • Mitigation of anticipated operation occurences concurrent with a CCF of the PS (MCR). • Mitigation of postulated accidents concurrent with a CCF of the PS (MCR). • Mitigation of severe accidents (MCR).
Task Analysis (TA)	A method for describing what plant personnel must do to achieve the purposes or goal of their tasks. The description can be in terms of cognitive activities, actions, and supporting equipment.

1.6 *Abbreviations and Acronyms*

This is the master list for all of the Human Factors Engineering program element implementation plans. Not all of these abbreviations and acronyms are used in any one implementation plan, which includes this program management plan. In order to create a higher consistency within the plans, certain terms are defined with possible different industry interpretations held within brackets or parenthesis. Only the term that is defined should be used.

Acronym	Definition
ALO	Additional Licensed Operator
AOO	Anticipated Operational Occurrence
AOP	Abnormal Operating Procedure
ARP	Alarm Response Procedure
ASHRAE	American Society of Heating, Refrigerating and Air-Conditioning Engineers
ATWS	Anticipated Transient Without Scram
BWR	Boiling Water Reactor
CAP	Corrective Action Program
CBP	Computer-Based Procedures
CDF	Core Damage Frequency

Acronym	Definition
CNV I&C	Conventional Instrumentation and Control
COL	Combined License
COO	Concept Of Operations
CR	Control Room
CRS	Control Room Supervisor
DCD	Design Certification Document
DCS	Digital Control System
DRB	Design Review Board
DV	Design Verification
EDF	Electricity De France
EDL	Engineering Discipline Lead
EOF	Emergency Operations Facility
EOP	Emergency Operating Procedure
EPG	Emergency Procedure Guideline
FA	Function Allocation (Allocation of Function (AOF))
FA3	Flamanville-3 Nuclear Power Plant
FBT	Functional Branch Tree
FRA	Functional Requirements Analysis
FSAR	Final Safety Analysis Report
FSS	Full Scope Simulator
GA	Gap Analysis
HA	Human Action
HED	Human Engineering Discrepancies
HEP	Human Error Probability
HFE	Human Factors Engineering
HITS	Human Factors Engineering Issue Tracking System (HFEITS)
HPM	Human Performance Monitoring
HSI	Human System Interface
HRA	Human Reliability Analysis
HVAC	Heating, Ventilation, and Air Conditioning
I&C	Instrumentation and Control
I&CSC	I&C Service Center
ISV	Integrated System Verification
LCS	Local Control Stations (Local Control Center (LCC))

Acronym	Definition
LOCA	Loss of Coolant Accident
LRF	Large Release Frequency
MCR	Main Control Room
NLO	Non-Licensed Operator (Equipment Operator (EO); Utility Operator (UO))
OCS	Operational Conditions Sampling
OER	Operating Experience Review
OL3	Olkiluoto-3 Nuclear Power Plant
OWP	Operator Work Place
P&ID	Piping and Instrumentation Diagram
PACS	Priority Actuator Control System
PAS	Process Automation System
PBP	Paper-Based Procedure
PICS	Process Information and Control System
P&ID	Process and Instrumentation and Display
POP	Plant Overview Panel (Wide Display Panel (WDP); Group View Display (GVD))
PRA	Probabilistic Risk Assessment
PS	Protection System
PSF	Performance Shaping Factor
PTRD	Plant Technical Requirements Document
PWR	Pressurized Water Reactor
QA	Quality Assurance
QAP	Quality Assurance Program
RCSL	Reactor Control Surveillance & Limitation System
RMS	Records Management System
RO	Reactor Operator
RSS	Remote Shutdown Station (Remote Shutdown Panel (RSP); Auxiliary Control Room (ACR))
RTM	Responsible Technical Manager
SAMG	Severe Accident Management Guidelines
SAS	Safety Automation System
SAT	Systematic Approach to Training
SDD	System Description Document
SDRD	System Design Requirements Document

Acronym	Definition
SFGA	System Function Gap Analysis
SFRA	System Functional Requirements Analysis
SGTR	Steam Generator Tube Rupture
SICS	Safety Information and Control System
SM	Shift Manager
SRO	Senior Reactor Operator
SSC	Systems, Structures, and Components
SSE	Safe Shutdown Earthquake
STA	Shift Technical Advisor
TA	Task Analysis
TS	Technical Specification
TSC	Technical Support Center
V&V	Verification and Validation

2.0 GENERAL HFE PROGRAM GOALS AND SCOPE

The HFE program provides oversight of the design of the human-system interface (HSI) as well as the layout of the control rooms to verify that state-of-the art human-factors principles are applied. Through these program concepts, the HFE team establishes and provides reasonable assurance that the HFE program includes the following:

- Location and accessibility requirements for the control rooms and other control stations.
- Layout of the control rooms, including locations and design of individual displays and panels.
- Basic concepts and detailed design for the information displays, controls, and alarms for HSI control stations.
- Coding and labeling conventions for control room components and plant displays.
- Design of the screen-based HSI, including the actual screen layout and the standard dialogues for accessing information and controls.
- Requirements for the physical environment of the control rooms (e.g., lighting, acoustics, heating, ventilation and air conditioning (HVAC)).
- Layout of operator work stations and work space.
- Verification and validation (V&V) of the design of human system interfaces.
- Design implementation.
- Human performance monitoring.
- HSI associated with Instrument and Controls (I&C) and non-I&C systems.

2.1 *HFE Program Goals*

The goal of the HFE program is to provide the plant operators and technicians with task support and access to the information required to control plant processes and equipment safely and efficiently. The HFE program also establishes the time and performance criteria for required equipment operations via human reliability analyses and recognized guidelines.

The following generic human-centered HFE design goals are included in the HFE program:

- Personnel tasks can be accomplished within time and performance criteria.
- The HSIs, procedures, staffing/qualifications, training and management, and organizational support will support a high degree of operating crew situation awareness.
- The plant design and allocation of functions will maintain operation vigilance and provide acceptable workload levels (i.e., to minimize periods of operator underload and overload).
- The operator interfaces will minimize operator error and will provide for error detection and recovery capability.

2.2 *Design Assumptions and Constraints*

The following sections detail the assumptions and constraints that provide input to the U.S. EPR HFE program. These assumptions and constraints are not a result of U.S. EPR HFE analyses and evaluations, but provide input into the HFE program as well as the design of the HSI and the control rooms. Changes made to these assumptions can be made through the entire HFE analysis and evaluations (FRA/FA/TA/HSI design/V&V). The process will be followed and changes documented throughout the design process elements.

2.2.1 *Standard Design Features*

The U.S. EPR design is the U.S. implementation of the EPR design. The EPR design is an evolutionary Pressurized Water Reactor (PWR) design based on years of operation and design experience from the precursor PWR plants (e.g., based on European N4 and Konvoi plants, which are based on Westinghouse-designed PWRs currently operating in the U.S.). Predecessor plants, EPR plants whose conceptual design was done prior to the beginning of the U.S. EPR design, provide data and design outputs that formed the bases for the U.S. EPR design. Because the U.S. EPR design is based upon the predecessor plant designs, certain design details are considered standard features and will be evaluated as part of the HFE design process. These design details provide lessons learned and operating experience for the U.S. EPR design. The predecessor EPR designs are Olkiluoto-3 (OL3), and the Flamanville-3 (FA3).

2.2.1.1 *Control Rooms*

The control rooms are locations where major I&C display and control functions are available (i.e., I&C display and control functions not associated with a Local Control Station (LCS). They include the Main Control Room (MCR), the Technical Support Center (TSC), the Remote Shutdown Station (RSS), and the I&C Service Center (I&CSC). The MCR includes computerized operator workstations, a plant overview display, and conventional auxiliary panels. The I&CSC is located next to the MCR and is used for I&C configuration and maintenance. In case of unavailability of the MCR, the plant is monitored and controlled from the RSS.

2.2.1.1.1 Main Control Room

The MCR provides:

- A centralized location where actions to operate the plant safely are performed under normal conditions and where actions to reach and maintain a safe condition under accident conditions are performed.

- Adequate radiation protection that allows personnel to access and occupy the MCR under accident conditions without receiving radiation exposure in excess of 10 CFR 50 Appendix A (GDC 19) (Reference 2) requirements.
- The ability to transfer control outside the MCR to equipment that is designed to achieve prompt hot shutdown of the reactor and maintain a safe condition during hot shutdown with the possibility for subsequent cold shutdown of the reactor through suitable procedures.
- A means to communicate with the outside.
- A centralized location for initiating, monitoring, and authorization of maintenance for process equipment and systems.
- Protection from hazards and adverse environmental conditions for personnel and equipment required to operate the plant safely.
- A working environment for the operators that promotes reliable human performance.

The MCR houses the major HSIs with the main plant monitoring and control systems. The MCR is located in a hardened safeguards building where it is protected against radiation, internal and external missiles, and earthquakes.

The MCR is sized sufficiently so that the MCR staff can perform necessary actions. The arrangement of the adjacent control rooms facilitates coordination and communication between the members of the operating staff while reducing the need for access to the MCR by other plant personnel; such as field equipment operators, maintenance staff, and personnel in other HSI rooms (e.g., I&CSC). Several means of communication with non-licensed operators, maintenance personnel, Operations support staff, plant management, dispatchers, regulators, and public officials are provided in the MCR.

The MCR is equipped with:

- Operator workstations with HSI.
  (Note: The exact number of workstations is a design output.)

- A communication console.
  (Multiple means of communication are also available to each operator.)
- Plant Overview Panel (POP)

Storage space for paper-based procedures (PBPs) and documentation and for personal protective equipment.

2.2.1.1.2 Technical Support Center

The TSC is in close proximity to the MCR to simplify access to the MCR and maximize the efficiency of the interface with other HSI rooms.

If required, the technical support team uses the TSC to accommodate additional technical engineering, senior operations, and management staff who analyze the plant conditions and support the MCR operators during post-accident management. The TSC contains PICS monitors which have access to process information needed to monitor the state of the plant in all plant states; including maintenance, refueling, power, and accident conditions. The process control functions that are associated with PICS in the MCR are blocked in the TSC. The TSC is also provided with several means of communications within and outside the plant.

2.2.1.1.3 Remote Shutdown Station

The Remote Shutdown Station (RSS) contains the equipment necessary to bring the plant to a safe shutdown state during an event requiring evacuation of the Main Control Room (MCR), in addition to:

- A simultaneous single active failure (not required to accommodate a single failure in addition to equipment damage caused by a fire).
- A sustained loss of offsite AC power.

Consistent with 10 CFR 50 Appendix A, GDC 19, the RSS equipment at appropriate locations outside the MCR is provided: (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain

the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

The RSS is independent from the MCR. It is in a different fire zone and utilizes a different ventilation system than the MCR. The U.S. EPR RSS is not an alternate control room; therefore, plant recovery operations are not performed. After the event which results in evacuation of the MCR, the RSS is to be used for plant shutdown only.

2.2.1.1.4 Instrumentation and Control Service Center

The I&CSC provides a centralized location for I&C technicians and other specifically qualified plant staff to perform maintenance, periodic testing, and modification of I&C system software; including the interface equipment (e.g., PICS) and the monitoring and control equipment. Because some of the functions contained in the I&CSC systems (e.g., the loose parts and vibration monitoring system, leakage monitoring system, and the Aeroball and PowerTrax core monitoring systems) do not require constant control and monitoring, they are placed in the I&CSC to reduce operator burden.

The I&CSC is located in a vital area, within the MCR envelope. The main purpose of the I&CSC is to provide monitoring and maintenance equipment for I&C technicians and other qualified plant staff. Equipment located in the I&CSC is used to modify I&C plant automation system and HSI platform software and to perform maintenance and periodic testing of equipment. Controls are designed into the system to allow only the train of I&C which is off line and secured for maintenance to be accessed in the I&CSC. Testing of design changes performed in the I&CSC is also governed by administrative controls and applicable regulation. Changes to system software require proper design control approvals and multiple deliberate actions in order to implement (i.e., Changes are implemented in simulate mode and once tested are "committed" or saved. Additional administrative controls must be satisfied before the changes are then "activated"). Furthermore, the service units in the I&CSC are configured so that they are restricted by login access to only personnel who meet qualification requirements for the modification, maintenance, or testing to be performed. These activities are under

strict control of the Shift Manager and qualified personnel must get permission from this position before proceeding.

2.2.1.2 *Human System Interfaces*

The two I&C systems in the scope of the HFE program are the Process Information and Control System (PICS) and the Safety Information and Control System (SICS).

Operation of the U.S. EPR plant is normally performed by the PICS. The PICS is a non-safety-related digital HSI that provides an operator interface through an operator workplace (OWP). Each OWP includes monitors, keyboards, and a pointing device.

Backup operation is provided by the SICS. The SICS is a safety-related HSI that provides an operator interface through an OWP. Each OWP includes conventional instrumentation and controls. Display capabilities are provided to provide situational awareness and plant overviews. Overview of the plant is provided through the Plant Overview Panels (POP). The POP is a set of large overview displays belonging to the PICS.

2.2.1.2.1 Process Information and Control System

The PICS provides the screen-based interface for the operators in the MCR and in the RSS to control and monitor plant parameters during normal, abnormal, and accident condition. The PICS interfaces with the plant automation systems and receives both safety and non-safety data from the instrumentation. The PICS provides a state-of-the-art digital HSI to monitor the plant (i.e., an operator has access to available plant data at a single “workstation”). The PICS performs self-diagnostics; receiving and displaying self-diagnostic information from other plant systems, archiving data, and incorporating software changes. The PICS provides an alarm management interface for the operators.

2.2.1.2.2 Plant Overview Panel

The POP is a subset of the PICS. The POP is implemented as a set of large monitors driven by the PICS computers to present formats which show the overall plant state or other task-related formats. The POP is visible from workstations in the MCR and helps synchronize the operations staff with respect to common operational objectives. The graphical design of display screens incorporates expected viewing distances, and administrative controls provide recommendations for which screens are displayed on the POP.

2.2.1.2.3 Safety Information and Control System

The SICS provides the safety-related HSI for operators to use for control and information functions that are needed to monitor the plant safety status and bring the plant to a safe shutdown state and maintain it in case of unavailability of the PICS.

Class 1E conventional I&C, such as buttons and switches, are utilized for safety-related manual control. The Class 1E indication is also provided for credited safety parameters. The SICS provides all of the single-purpose (i.e., a button whose single purpose is to close a containment isolation valve), fixed-location, continuously available controls. The related displays for applicable safety-related functions are provided. These controls and displays are always available on the SICS.

2.2.1.3 *Alarm System*

Alarms are integrated with the HSI to assist the operator with situational awareness, alarm response, and any associated troubleshooting.

2.2.1.4 *I&C Architecture*

[ ]

2.2.1.5 *Plant Identification Coding*

A plant identification coding system is used to identify and label systems, structures, and components (SSC). The FA3 predecessor EPR design uses the ECS coding system to identify and label SSC. This system identifies SSCs by listing, for each SSC, a code with the following content; Plant Unit Code, System or Building Code, Identification Number, Equipment Code, and Information or Component.

For the U.S. EPR design, the coding system is based on ECS coding system; however, the coding uses acronyms more common to English speaking Operators.

2.2.2 *Concept of Operation Assumptions*

The following sections discuss the design assumptions made for the U.S. EPR design. These design assumptions provide the assumptions made concerning the operating

philosophy for the U.S. EPR design. These assumptions are the starting point and are subject to changes based on additional analysis and evaluations during detailed design. It is expected that these assumptions will not be changed significantly. All changes that are made will be documented within the HFE design process. The change process is covered through the individual implementation plans.

A U.S. EPR design goal is to design the plant and the HSI so that three licensed operators (one of which holds a senior reactor operator (SRO) license) can safely monitor and control the plant under operating conditions, including normal operation, startup, shutdown, abnormal operation, and accident conditions. This design goal includes providing a level of automation so that only one licensed operator will be required to be at the controls with one SRO-licensed operator in the MCR during normal, at-power operations. Additionally, each operating crew will only be required to include an SRO-licensed Shift Manager, a Shift Technical Advisor (may be combined with the Shift Manager position), a number of non-licensed equipment operators (NLOs), and a maintenance crew consisting of a supervisor and chemistry, radiation protection, I&C, electrical, and mechanical technicians.

As this is a design goal, a combined license (COL) applicant that references the U.S. EPR design certification will develop a complete staffing arrangement. It is expected that a COL applicant that references the U.S. EPR design certification will determine staffing levels and qualifications of plant personnel based on the COL applicant's corporate staffing philosophy, existing site operations, fleet operations, final plant design, and current regulations.

2.2.2.1 *Staffing*

Staffing assumptions for the U.S. EPR MCR include, at a minimum, a Shift Manager (SM), Shift Technical Advisor (STA), Control Room Supervisor (CRS), Reactor Operator (RO), and an Additional Licensed Operator (ALO). This staff performs the following:

- Carry out or request manual actions which are necessary to put plant systems into or out of service or modify the plant systems during normal operation or after an incident or accident.
- Use parameters and information delivered by the information systems to monitor the safety and operability of the plant.
- Perform checks and periodic tests to confirm that safety systems remain fully operable.
- Initiate corrective action in case of equipment malfunctions or unforeseen events.
- Request field operators or maintenance personnel to perform additional corrective actions if actions from the MCR are not sufficient.
- Take into account unavailability of equipment (e.g., during maintenance) so that the plant is continuously operated safely within the bounds of the technical specifications.
- Execute appropriate actions following an accident.
- Review the actions of other operators.

2.2.2.2 *Operating Philosophy*

The following sub-sections provide the assumptions for the operating philosophy for the U.S. EPR design. These assumptions are used as input to the design of the HSI and control rooms. Modifications to these assumptions based upon analyses feedback will introduce a change in the design, governed by the design change control process discussed in Reference 3.

2.2.2.2.1 Procedures

The plant is operated in accordance with the Technical Specifications and with the applicable normal, abnormal, or emergency operating procedures (EOPs). Plant operating procedures (i.e., normal, abnormal, emergency) are based upon the different roles, functions, and responsibilities for the MCR operators functioning as an integrated team. CBPs are displayed on the PICS. The PICS HSI design provides the capability to jump to other procedures or displays of immediate interest without excessive navigational steps. For operation from SICS, PBPs are used.

2.2.2.2.2 Alarms

Operators monitor plant performance to detect failures in mechanical, electrical, or I&C systems. The alarm systems supplement this monitoring by alerting operators to certain types of failures. Upon detecting such failures, operators implement applicable specific alarm response procedures. This may include performing additional diagnostics, performing actions to compensate for the failure, or requesting field operators or other staff to perform additional diagnostics or repair actions. In addition, operators assess and respond to keep the plant and components in a safe state based on their training and understanding of the plant situation.

2.2.2.2.3 Normal Operations

Normal operations are defined as operating within the modes described in Technical Specifications in a controlled manner with no major equipment faults.

2.2.2.2.4 Abnormal Operations and Incidents

Abnormal operations refer to incidents that may occur once or more during the life of the plant; and result, at worst, in a reactor trip with the plant capable of returning to power. These incidents are easily recognized and identifiable. Operator responses to such anticipated transients are in accordance with the event-oriented abnormal operating procedures which are developed to support optimal responses to recognized conditions.

2.2.2.2.5 Emergency Operations and Accidents

Emergency procedures provide direction for the operators to mitigate the consequences of transients and accidents that result in exceeding reactor protection system or engineered safety features actuation setpoints or require a plant shutdown. The emergency procedures for the U.S. EPR design are based on emergency procedure guidelines which are developed from analyses of transients and accidents that are specific to the U.S. EPR design and operating philosophy. These analyses will include both design bases events and beyond design bases events as required by NUREG-0737 (Reference 4) and other requirements.

The emergency procedures for the U.S. EPR design are symptom-based procedures which will provide guidance for the operator to mitigate transients without having to diagnose a specific event. HSI issues will be considered during the development of these procedures to provide reasonable assurance that the procedures support and guide operator interaction with plant systems. The use of the procedures with the HSI will be verified and validated to provide reasonable assurance that accepted HFE principles are incorporated.

In addition, as a result of emergency planning, operators have procedures, equipment, and facilities to support an integrated response.

Key features of this plan include:

- Standard emergency classification and action level schemes to determine minimum response measures.
- Procedures for notification of response organizations (i.e., federal, state, and local response organizations and emergency personnel).
- Adequate emergency facilities and equipment to support the emergency response (e.g., TSC).
- A range of protective actions for the plume exposure pathway for emergency workers and the public.

- Methods, systems, and equipment for assessing and monitoring actual or potential offsite consequences of radiological emergency conditions

2.2.2.2.6 Usage of PICS and SICS

While the PICS is available, plant operations are performed via the PICS at a sit-down workstation. In the event the PICS is unavailable or when the plant conditions require it, the plant operations are performed using the SICS.

Depending on plant conditions and the availability of systems, the operators may use the SICS to maintain steady-state operations or commence shutdown to a safe state via conventional SICS controls.

The displays are expected to mimic the operation and format of the PICS displays for certain safety-related functions, that are required in order to shut down the plant to a safe state, and maintain it in that state in the event that the PICS is unavailable. The SICS contains the controls and displays required for design basis accident monitoring.

For failures that are beyond the design basis, both the PICS and SICS are available for monitoring and control. The PICS is the preferred HSI; SICS is the credited HSI to be used as a back-up when the PICS is not available.

2.2.2.2.7 Loss of Computerized I&C

Loss of computerized I&C refers to the loss of I&C systems other than, or in addition to, the PICS. If PICS is available, notification that indicators and controls are unavailable shall be provided to the operator. Additionally, the PICS shall provide the status of the I&C systems, including faults occurring in various I&C systems.

The operating manual shall identify actions that are required for dealing with the loss of computerized I&C systems and measures that establish the priority of the actions implemented with the remaining conventional systems.

2.2.2.2.8 *Loss of Computer-Based Operating Procedures*

In case of a loss of the CBPs on the PICS, plant operation shall be transferred to the SICS. Monitoring of the plant state and plant shutdown from SICS shall be supported by PBP procedures. CBPs should contain means of navigating to appropriate HSI screens necessary to control or monitor response for the required procedure steps. Aside from the navigation and layout differences and the availability of live data, the computer-based and hard copy procedures shall contain similar information in a similar format and shall be compatible.

2.2.2.2.9 *Loss of MCR*

If the MCR becomes uninhabitable, the plant is tripped as the operators leave the MCR. Operators shall conduct further shutdown activities in the RSS. Emergency operations are not postulated from the RSS. Recovery operations shall not be attempted from the RSS, considering the possibility of later emergency situations after the MCR is abandoned.

2.2.2.2.10 *Periodic Surveillances, Operations, and Tests*

The I&C systems include integral self-testing features. HFE requirements define the selection criteria to determine the level or type of alarms to be displayed in the control room. Operators have no responsibility with regard to these self-testing features other than monitoring and responding to alarms when the self-testing indicates problems.

Only licensed operators use the normal operator interfaces (e.g., PICS and SICS) to perform any periodic testing which entails the operation of plant process equipment (e.g., changing valve positions, cycling pumps and motors on and off) in strict compliance with authorized test procedures.

During operational modes, the conventional operator interfaces (i.e., SICS devices) may require simple lamp and horn tests. The MCR operators manually perform such tests at the proper intervals. The simple testing of the conventional panel equipment does not require additional personnel in the MCR.

Routine calibration and testing within the digital I&C system will be performed from the I&CSC engineering workstation and service units and shall have minimal impact on MCR operations. A monitor with access to operational displays but with no control capabilities is provided in the I&CSC to support such activities.

2.2.2.2.11 Maintenance

Maintenance on the I&C systems, such as software updates and component replacement, are governed by procedures. Because the components of the I&C systems are not all located within the MCR, administrative procedures along with other design features, such as cabinet locks, are utilized to prevent unauthorized access.

Additionally, indication of maintenance on plant equipment is notified to the operator through the HSI. Features, such as tag-out indications to the operator, prevent plant equipment from being operated while out of service.

2.3 *Applicable Facilities*

2.3.1 *A/E Scope*

The HFE program scope applies to the design of the MCR, the TSC, the I&CSC, the RSS, and LCSs that provide computer-based HSI. The design of LCSs that provide non-computer-based HSI (e.g., manual valves) is typically accomplished concurrent with the applicable system; however, a style guide developed by the HFE team provides HFE requirements for the design of the HSI portion of the LCS.

2.3.2 *COL Scope*

HFE design implementation for a new Emergency Operations Facility (EOF) or changes to an existing EOF resulting from the addition of a U.S. EPR plant are part of COL applicant scope. The HFE 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 U.S. EPR HSI facilities.

2.4 *Applicable HSIs*

The scope of the HFE program includes HSIs associated with monitoring and controlling U.S. EPR design 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) will follow guidelines established by the HFE team. 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).
- Local Control Stations (LCS).

2.5 *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 other personnel; including technicians, maintenance personnel, engineering support staff, and management.

Plant personnel addressed by the HFE program include licensed control room operators as defined in 10 CFR Part 55 (Reference 5), and the following categories of personnel defined by 10 CFR 50.120 (Reference 6).

- Non-licensed operators.
- Shift manager.
- Shift technical advisor.
- Instrument and control technician.
- Electrical maintenance personnel.

- Mechanical maintenance personnel.
- Radiological protection technician.
- Chemistry technician.
- Engineering support personnel.

2.6 *Effects of Modifications on Personnel Performance*

The HFE program applies to the equipment supplied for the original configuration of the U.S. EPR design. Modifications to the original interface configuration are required to adhere to the guidelines of Reference 3. 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 3 and RG 1.174 (Reference 1). Throughout the life of the plant, HFE issues resulting from plant modifications are documented and dispositioned in accordance with the Human Performance Monitoring plan.

3.0 HFE TEAM AND ORGANIZATION

The HFE team is the multi-disciplinary team responsible for implementing the HFE program. The HFE 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 NUREG -0800, Standard Review Plan, Section 13.1.1, Management and Technical Support Organization (Reference 7). The HFE team is guided by the HFE program described herein for the proper development, execution, oversight, and documentation. The HFE 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).

3.1 *Responsibility*

The HFE team is responsible with respect to the scope of the HFE program for:

- Development of all HFE plans and HFE procedures.
- Oversight and review of all HFE design, development, test, and evaluation activities.
- Initiation, recommendation, and provision of solutions through designated channels for problems identified in the implementation of the HFE activities.
- Verification of implementation of team recommendations.
- Assurance that all HFE activities comply with the HFE plans and HFE procedures.
- Scheduling of activities and milestones.
- Coordination of HFE requirements with portions of the U.S. EPR design that are not conducted by I&C Engineering (i.e., LCSs for non-I&C equipment).
- Designer's input for COL applicants for operating procedure development, staffing requirements, and training.

The HFE team is responsible with respect to the scope of the control room design for:

- Location and accessibility requirements for the control rooms and other control stations.
- Layout of the control rooms, including the location and design of individual displays, panels, and workstations.
- Requirements for the physical environment of the control rooms (e.g., lighting, acoustics, temperature, humidity, and air flow).
- Layout of operator workstations and work space.

The HFE team is responsible with respect to the scope of the HSI design for:

- Basic concepts and detailed design for information displays, controls, and alarms for the control rooms and other control stations.
- Coding and labeling conventions for control room components and plant displays.
- Design of the screen-based HSI, including standard dialogues for access to information and controls and actual screen layout.

3.2 *Organizational Placement and Authority*

The HFE team consists of the HFE Responsible Technical Manager (RTM), an HFE Engineering Discipline Lead (EDL), and an HFE team composed of individual members of the New Plants Engineering organization, who are referred to as responsible engineers. The RTM is responsible for Organization management of the responsible engineers. The HFE EDL reports to the U.S. EPR Integration Manager. The HFE EDL is responsible for providing budget, schedule, and oversight of the technical details of the U.S. EPR design. The EDL is matrixed to the structure to provide functional management of the responsible engineers.

The HFE EDL is responsible for integration of the HFE Analysis to support HSI and control room design with the overall plant design and tracks the HFE issues as

described in Section 5.0. The HFE EDL is also responsible for assisting in coordinating activities with other disciplines and managing schedules. The HFE organization chart is provided in Figure 3-1 below. The solid lines represent organizational responsibility and the dashed lines represent functional responsibility. The dotted line represents a communication link.

The RTM and the EDL communicate but do not have functional or organizational authority over one another.

[ ]

Figure 3-1: HFE Organization

[ ]

Figure 3-2: HFE Qualification / Task Matrix

3.3 *Composition*

The HFE team is composed of individuals experienced in various technical disciplines. The HFE RTM leads the team and is responsible for integration of the technological input. The HFE RTM has experience in managing multi-discipline designs and operational systems. The technical discipline expertise required on the team includes:

- Technical Project Management.
- Systems Engineering.
- Nuclear Engineering.
- I&C Engineering.
- Architect Engineering.
- Human Factors Engineering.
- Plant Operations.
- Computer System Engineering.
- Plant Procedure Development.
- Personnel Training.
- Systems Safety Engineering.
- Maintainability and Inspectability Engineering.
- Reliability and Availability Engineering.

The HFE team composition is provided in Figure 3-3 below.

Figure 3-3: HFE Team Composition

3.4 *Team Staffing*

The specifics of the U.S. EPR HFE team assignments and job descriptions evolve as the project progresses. The HFE team is split into two separate functions, each run by a supervisor. One function involves the HFE analysis activities while the other focuses on the HFE design.

The HFE analysis supervisor is responsible for the planning and analysis activities of the HFE program. This includes the OER, FRA/FA, TA (including staffing and qualifications), and Human Reliability Analysis (HRA). The HFE design supervisor is responsible for the system platform design and specification of the equipment, the HSI layout (which includes conventional and screen-based HSIs), the layout of the control rooms, and the interface with other disciplines related to control room design (e.g., HVAC, radiological protection, control room habitability, security).

Senior members of the team are assigned as system engineers or system managers for each of the control rooms and the HSI platforms in the scope of the HFE program. These system managers conduct the analysis and design activities as part of the evolution of their design. Other members of the team support the system managers, task managers, and program manager as needed. Integration of these activities, as well as maintenance and ownership of the program level documentation, is the responsibility of the HFE RTM.

The professional experience of the HFE team collectively satisfies the qualifications presented below. The technical disciplines described do not necessarily equate to a single individual. Greater emphasis is placed on experience than on education credentials. Also, individual team members may report administratively to various discipline design leads. For the purposes of the HFE and control room design, individual team members report functionally to the Manager of I&C Engineering through the HFE RTM.

- Technical Project Management
  - Minimum Qualifications:
    - Bachelor's degree.
    - Five years of experience in nuclear power plant design or operations.
    - Three years of management experience.
  - Responsibilities:
    - Develops and maintains the schedule for the HFE design process.
    - Provides a central point of contact for the management of the HFE design and implementation process.
- Systems Engineering
  - Minimum Qualifications:
    - Bachelor of Science degree.

- ♦ Four years of cumulative experience in at least three of the following areas of systems engineering: design, development, integration, operation, and test and evaluation.
- Responsibilities:
  - ♦ Provides knowledge of the purpose, operating characteristics, and technical specifications of major plant systems.
  - ♦ Provides input to HFE analyses, especially the function analysis and task analysis.
  - ♦ Participates in the development of procedures and scenarios for task analyses and integrated system validation.

- Nuclear Engineering
  - Minimum Qualifications:
    - ♦ Bachelor of Science degree.
    - ♦ Four years of experience in nuclear design, development, testing, or operations .
  - Responsibilities:
    - ♦ Provides knowledge of the processes involved in reactivity control and power generation.
    - ♦ Provides input to HFE task analyses.
    - ♦ Participates in the development of scenarios for task analyses and integrated system validation.
- I&C Engineering
  - Minimum Qualifications:
    - ♦ Bachelor of Science degree.

- Four years of experience designing of hardware and software aspects of process control systems.
- Experience in at least one of the following areas of I&C engineering: development, power plant operations, and test and evaluation.
- Familiarity with the theory and practice of software quality assurance and control.

- Responsibilities:
  - Provides detailed knowledge of the HSI design, including control and display hardware selection, design, functionality, and installation.
  - Provides knowledge of information display design, content, and functionality.
  - Participates in the design, development, test, and evaluation of the HSI.
  - Participates in the development of scenarios for human reliability analysis (HRA), validation, and other analyses involving failures of HSI data processing systems.
  - Provides input to software quality assurance programs.

- Architect Engineering
  - Minimum Qualifications:
    - Bachelor of Science degree.
    - Four years of experience designing power plant control rooms.
  - Responsibilities:
    - Provides knowledge of the overall structure of the plant, including performance requirements, design constraints, and design characteristics of the following: control room, remote shutdown area, and LCSs.

- Provides knowledge of the internal configuration of plant components.
- Provides input to plant analyses.

- Human Factors Engineering
  - Minimum Qualifications:
    - Bachelor's degree in human factors engineering, engineering psychology, or a similar science.
    - Four years of experience in human factors aspects of human-computer interfaces, including process control (e.g., design, development, and test and evaluation).
    - Four years of cumulative experience related to the human factors aspects of workplace design (e.g., design, development, test and evaluation of workplaces).
  - Responsibilities:
    - Provides knowledge of human performance capabilities and limitations, human factors design and evaluation practices, and human factors principles, guidelines, and standards.
    - Develops and performs human factors analyses.
    - Participates in the resolution of human factors problems.
- Plant Operations
  - Minimum Qualifications:
    - Current or prior SRO with two years of experience on shift with qualification.

    OR

    - Current or prior RO with six years of experience on shift with license.

- Responsibilities:
    - Provides knowledge of operational activities that are relevant to characterizing tasks, HSI, and environment technical requirements.
    - Provides knowledge of operational activities to support HSI activities (e.g., development of HSIs, procedures, and training programs).
    - Participates in the development of scenarios for HRA evaluations, task analyses, HSI tests and evaluations, and V&V.
    - Participates in preliminary validation exercises on static mockups and provides input relating to the expected plant response.
    - Participates in final validation exercises on a simulator by observing and evaluating the subject operator's response.

- Computer System Engineering
    - Minimum Qualifications:
        - Bachelor of electrical engineering or computer science degree or graduate degree in another engineering discipline (e.g., mechanical, chemical).
        - Four years of experience designing digital computer systems and real-time systems applications.
        - Familiarity with the theory and practice of software quality assurance and control.
    - Responsibilities:
        - Provides knowledge of data processing associated with displays and controls.
        - Participates in the design and selection of computer-based equipment (e.g., controls and displays).
        - Participates in the development of scenarios for HRA, validation, and other analyses involving failures of the HSI data processing systems.

- Plant Procedure Development
  - Minimum Qualifications:
    - ♦ Bachelor's degree.
    - ♦ Four years of experience in developing nuclear power plant operating procedures.
  - Responsibilities:
    - ♦ Provides knowledge of operational tasks and procedure formats.
    - ♦ Participates in the development of scenarios for HRA evaluations, task analyses, HSI tests and evaluations, validation, and other evaluations.
    - ♦ Provides input for the development of EOPs, procedure aids, CBPs, and training systems.
    - ♦ Participates in the development and preparation of the procedures and training systems.
- Personnel Training
  - Minimum Qualifications:
    - ♦ Bachelor's degree.
    - ♦ Four years of experience developing personnel training programs for power plants.
    - ♦ Experience in the application of systematic training development methods.
  - Responsibilities:
    - ♦ Develops the content and format of personnel training programs.
    - ♦ Coordinates training issues that arise from activities (e.g., HRA, HSI design, and procedure design).
    - ♦ Participates in the development of scenarios for HRA evaluations, task analyses, HSI tests and evaluations, and V&V.

- Systems Safety Engineering
  - Minimum Qualifications:
    - Bachelor of Science degree.
    - Four years of experience in system safety engineering.
  - Responsibilities:
    - Identifies safety concerns and performs a system safety hazard analysis.
    - Provides results of system safety hazard analysis to probabilistic risk assessment/HRA and human factors analyses.
- Maintainability and Inspectability Engineering
  - Minimum Qualifications:
    - Bachelor of Science degree.
    - Four years of experience in at least two of the following areas of power plant maintainability and inspectability engineering: design, development, integration, and test and evaluation.
    - Experience in analyzing and resolving plant I&C system or equipment-related maintenance problems.
  - Responsibilities:
    - Provides knowledge of maintenance, inspection, and surveillance activities.
    - Supports the design, development, and evaluation of the control room and other HSI components.
    - Provides input in the areas of maintainability and inspectability.
    - Participates in the development of scenarios for HSI evaluations, including task analyses, HSI design tests and evaluations, and validation.

- Reliability and Availability Engineering
    - Minimum Qualifications:
        - Bachelor's degree.
        - Four years of cumulative experience in at least two of the following areas of power plant reliability engineering activity: design, development, integration, and test and evaluation.
        - Knowledge of computer-based, human-interface systems.
    - Responsibilities:
        - Provides knowledge of plant component and system reliability and availability and assessment methodologies.
        - Participates in human reliability analyses.
        - Participates in the development of scenarios for HSI evaluations, especially validation.
        - Provides input to the design of HSI equipment.

4.0 HFE PROCESS AND PROCEDURES

The HSI and control room design is performed in accordance with the U.S. EPR Quality Assurance Program (QAP) (Reference 3). The U.S. EPR QAP directs the development of procedures, directives, and guidelines to flow-down requirements from the U.S. EPR QAP into the design and engineering work. AREVA NP Inc. (AREVA NP) generic design control measures are implemented through the procedures, which include the provisions for the control of design inputs, processes, outputs, verification, independent review, analysis, verification testing, design changes, organizational interfaces within AREVA NP and with suppliers, records and QA reviews.

The HFE team is responsible for developing procedures, directives, guidelines, and HFE documentation under the U.S. EPR QAP for activities within the scope of the HFE program.

4.1 *General Process Procedures*

To guide the HFE activities, work plans are written to direct the HFE team to execute its responsibilities. The HFE work plans are developed and maintained by the HFE team under the direction of the HFE RTM. These work plans provide the following:

- Governing procedures for:
  - Equipment design changes.
  - Design Review Boards (DRB) (where applicable).
- Roles and responsibilities for:
  - Assigning HFE activities to individual team members.
  - Internal management of the team.
  - Making management decisions regarding HFE.
  - Making HFE design decisions.

- Workflow:
  - Required input to perform design or analysis activities.
  - Method to perform design or analysis activities.
- Work products (output documentation).
- Reviews:
  - Individual HFE review.
  - Design team review of HFE products (where applicable).

4.2 *Process Management Tools*

Tools and techniques utilized by the HFE team to fulfill their responsibilities include design documentation, design verification checklists, product upgrade lists (i.e., a method of tracking open items in design documents), and plant-level design freezes. Specific tools and techniques used for each HFE activity are described in the implementation plans (listed in Section 6.1) and work plans. Internal administrative procedures for design control process, design change control, and release of product documentation describe the methods for utilizing these tools and techniques.

4.3 *Integration of HFE and Other Plant Design Activities*

The HFE design process is iterative as shown in Figure 1-1. As the design evolves through the four phases (i.e., conceptual design, basic design, detailed design, construction/operation) the current available design information is used. When a design phase is complete a design freeze will occur based on the project schedule and design implementation schedule. Once a design freeze occurs, changes will follow the design change process to involve the HFE team and other engineering disciplines for potential design impacts. If a HFE design impact or a human factors issue is discovered, the HFE team will go back to HFE analysis as needed. The HFE analysis is updated and additional analysis occurs as part of the iterative design.

The HFE design team receives and produces design input/output relative to other engineering discipline designs. For example, as the I&C architecture design is complete through conceptual design, the HFE MCR concept design will integrate with the documented design constraints. The I&C engineering organization develops the I&C system designs, which includes defining design requirements, reviewing inputs, producing system documentation, verifying that the design inputs link to the outputs, and outlining expected acceptance testing. The HFE team integrates the I&C system designs with the HSI and performs design and layout of the control rooms. Both functions involve an iterative process. The HFE team has the same design input/output relationship with the other engineering disciplines (e.g., mechanical and electrical system engineers). Once the system design is complete, task analysis will be developed for the particular design phase. The HFE team will receive the design output from the system design engineers to perform TA.

Documentation produced by systems and component engineering organizations include design requirements, system descriptions (e.g., design bases, safety classifications), design system interfaces, drawings, calculations, and ancillary documents. A design verification checklist is required for certain portions of the design to support the evaluation of design adequacy.

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 (e.g., 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.

4.4 HFE Program Milestones

Figure 4-1: Human Factors Program Timeline

[ ]

Figure 4-2: HFE Program Implementation

[ ]

4.5 *HFE Process and 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. 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, implementation plans for the various analyses, or in reports generated as a result of the analyses.

4.5.1 *U.S. EPR Design Control*

The purpose of the design control process is to define the method used to provide control of design, design verification, and analysis activities. The AREVA NP design control process procedure is described in Reference 3. This process contains a controlled, logical, systematic, and comprehensive flowchart; and a hierarchy of design information to expeditiously and correctly integrate and transform design inputs into design outputs. 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 process also either integrates the various design control measures described below as part of the process procedure or incorporates various design control measures in the procedure by reference.

The design control process develops a design and establishes a design configuration in the Records Management System (RMS). Once released to the RMS, documents produced within the design control process become part of the design configuration.

U.S. EPR project management establishes the scope, objectives, requirements, and safety classification in writing for the responsible design organizations. These procedures govern the preparation and review of design documents and also establish methods for the identification and control of design interfaces; the coordination among participating design organizations; and the review, approval, release, distribution, and revision of documents.

The appropriate engineering organization prepares reviews, approves, and verifies design documents for items and services within their respective area. Procedures are established to promote adequacy and accuracy of design documentation. The following are types of design documents that support facility design, construction, and operation:

- Plant technical requirements.
- System design requirements.

- System descriptions.
- Design drawings.
- Design analyses.
- Computer program documentation.
- Specifications and procedures.

These documents specify technical and quality requirements that are appropriate to the activities they cover. A qualified individual, other than the preparer of the document, performs an independent review of the documents for completeness and technical accuracy. Revisions to approved design documents are considered design changes and are subject to the same review and approval process as the original documents.

Verification methods include: independent review of design documents, design analyses (e.g., calculations), design review boards, and design verification testing. Calculations can either establish design requirements or verify the design. The analyst documents the purpose, assumptions, methods, design input data, results, and conclusions of the calculation in a manner that an independent reviewer can verify the technical accuracy of the calculation. Independent reviewers shall be competent in the particular type of analysis. Design Review Boards (DRB) are conducted in accordance with written procedures for new designs and major changes to the existing design configuration as determined by the responsible technical manager and project management. A DRB provides an independent evaluation of a design to verify that the design as proposed was accomplished, that the design is correct, and that it is complete. When engineering judgment concludes that design analyses or previous experience cannot substantiate a design or design feature, testing is performed for design verification.

An integrated Quality Assurance (QA) organization oversees audits of design documents for the inclusion of appropriate QA requirements. Deviations from specified quality standards are identified and controlled in accordance with written procedures.

Reference 3 provides a description of the QA organization and the QAP requirements, including an overview of the design control process.

The HFE team is required to follow the same design processes as other engineering disciplines and is accountable for verifying the quality of the HSI and control room layout per Reference 3 and under the guidelines of the AREVA NP design control process. Changes to the design configuration are performed in accordance with the AREVA NP design change control process described in Reference 3.

System design requirements decompose higher level (i.e., plant) requirements to define the design inputs for each system. System descriptions for control rooms and for HSI platforms are produced as roll-up documents. The documentation of the HFE and Control Room Design is included in the system descriptions, in implementation plans for the various analyses, or in reports generated as a result of the analyses.

4.5.2 *Plant Technical Requirements Document*

The Plant Technical Requirements Document (PTRD) specifies the initial design inputs for designing a nuclear power plant to capture overall plant design requirements and restraints. The PTRD includes the reasoning for each design input based on design considerations to provide a consistent basis for making design decisions, accomplishing design verification measures, and evaluating design changes. The PTRD requirements include sufficient detail to allow requirements to be decomposed into the requirements specified in the System Design Requirements Documents (SDRDs). The OL3 EPR reference design provides the starting point for development of design inputs for the U.S. EPR design.

4.5.3 *System Design Requirements Documents*

SDRDs specify design inputs for systems, structures and components which have been decomposed from plant level inputs. SDRDs document and convey design inputs so that they can be reviewed and approved by the responsible design organization. SDRDs are released before subsequent design output documents to provide

reasonable assurance that inputs are specified to a level of detail necessary to permit further design activity. SDRDs include the reason and design basis for each design input so that the basis for design decisions, changes to the configuration, and verification measures are consistently applied. SDRDs adequately define design inputs so that the hierarchy of their application is clear.

For the U.S. EPR HFE program, SDRDs are produced for the control rooms (e.g., MCR, TSC, RSS, and I&CSC) and the HSIs (e.g., PICS and SICS). SDRDs for LCSs are developed by the engineering discipline responsible for the process system that the LCS controls; however, HFE requirements provided through style guides are used as an input.

4.5.4 *System Description Document*

A System Description Document (SDD) is the principal document which defines a system design. The SDD describes the system design in sufficient detail to permit verification that the design satisfies the design requirements. The SDD identifies interfaces with other systems so that the design input requirements for each system can be understood. Cross-discipline independent reviews of SDDs for systems which interface with non-HSI, non-control room, or non-I&C systems are also required.

The SDD is a living document and the level of detail expands during successive iterations as the system design develops. The final version of an SDD is used to write the system equipment specification, which is used to procure, fabricate, and install the system.

SDDs follow a predefined format and require specific content, which includes:

- System and component functions.
- General description.
- Operation.
- Design requirements and how the design accomplishes the requirements.

- Interface requirements.
- Operational aspects (e.g., testing, installation, inspection, and maintenance).
- Technical system specifications.

To avoid unverified design information from being incorporated as verified during successive iterations, unverified design information is identified as such via a separate process.

In addition to providing a description of the design of the HSI hardware, the SDD for each of the HSIs provides the mechanism for capturing generic human factors requirements in conjunction with the HSI design implementation plan (see Section 6.1). These documents 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 system, plant information system, and hard-wired control integration in panels and workstations.

Within the U.S. EPR HFE program, SDDs are produced for the control rooms (e.g., MCR, TSC, RSS, and I&CSC) and the HSIs (e.g., PICS and SICS). The SDDs reference applicable layout drawings for the control room floors. The SDDs for the MCR and RSS contain the design and layout for workstations, which include drawings and text but does not include individual screen designs.

SDDs for LCSs are developed by the engineering discipline responsible for the process system that the LCS controls; however, HFE requirements provided through the style guides are used as an input.

4.5.5 *Design Drawings*

Design drawings disclose, by means of pictorial and/or textual presentations, the physical and functional engineering, manufacturing, and product requirements of an item. For the U.S. EPR design, these drawings include: P&IDs, electrical one lines, and piping isometrics. These design drawings are official records stored in the RMS.

The HFE program utilizes these drawings as design input the HSI and control room designs.

Design drawings are created by the HFE team for the MCR layout/ergonomic studies and for aspects of the HSI design (e.g., individual panel and display layouts.) These drawings are included in the SDDs or other HFE documentation, and are not individual records stored in the RMS.

4.5.6 *Design Analyses*

Design analyses are used to establish design requirements or to verify the design. The analyst is required to document the analysis as to purpose, assumptions, method, design input data, results, and conclusions; in such a manner that an independent reviewer can verify its technical accuracy. Design analyses are checked by independent reviewers who are competent in the particular type of analysis. Computer programs used for design analyses are certified or verified and validated as appropriate.

For the U.S. EPR HFE program, design analyses documentation are created for each of the following analysis activities:

- Operating Experience Review.
- Functional Requirements Analysis/Function Allocation.
- Task Analysis (including Staffing and Qualifications).
- Human Reliability Analysis.

Due to the volume of data expected for the Operating Experience Review, Functional Requirements Analysis, Function Allocation, and Task Analysis, the results of these analyses will not be included in the design analyses documentation. Instead, these results will be maintained in data structures.

Additional design analyses documentation is created for the various HSI and control room evaluations performed during the design phase.

4.5.7 *Computer Program Documentation*

Computer programs are used for a variety of tasks throughout the life of the HFE program. These programs include both purchased computer programs as well as internally developed computer programs. Internal administrative procedures provide requirements and responsibilities for developing software, certifying software, the quality assurance program, and documentation requirements for computer programs used in engineering design applications. The computer program documentation is included in the design analyses report and held in the RMS.

4.5.8 *Specifications*

A specification document defines the technical characteristics and design requirements of system equipment to procure, fabricate, and install the components of that system. A System Design Requirements Document (SDRD) specifies the system-level design requirements and their technical bases. An SDD only needs to specify the component-level design requirements which are satisfied for the system to perform its intended functions. An equipment specification may be used to specify other component requirements.

As part of the design control process described in Reference 3, a specification contains the following sections:

- Scope.
- Definitions.
- Design requirements.
- Material requirements.
- Fabrication requirements.
- Examination and testing requirements.
- Cleaning and preparation for shipping requirements.
- Quality assurance requirements.

- Engineering documentation requirements.
- Technical proposal requirements.
- Contract information.

Specifications are produced for the HSI system equipment and for associated sub-functions for the control rooms (e.g., lighting, sound isolation, HVAC requirements).

4.5.9 *Procedures*

Company administrative policies, procedures, directives and instructions detail the methods for preparation, review, approval, revision, distribution, and use of documents. In addition, procedures govern the coordination and control of interface documents. Interface documents may include those between engineering disciplines, engineering projects, affiliate companies, suppliers or customers.

For the U.S. EPR project, procedures are written to direct the development of design documentation as well as interdisciplinary reviews. Additionally, procedures are written by the HFE team to describe how HFE-related activities are performed. Adherence to procedures provides consistency in the design of the U.S. EPR plant, including the HSI and control rooms.

4.6 *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 in that:

> "The acceptability of suppliers of safety related materials, items, or services are based on the following items:
>
> - A direct evaluation of their QA Program to 10 CFR 50 Appendix B and NQA-1 to determine the capability to supply materials, items, or services meeting all procurement document requirements
> - A survey/audit of the supplier's facility.
>
> Suppliers are required to ensure that their products meet the requirements of the procurement documents. These methods are reviewed by the cognizant Manager/Supervisor with an overview by the QA organization.

> Additionally, AREVA NP Inc. may verify acceptance of products by independent analysis.
>
> Reviews of the vendor quality program, performance of audits, performance of preaward evaluations and annual evaluations are performed in accordance with an administrative procedure which follows the guidance of Regulatory Guide 1.28; these methods are used to verify the quality of the products and services provided by subcontractors/sub-vendors. As part of this program subcontractors/subvendors are required to furnish documents such as QA Data Packages, procedures, source audit and surveillance reports, and QAP documents. Sub-vendor/subcontractor QAP's are reviewed and accepted during the pre-award evaluation of the sub-vendor/subcontractor prior to placement on the Approved Suppliers Listing (ASL)."

HFE requirements are included in each contract through the equipment specification (see Section 4.5.8). After the initial specification is issued to the subcontractor, a conformance period will begin to reconcile differences between design requirements and system capabilities. The results are a fully conformed equipment specification. Upon receipt of the delivery of the equipment, reviews of the design verify that it conforms to the requirements specified in the conformed equipment specification, which includes HFE requirements.

Subcontractors working for AREVA NP, as part of the HFE team, receive the same project-specific training as other engineers assigned. The HFE RTM approves, and is ultimately responsible for, any work products from the HFE team.

5.0 HFE ISSUES TRACKING

HFE issues are identified and tracked in a data structure throughout the life cycle of the HFE program for the U.S. EPR design project. Inputs into the HFE Issues Tracking Database come from operating experience review results, Human Engineering Discrepancies (HEDs), design review board results, and cross-discipline reviews not incorporated by the normal detailed design process.

5.1 *Availability*

The HFE Issues Tracking Database is accessible by any member of the U.S. EPR design team. Read-only access is provided to other users on a need to know basis.

5.2 *Method*

Once an HFE issue has been identified, it is entered into the HFE Issues Tracking Database and is assigned a unique tracking number. Supporting documentation in electronic format may be attached to the database item. The issue is screened and evaluated as appropriate considering importance. Corrective actions to resolve the issue are assigned as necessary. As applicable, due dates for resolution of the overall evaluation or for each corrective action are assigned by the HFE Issues Tracking Database administrator or the issue evaluator. Issues and due dates may be reassigned by the HFE Issues Tracking Database administrator or the HFE RTM as necessary, but approval of the HFE Issues Tracking Database administrator is required for this type of reassignment. Issue closeout with proper documentation is approved by both HFE RTM and the HFE Issues Tracking Database administrator.

5.3 *Documentation*

Each HFE issue or concern that meets or exceeds the threshold established by the design team is entered into the HFE Issues Tracking Database when it is first identified. For each issue, the HFE Issues Tracking Database documents the following:

- Date the issue was entered.
- Any supporting information, such as attachments documenting the issue.
- Assigned issue evaluator and issue owner.
- Proposed resolutions.
- Design team acceptance/rejection.
- Actual resolutions.
- Actions taken.
- Affected documents.

HFE-related design issues which are determined to be deviations from the standard design are placed in the design review and issue resolution process.

5.4 *Responsibility*

The HFE RTM has overall responsible for administering and managing the HFE Issues Tracking Database. The following responsibilities for entering, reviewing, and closing out issues are listed below.

A database administrator is assigned responsibility to manage the database. The administrator does not have to be a member of the HFE team. Each member of the HFE team may be assigned the role of initiator, evaluator, or issue owner.

- HFE RTM:
    - Provide oversight of the HFE issues tracking.
    - Re-assign issue or due date.

- Approve issue resolutions.

- Database Administrator:
  - Manage of database.
  - Maintain hardware and software for optimum performance.
  - Manage security:
    - ♦ Adding / removing users authorized to modify database.
    - ♦ Maintaining database security against unauthorized modifications.
  - Track issue due dates.

- Issue Initiator:
  - Enter issue into database.

- Issue Evaluator:
  - Evaluate issue:
    - ♦ Assign severity level.
  - Assign issue owner (may be individual, team, and / or other disciplines).
  - Assign resolution due date.

- Issue Owner:
  - Resolve issue (design changes will follow the design change control process).
  - Update database with proposed or completed actions.
  - Update design documentation.

6.0 TECHNICAL PROGRAM

6.1 *Implementation Plans, Analyses, and Evaluations*

Implementation plans are written to guide the defining of HFE requirements, designing HSIs and control room layouts, operating procedures and licensed operator training material development, and design, validation, implementation, and monitoring. Each implementation plan provides the interfaces between other HFE programmatic elements, the objectives and scope of the HFE programmatic element, the methodology for conducting the HFE programmatic element, and the results and documentation that will be generated upon completion of the HFE programmatic element. For the U.S. EPR design, an implementation plan is written for each of the following:

- Operating Experience Review.
- Functional Requirements Analysis and Function Allocation.
- Task Analysis (includes Staffing and Qualifications.)
- Human Reliability Analysis.
- Human-System Interface Design.
- Procedure Development.
- Training Program Development.
- Human Factors Verification and Validation.
- Design Implementation.
- Human Performance Monitoring.

6.2 *HFE Requirements*

HFE requirements are documented in implementation plans, SDRDs, and HFE guidelines, such as the HSI Style Guide. The HFE guidelines evolve as the design progresses and provide HFE requirements and consistency during the HSI and control

room design. These guidelines are procedurally required to be followed by all engineering disciplines for such designs activities as: piping and valve layout, local control station design, and environmental conditions will that impact the human.

The design of the HSI shall meet the following basic requirements:

- Operator tasks shall be executable (sufficient time allocated, needed controls and information available).
- The operator shall be able to check the success of an action against the objective of the action.
- The allocated tolerance range (safety limits, time limits, precision) shall be clearly defined.
- Actions that fail or are erroneous shall be recoverable, if possible.
- The operator shall be able to evaluate the system or plant response to a control action. Multiple process monitoring contexts (i.e., physical, functional) are preferred.
- The operator shall be able to evaluate the current safety state of the plant processes from the available displays.

The sections below provide high-level HFE requirements for the design of the HSIs, controls rooms, and other work environments for the operating and maintenance staffs.

6.2.1 *Mechanical Properties and Dimensions for the Work Environment*

The layout of the MCR and other HSI rooms shall meet basic arrangement requirements for information presentation on screens and control panels. The layout of the MCR and other HSI rooms accounts for visibility constraints, accessibility requirements, and communication requirements between the operating and maintenance staff members during all plant states.

Similarly, the layout of the operator workstations (including safety and non-safety HSI) and the POP shall be defined taking into account visibility, reach and grasp

requirements, and anthropometric dimensions for the intended user population. Validation of these design results shall be performed by conducting walk-throughs, using a selected set of emergency procedures, in a mock-up of the MCR.

6.2.2 *Acoustic Environment*

The acoustic environment and the mean noise level in the MCR shall aid operator alertness so that the monitoring and controlling of processes and the associated mental activities are performed in comfort and promote communication between the members of the operating staff.

6.2.3 *Lighting of the HSI Rooms and Workspace*

The lighting in the control rooms shall provide optimum working conditions for personnel by:

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

6.2.4 *Ambient Conditions in the Control Rooms*

During normal operation at basic atmospheric conditions, the temperature and humidity in the MCR and the associated HSI rooms shall be controlled to normal comfort levels. The air-conditioning system shall be able to adjust the temperature. During some design basis events, the temperature in the MCR may exceed comfort levels, but the temperature shall not exceed maximum set by SDD.

6.2.5 *Coding, Language, and Information Presentation*

In order to minimize human error, rules for the arrangement of information on screens and conventional control boards and for coding and labeling of information on the different types of HSIs specified by the HFE team shall be followed. In order to maximize consistency between operating procedures and operator interfaces,

nomenclature and terminology conventions specified by the HFE team shall be followed.

6.2.6 *Requirements for Screen-Based Information Presentation and Dialogs*

Operators are provided with an overview of the plant state and rapid access to specific pieces of information and specific controls. For conventional control boards, this will be accomplished by logical grouping of indicators, alarms, and status displays in functional groupings which provide clear relationships between associated indicators and controls. For the screen-based controls, the organization of operating displays and navigation methods accounts for the limitations of display area and the serial character of information access to provide an overall vision of plant state as well as access to details.

Four principal criteria apply to the design of screen-based HSI:

- The information hierarchy at the top levels shall contain overview displays showing essential plant state information. Lower level displays should progress through increasing levels of detail.
- Multiple monitors shall be used to allow simultaneous display of several types of information.
- Task-oriented presentation of the same information in different arrangements shall be adapted to different operator processes.
- Calculated, pre-processed, and condensed information shall be used to allow a rapid grasp of the state of a complex system (e.g., core average axial power shape monitoring, departure from nuclear boiling ratio (DNBR) and critical heat flux monitoring, plant calorimetric calculation, saturation temperature, saturation pressure, curves and limits for heat-up and cool-down).

The information presentation shall:

- 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).
- Guide the operator from summary information (e.g., from a fault flag or an alarm) to the detailed fault information (e.g., a detailed circuit format) or to the associated procedure or alarm sheet.

6.2.7 *Information Needs and Controls*

Information that allows the operator to evaluate the plant state and provides feedback for any action shall be displayed in a consistent manner.

The operators shall be provided with an appropriate means to interact with screen-based and conventional controls so that, as a minimum, the following types of information are accessible:

- Plant equipment data (fluid, mechanical, electrical, and I&C systems and components).
- Process dynamics.
- Functional relationships between sub-processes.
- Automation equipment functions (e.g., control loops, automatic sequencers, protection systems) and their relation to the state of the process.
- Operational guidance (e.g., procedures and technical data sheets).

Information about the first three types of items shall be communicated to the operators by state and status information and by alarms, irrespective of the technology of the HSI systems.

The operational guidance provided during operations using screen-based HSI systems shall use CBPs. Operational guidance provided during operations from conventional HSI systems shall use PBPs. Aside from the navigation and layout differences and the availability of live data, the computer-based and hard-copy procedures shall contain similar information in a similar format.

6.2.8 *Alarm System*

The alarms alert and inform the operators when unexpected events occur that require manual actions to correct, mitigate, compensate for a failure, make repairs; or when a failure should be accounted for during further process control because either the failure restricts the reachable plant states or requires alternate means of reaching the desired state.

Alarms consist of either binary signals regarding the state of the process or the equipment or acoustic and optical annunciations to alert and guide the operator to the applicable HSI display.

Alarms should be generated when process variables leave their operating range, when equipment is not in the operating mode that is required for the actual process state, or when equipment fails. Status messages (i.e., messages indicating response to process or equipment events) should also be generated within the alarm hierarchy.

The operators shall not be burdened by multiple alarms that demand simultaneous actions; however, operator training establishes the priorities for responding to alarms to maintain a high level of safety. The following factors are examples of criteria that determine how alarm priorities shall be established:

- The available reaction time.
- The safety relevance of the event.
- The relevant impact of the event (e.g., leading to or the imminent loss of a function, degradation of a function).

The following principles shall be applied when designing the logic of alarms and overall alarm processing:

- Alarm signals shall be based on information that indicates the true cause of the reported event. Anticipatory alarms should be included only to signify the impending initiation of a protective function or violation of a setpoint with safety significance. Therefore, anticipatory alarms precede actuation of plant protective functions which are then considered “true cause” of the mitigating action.
- Alarms shall be integrated with the HSI to assist the operator with situational awareness, alarm response, and any associated troubleshooting.
- Alarm signals shall include logic so that only operationally relevant conditions are alarmed (e.g., the alarm logic for "low discharge pressure" downstream of a pump will produce an alarm only if the pump is supposed to be running).
- The overall plant state shall be taken into account for the generation of alarms, or at least to inhibit alarms which are not relevant for the actual plant state.
- Pre-alarms shall be provided before automatic actuation only if manual corrective actions are different from automatic actions and when an operator has sufficient time to identify and perform these actions.

Conventions for alarm processing and presentation on the various screen-based HSI components specified in the style guide shall be followed.

6.2.9 *Plant Operating Procedures*

Besides constituting the means to perform overall process supervision, monitoring and supporting performance of elementary process control actions, procedures provide guidance for more complex tasks. This is accomplished by alarm sheets, procedures for normal operation (including startup and shutdown procedures), and abnormal and accident procedures.

Operating procedures for the U.S. EPR design may use CBPs on the PICS. The CBPs should be implemented in screen-based formats which do not provide control

capabilities. CBPs should include format links to other computer displays to access process information. Format links should provide access to underlying additional information and direct the operator to control screens. CBPs on the PICS should contain means of navigating to appropriate HSI screens necessary to control or monitor response for the required procedure steps. PBPs are provided for the SICS.

The computer- based procedures format of operating procedures shall meet the following requirements:

- Action objectives shall be clearly defined (i.e., the operator shall be able to visualize the current plant or system state and understand the expected result).
- Each applicable procedure step shall establish a given objective, including the parameters used to evaluate the objective, and (where appropriate) indicate the HSI location (screen) for the state of the systems and the required functions. If the action specified in the procedure is performed and the expected response is not achieved, the procedure shall direct the operator to perform mitigating actions.
- The appropriate sequence of actions shall be clear and concise.
- The procedure shall provide concise descriptions for the execution of tasks and actions by providing step-by-step methods of manual execution or referencing the appropriate automated sequences.

Operator guidance shall be structured with several levels of detail (i.e., objectives, tasks, actions).

6.3 *HFE Facilities, Equipment, Tools and Techniques*

The U.S. EPR HFE program uses mockups, part-task simulations (engineering simulators), and full-scope simulators to provide feedback and evaluations on design solutions throughout the design process.

- Mockups – Consist of virtual (use of computer aided drawing software) and physical representations of the HSI.

- Part-task (engineering) Simulations – Consist of simulation of:
  - Part-task Engineering Simulator – Consists of a workstation connected to one or more of the system models (e.g., process, logic) or the plant model.
  - Plant systems' thermodynamics and hydraulics process.
  - Mechanical systems' I&C logic.
  - HSI systems.
  - Electrical systems.
  - Integration of plant system process, system logic, HSI systems, and electrical systems.
  - Plant model (providing complete dynamic plant behavior).
- Full-scope Simulators
  - Full-Scope Engineering Simulator – Consists of operator interface (operating consoles and HSI) in a replica of the control room and is connected to an emulation of the PICS and SICS hardware and the plant model and meets the requirements of 10 CFR 50.34(f)(2)(i) (Reference 8).
  - Training Simulator – Consists of the verified control room and HSI design, verified operating procedures, and verified licensed operator training materials and meets ANSI/ANS-3.5-2009 (Reference 9).
  - Validation Simulator – Consists of operator interface, I&C cabinets, and maintenance / surveillance interfaces and certified according to ANSI/ANS-3.5-2009 (Reference 9).

Other tools and techniques utilized in the HFE program are described in Section 4.2.

7.0 REFERENCES

1. RG 1.174, “An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis.”

2. 10 CFR 50, Appendix A, “General Design Criteria for Nuclear Power Plants.”

3. ANP-10266A-001, “AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR,” AREVA NP Inc., April 2007.

4. NUREG-0737, “Clarification of TMI Action Plan Requirements,” November 1980.

5. 10 CFR 55, “Operators’ Licenses.”

6. 10 CFR 50.120, “Training and qualification of nuclear power plant personnel.”

7 NUREG-0800, Standard Review Plan, Section 13.1.1 “Management and Technical Support Organization”. Rev. 5, 2007.

8. 10 CFR 50.34, “Contents of Application; Technical Information.”

9. ANSI/ANS-3.5-2009, “Nuclear Power Plant Simulators for Use in Operator Training and Examination.”