DESIGN CONTROL DOCUMENT FOR THE

US-APWR

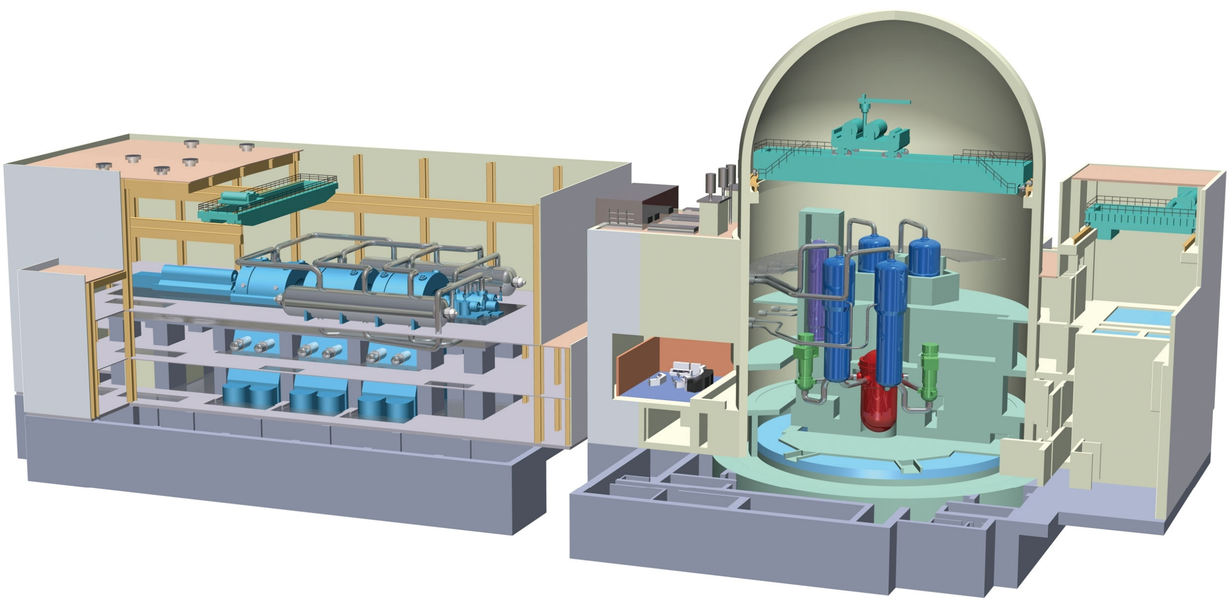
Chapter 18

Human Factors Engineering

MUAP- DC018

REVISION 4

AUGUST 2013



MITSUBISHI HEAVY INDUSTRIES, LTD.

©2013
Mitsubishi Heavy Industries, Ltd.
All Rights Reserved

© 2013

MITSUBISHI HEAVY INDUSTRIES, LTD.

All Rights Reserved

This document has been prepared by Mitsubishi Heavy Industries, Ltd. (“MHI”) in connection with the U.S. Nuclear Regulatory Commission’s (“NRC”) licensing review of MHI’s US-APWR nuclear power plant design. No right to disclose, use or copy any of the information in this document, other than by the NRC and its contractors in support of the licensing review of the US-APWR, is authorized without the express written permission of MHI.

This document contains technology information and intellectual property relating to the US-APWR and it is delivered to the NRC on the express condition that it not be disclosed, copied or reproduced in whole or in part, or used for the benefit of anyone other than MHI without the express written permission of MHI, except as set forth in the previous paragraph.

This document is protected by the laws of Japan, U.S. copyright law, international treaties and conventions, and the applicable laws of any country where it is being used.

Mitsubishi Heavy Industries, Ltd.

16-5, Konan 2-chome, Minato-ku

Tokyo 108-8215 Japan

CONTENTS

TABLES

FIGURES

ACRONYMS AND ABBREVIATIONS

AOO	anticipated operational occurrence
ANS	American Nuclear Society
ANSI	American National Standards Institute
APWR	advanced pressurized-water reactor
BISI	bypassed and inoperable status indication
CAS	central alarm station
CCW	component cooling water
CCWS	component cooling water system
COL	Combined License
CFR	Code of Federal Regulations
CBP	computer-based procedure
CVCS	chemical and volume control system
C/V	containment vessel
DAS	diverse actuation system
DHP	diverse HSI panel
DOE	Department of Energy
DTM	design team manager
ECCS	emergency core cooling system
EFW	emergency feedwater
EOF	emergency operations facility
EOP	emergency operating procedure
ESFAS	engineered safety features actuation system
FA	function allocation
FRA	functional requirements analysis
GDC	General Design Criteria
GOMS	goals, operators, methods, and selection
HA	human action
HED	human engineering discrepancy
HF	human factors
HFE	human factors engineering
HPM	human performance monitoring
HRA	human reliability analysis
HSI	human-system interface
HSIS	human-system interface system
HVAC	heating, ventilation, and air conditioning
I&C	instrumentation and control

ACRONYMS AND ABBREVIATIONS (CONTINUED)

IAEA	International Atomic Energy Agency
ISV	integrated system validation
ITV	industrial television
LCS	local control station
LDP	large display panel
LER	licensee event report
LOCA	loss-of-coolant accident
MCR	main control room
MFW	main feed water
MHI	Mitsubishi Heavy Industries, Ltd.
NRC	U.S. Nuclear Regulatory Commission
NEI	Nuclear Energy Institute
NIS	nuclear instrumentation system
OER	operating experience review
OSD	operational sequence diagram
PA	postulated accident
PAM	post-accident monitoring
PCMS	plant control and monitoring system
PM	project manager
PRA	probabilistic risk assessment
PSF	performance shaping factor
PSMS	protection and safety monitoring system
PWR	pressurized-water reactor
QA	quality assurance
RCP	reactor coolant pump
RCS	reactor coolant system
RG	Regulatory Guide
RHR	residual heat removal
RIHA	risk-important human action
RO	reactor operator
RSC	remote shutdown console
RSR	remote shutdown room
RV	reactor vessel
RWSP	refueling water storage pit
SA	staffing and qualification analysis
SAS	secondary alarm station
SBO	station blackout

ACRONYMS AND ABBREVIATIONS (CONTINUED)

SDCV	specially dedicated continuously visible
SER	significant event report
SFP	spent fuel pit
SG	steam generator
SOER	significant operating experience report
SPDS	safety parameter display system
SRO	senior reactor operator
STA	shift technical advisor
SW	service water
TA	task analysis
TC	thermo couple
TSC	technical support center
V&V	verification and validation
VDU	visual display unit
VTM	V&V team manager

18.0 HUMAN FACTORS ENGINEERING

Section 18.1 through 18.12 describe the US-APWR compliance to the 12 HFE program elements of reference 18.1-7, Human Factors Engineering Program Review Model, NUREG-0711, Revision 2.

18.1 HFE Program Management

18.1.1 General HFE Program and Scope

The US-APWR human factors engineering (HFE) program ensures that an adequate HFE program is developed and that the program is implemented in accordance with NRC approved implementation plans. The HFE program ensures that each human-system interface (HSI) reflects modern human factors principles and satisfies the applicable regulatory requirements.

The general objectives of the HFE program are stated in "human centered" terms which, as the HFE program develops, are defined and used as a basis for HFE test and evaluation activities. The specific HFE program ensures that:

- Personnel tasks are accomplished within the required time and in accordance with specified performance criteria.
- The HSI staffing, qualifications, procedures, training, management and organizational support result in a high degree of operating crew awareness of plant conditions.
- The plant design and allocation of functions results in an integrated HSI design that maintains operational vigilance and provides acceptable workload levels to minimize periods of operator under load and overload.
- The operator interfaces minimize operator error and provide error detection and recovery capability.

The scope of HFE program management includes the following topics:

- HFE design team and organization
- HFE process and procedures
- HFE issues tracking
- HFE technical program
- Combined license (COL) information

This section documents the execution of the HFE process for each topic.

The US-APWR HFE program is accomplished through the activities implemented by the US-APWR HFE team addressed in Section 18.1.2. The US-APWR HFE team uses and implements the US-APWR HFE processes and procedures discussed in Section 18.1.3. The site-specific HFE team is responsible for establishing HFE processes and procedures that maintain the certified US-APWR HFE design in the site-specific as-built plant. The site-specific HFE team is also responsible for the detailed design of the Emergency Offsite Facility (EOF) and for development and implementation of the Human Performance Monitoring program (Section 18.12). The site-specific HFE processes and procedures will be used for all site-specific HFE responsibilities, including HSI design changes after the certified US-APWR design responsibility is officially turned over to the site-specific HFE Team.

18.1.1.1 Assumptions and Constraints Identification

The assumptions and constraints of the design, such as a specific staffing plan or the use of specific HSI technology are inputs to the HFE program in addition to the results of HFE analyses and evaluations. The US-Basic HSIS is the starting point for the US-APWR HSIS; therefore it is considered a constraint of the US-APWR HSIS. The inventory of controls, indications, alarms and procedures needed to operate the US-APWR will be implemented using the HSI components of the US-Basic HSIS. These HSI components include the large display panel, operational visual display units (VDU), alarm VDUs, computer based procedure VDUs, safety VDUs and conventional HSI. The HSI components encapsulate the HSI design bases and methods for control, indication, alarm and procedures. In a broader sense, the US-Basic HSIS encapsulates the general arrangement and integration of these HSI components. These aspects of the US-Basic HSIS will not be changed for the US-APWR HSIS unless something unique for the US-APWR plant requires a change. The design assumptions and constraints of the US-Basic HSI System are clearly identified in Section 5.1.1.2 of Reference 18.1-1. The regulatory requirements applicable to the US-Basic HSI System are listed in Reference 18.1-1, Section 3.0, “Applicable Codes, Standards and Regulatory Guidance”.

A fundamental design constraint of the US-Basic HSIS that also applies to the US-APWR HSIS, is that the plant can be operated with just one reactor operator (RO) and one senior reactor operator (SRO) in the main control room (MCR) during postulated plant operating modes (Reference 18.1-1, Section 4.1.f, Design Basis, MCR Staff). The SRO fulfills the role of MCR Supervisor and STA, during normal operation. This MCR staffing meets the regulatory requirements of 10 CFR 50.54(m)(2)(iii) (Reference 18.1-2). The normal MCR staff is supplemented by one additional SRO and one additional RO that is to be at the plant to accommodate unexpected design conditions, including conditions where the human-system interface system (HSIS) is degraded. In addition, the minimum staff includes one more person present at the facility during its operation with SRO or STA qualifications. During emergency conditions, this person will relieve the MCR Supervisor of either the supervisor or STA responsibilities. The person can be shared by multiple units. The overall plant staffing meets the regulatory requirements of 10 CFR 50.54(m)(2)(i) (Reference 18.1-2). The minimum staffing organization is shown in Figure 18.1-2. While the HSIS is designed to accommodate the minimum MCR and plant staffing described above, the space and layout of the MCR are designed to accommodate the foreseen maximum number of operating and temporary staff.

The maximum MCR operating staff is shown in Figure 18.1-3. In addition, physical and habitability accommodations are provided within the MCR envelope for several active observers. The quantities and expected roles of the observers are defined in Reference 18.1-18, Section 4.2.1.1.

The US-APWR HFE design process is described by Reference 18.1-1, the US-Basic HSIS design, along with References 18.1-12 through 18.1-17. The US-Basic HSIS design has evolved from the Japanese Basic HSIS design, which was applied to Japanese PWRs and is planned to be applied to additional Japanese PWRs. Both designs make extensive use of screen-based digital displays and controls. The US-Basic HSIS consists of generic designs for operator consoles, the large display panel and alarm presentation, display navigation, soft control functions, and layout of display configurations for both safety and non-safety HSIs, as described in Section 4 of Reference 18.1-1. The US-Basic HSIS was developed using an HFE process that includes dynamic testing with multiple crews of US-licensed operators and US HFE experts.

The US-APWR HFE process is conducted based on the US-Basic HSIS foundation and is performed for the US-APWR plant-specific application as described in Reference 18.1-12 (Part 1).

The integrated US-APWR HSIS is developed in accordance with the HFE Program Elements described in Sections 18.2 through 18.12. For the Operating Experience Review (OER), Functional Requirements Analysis/Function Allocation (FRA/FA), and Human Reliability Analysis (HRA) Program Elements, results summary reports are provided in References 18.1-12 and 18.1-13 (Part 2). The TA results report for risk-important human actions (RIHA) for the US-APWR and the Task Analysis Implementation Plan which governs the remaining TA are included in Reference 18.1-12. The remaining HFE Program Elements are conducted in accordance with the HFE Implementation Plans References 18.1-14 through 18.1-17.

18.1.1.2 Applicable Plant Facilities

The HFE program applies to the following areas or facilities:

- MCR
- Remote shutdown room (RSR)
- Technical support center (TSC)
- Local control stations (LCSs) - consideration of HFE activities for LCSs are limited to those LCSs that support:
  - Technical specification activities for surveillance testing, radiological protection, and chemical monitoring
  - Operability restoration (after maintenance or testing) for equipment controlled by technical specifications
  - Emergency and abnormal conditions response
- Emergency operations facilities (EOFs)

Overall HFE issues associated with the central alarm station (CAS) and the secondary alarm station (SAS) are discussed in Section 13.6, Security. The US-APWR HFE program encompasses the interface between the MCR and the CAS/SAS. The US-APWR HFE team determines the information that must be communicated between the CAS/SAS and the MCR, in accordance with regulatory requirements and guidance, and incorporates this information in the HSI design (Sections 18.7, 18.8, and 18.9) and the V&V process (Section 18.10) based on the task analysis process described in Section 18.4. The CAS/SAS design itself, is outside the scope of the US-APWR HFE Implementation Plans.

The communications and information requirements of the EOF will be designed in accordance with the US-APWR HFE program. The US-APWR HFE team determines what EOF information must be transmitted from the plant to the EOF, in accordance with regulatory requirements and guidance, and based on the task analysis process described in Section 18.4. The EOF itself, including the detailed design of EOF displays and corresponding V&V, training and procedures, is outside the scope of the US-APWR HFE Implementation Plans. The EOF facility is designed in accordance with NUREG-0696. The EOF design process specifies the complete EOF facility design, including the method of incorporating the communications and information requirements established by the US-APWR HFE program.The HSI displays at the EOF include the following:

- SPDS
- Meteorological displays
- Off-site radiation monitoring
- Post accident monitoring

18.1.1.3 Applicable HSIs, Procedures and Training

The applicable HSIs, procedures, and training developed and evaluated by the HFE program directly support normal operations and emergency operations for MCR operators, and for auxiliary operators as may be credited in operating procedures. In addition, the HFE program includes the development of HSIs, procedures, and training for surveillance and operability restoration of safety-related plant equipment.

18.1.1.4 Applicable Plant Personnel

Plant personnel positions addressed by the HFE program include licensed control room operators as defined in 10 CFR 55 (Reference 18.1-4) and the categories of personnel defined by 10 CFR 50.120 (Reference 18.1-5). These positions are identified and evaluated in Subsection 18.5.2. In addition, other plant personnel who directly perform surveillance or restoration of safety-related plant equipment and personnel who are specifically credited for accident management are addressed by the HFE program.

18.1.1.5 Effects of Modifications on Personnel Performance

The HFE program addresses the effects that a plant modification may have on personnel performance. The US-APWR HSIS is verified and validated (V&V) and is described in Section 18.10. The HFE Design Implementation Plan, Section 18.11, ensures that design changes occurring after V&V and prior to close-out of all US-APWR pre-fuel load inspections and tests, are evaluated from an HFE perspective. The Human Performance Monitoring program, Section 18.12, evaluates impacts on human performance for design changes occurring after close-out of all US-APWR pre-fuel load inspections and tests. In both cases additional HFE analysis or testing is conducted for design changes, as deemed necessary by the responsible HFE organization, US-APWR HFE team or site-specific HFE team.

18.1.2 HFE Team and Organization

The following section describes the US-APWR HFE team and organization.

18.1.2.1 HFE Responsibility

The US-APWR HFE team is responsible (with respect to the scope of the HFE program) for the following:

- Development of all HFE plans and procedures
- Oversight and review of all HSI design, development, test, and evaluation activities
- Evaluation of problems and solution development for problems identified in the implementation of the HFE activities
- Verification of team implementation recommendations
- Assurance that all HFE activities comply with the HFE plans and procedures
- Scheduling of activities and milestones

18.1.2.2 HFE Organizational Placement and Authority

The primary HFE organization within the US-APWR program is identified below. The organizational structure to manage the HFE team is shown in Figure 18.1-1. When more than one organization is responsible for HFE, the lead organizational unit responsible for the HFE program plan is identified. The team has the authority and organizational placement to provide reasonable assurance that all its areas of responsibility are accomplished and to identify problems in the implementation of the overall plant design. The team has the authority to control further processing, delivery, installation, or use of HFE products until the disposition of a nonconformance, deficiency, or unsatisfactory condition has been achieved.

The roles and responsibilities for the key sections of the organization are as follows:

- Engineering Management Director (EMD)

  The EMD is responsible for controlling engineering resources/organizations and directing responsible organizations to resolve critical design or engineering issues that include human factor engineering issues.

- HFE Manager

  The HFE Manager assures that all HFE elements are appropriately implemented in accordance with the HFE implementation plans.

  The HFE manager is responsible for organizing the HFE team, oversight of the HFE processes, and controlling HFE resources.

- HSIS Design Team Manager (DTM)

  The DTM is responsible for implementing all of the HFE elements with the exception of the V&V, which is the responsibility of the HSIS V&V Team Manager.The design team conducts all design activities for hardware and software. The DTM assures that the design team correctly performs design activities based on the technical requirements and the development process in accordance with Reference 18.1-6. The DTM is also responsible for:

  - Implementing all HFE elements with the exception of the V&V
  -
  - Assuring HFE activities comply with HFE plans and procedures
  - Scheduling activities
  - Developing methods for identifying, closing, and documenting human factors issues
  - Controlling HSI design and HFE documentation configuration

- HSIS V&V Team Manager (VTM)

  The HSIS V&V team manager is responsible for all activities of the V&V team. The V&V team manager ensures sufficient resources are available, and: ensures that V&V activities are not adversely affected by commercial and schedule pressures. The HSISVTM ensures that the HSIS V&Vs are conducted in accordance with the US-APWR HSIS V&V implementation plan described in Section 18.10.

- QA Organization

  The Quality Assurance (QA) organization establishes QA procedures and conducts periodic QA audits of the US-APWR HFE program to ensure the HFE program is conducted in accordance with applicable licensing commitments, including Implementation Plans. Where HFE activities are performed by suppliers, the QA organization audits supplier HFE activities.

The HSIS design team is directly responsible for the design of the HSI for the MCR, RSR and TSC. This includes approval of man-machine allocations for functions controlled and monitored from these facilities. The HFE team also approves the designs of HSIS outside these facilities for safety-related plant equipment (see Section 18.1.1.3). To effectively execute these responsibilities, the HFE team's role and position within the overall MHI engineering organization are described in Reference 18.1-12, Part 1, Section 3.2.

18.1.2.3 HFE Organizational Composition

This section describes the organizational composition of the US-APWR HFE team.

18.1.2.3.1 HSIS Design Team Organizational Composition

The HSIS design team conducts all design activities for HSIs. The HSIS design team consists of a multi-disciplinary technical staff. The team is under the leadership of an individual experienced in the management of the design and operation of complex control technologies. The HSIS design team technical disciplines include:

- HFE
- Technical project management
- Systems engineering
- Nuclear engineering
- Instrumentation and control (I&C) engineering
- Architect engineering
- Plant operations
- Computer system engineering
- Plant procedure development
- Personnel training
- Systems safety engineering
- Maintainability/inspectability engineering
- Reliability/availability engineering

The term "HSIS design team" is used in a generic sense to refer to the personnel who are contributors for HSIS design. Many of the technical disciplines listed above are assigned to support HSIS design on a "matrixed" basis, but report organizationally through other technical groups.

These HFE disciplines are organized into separate groups for HFE Analysis and HSI Design, Procedure Development and Training Development. Each group is under a technical leader who reports to the HSIS DTM. These groups mutually support the production of an integrated US-APWR HSIS design product, and have access to other engineering support, as needed, and may be augmented by subcontractor support, as the workload requires. These groups integrate the development of scenarios for human reliability analysis (HRA) evaluations, task analyses, HSI tests and evaluations, validation, and other HFE-related evaluations.

18.1.2.3.1.1 HFE Analysis and HSI Design

This group performs human factors analyses, develops HSI designs based on human factors principles, guidelines, and standards, and participates in the resolution of identified human factors problems.

18.1.2.3.1.2 Training Development

This group develops content and format for personnel training programs for licensed and non-licensed plant personnel and coordinates training issues arising from activities such as HRA, HSI design, and procedure design.

18.1.2.3.1.3 Procedure Development

This group develops operating and emergency operating procedures (EOPs), procedure aids, and computer-based procedures (CBPs), based on analysis of operational tasks. The group establishes procedure formats, based on emergency procedure guidelines and operational procedures from current and predecessor plants.

18.1.2.3.1.4 Plant Operations Support

The plant operations group personnel provide practical nuclear plant operating knowledge to the other HFE groups so that HSIs are fully integrated. These personnel provide knowledge of operational activities including task characteristics, HSI characteristics, environmental characteristics, and technical requirements related to operational activities. The Plant Operations Support personnel act as an information resource in support of other HSI design activities, and obtain and evaluate engineering information for HSI development, procedures, and training groups.

18.1.2.3.2 HSIS V&V Team Organization Composition

The HSIS V&V team conducts the HSI V&Vs in accordance with the US-APWR HSI V&V Implementation Plan (Reference 18.1-15). The HSI V&V team includes personnel with the following technical skills:

- HFE
- Plant operations
- Operator training
- HSI design

The V&V team adds other technical disciplines as needed during the V&V process.

18.1.2.4 HFE Personnel Qualifications

The minimum qualifications of HFE team personnel are documented in Reference 18.1-12. The HFE team contains HFE experts, I&C experts, and nuclear plant process, systems, and operations experts. Experts have at least 10 years of nuclear experience in their expert field and an education background that supports their expert credentials. US-licensed reactor operators and senior reactor operators are integrated into the HFE team. Personnel qualifications are controlled by Reference 18.1-6.

The requisite professional experience is satisfied by the HFE design team. It is recognized that one person may possess multiple skills and that people may have additional responsibilities beyond the HFE design team. The roles and responsibilities for the key sections of the organization are described in Reference 18.1-12, Part 1 Section 3.2.

Alternative personal credentials may be accepted as the basis for satisfying the minimum personal qualification. Acceptance of alternative personal credentials is evaluated on a case-by-case basis and approved, documented, and retained in auditable project files as described in Reference 18.1-6.

18.1.3 HFE Processes and Procedures

HFE activities are performed in accordance with documented processes (i.e., results reports, implementation plans or implementing procedures) that are executed under the QA Program for the US-APWR (Reference 18.1-6). The documents control the HFE processes described below. Processes for each HFE program element are described in Sections 18.2-18.12.

18.1.3.1 General Process Procedures

The processes through which the team executes its responsibilities include procedures for:

- Assigning HFE activities to individual team members
- Governing the internal management of the team
- Making management decisions regarding HFE
- Making HFE design decisions
- Governing equipment design changes
- Reviewing HSI designs

All HFE processes and procedures are developed and performed as described in Reference 18.1-6.

18.1.3.2 Process Management Tools

Verification tools and techniques (e.g., review forms) utilized by the team to ensure that they fulfill their responsibilities are identified. HFE analytical procedures and associated engineering documentation developed and controlled are described in Reference 18.1-6.

18.1.3.3 Integration of HFE and Other Plant Design Activities

The integration of design activities uses inputs from other plant design activities to the HFE program and the outputs from the HFE program to other plant design activities. The iterative nature of the HFE design processes is addressed. HFE design controls are described in Reference 18.1-6. The work process used by the HFE team to interact with other plant design organizations is described in Reference 18.1-12, Part 1 Section 5.

18.1.3.4 HFE Program Milestones

HFE program milestones are used to evaluate HFE program effectiveness at critical checkpoints, and the relationship to the integrated plant sequence of events is identified. An integrated program plan showing the correlation between HFE elements and activities, products, and reviews has been developed (Reference 18.1-12, Part 1, Section 5). The schedules and milestones are shown in Reference 18-12, Part 1, Section 5, Attachment-2.

18.1.3.5 HFE Documentation

Controlled HFE design documents are identified and briefly described, and the procedures for retention and access of these documents are defined. HFE document control is described in Reference 18.1-6.

18.1.3.6 Subcontractor HFE Efforts

HFE requirements are included in each subcontract for HFE support, and the subcontractor’s compliance with HFE requirements is periodically verified. HFE work performed by subcontractors is controlled as described in Reference 18.1-12, Part 1, Section 5 and 18.1-6.

18.1.4 HFE Issues Tracking

The HFE issues tracking system is integrated into the existing tracking system used for the US-APWR design effort as a whole. The HFE issues tracking system addresses human factors issues that are (a) known to the industry and (b) identified throughout the execution of the US-APWR HFE program elements.

The HFE issues tracking system provides a mechanism to address the items that need to be addressed later in the project to ensure that they are not overlooked. The HFE issue tracking system provides assurance that HFE issues are tracked from identification until resolution has been fully documented and approved by an independent Expert Panel. Resolutions include testing where the adequacy of the resolution cannot be expertly judged or where the problem resulted in failure of a previous test. The process ensures the potential for negative effects on human performance is reduced to an acceptable level.

The HFE issues and concerns that are not immediately resolved are entered in the HFE issues tracking system. These issues are referred to as Human Engineering Discrepancies (HED). The HFE design team members are responsible for issue logging, tracking, resolution, and resolution acceptance. HEDs are tracked and dispositioned as required by Reference 18.1-6.

The problem and resolution are thoroughly detailed and documented. Where testing is deemed necessary the resolution includes testing requirements. The resolution is approved by both the HSI Design Team and the independent HFE Expert Panel.

The process through which the HFE design team executes its responsibilities is described in Reference 18.1-12, Part 1, Section 6 and Section 7. In various HFE documents, HFE issues are also referred to as Human Engineering Discrepancies (HED). HEDs are tracked to closure using an HED database, as described in Reference 18.1-12 (Part 1, Section 6).

18.1.5 HFE Technical Program

The HFE technical program is performed in accordance with the HFE process specified in the US-APWR HFE implementation plan (Reference 18.12, Part 1, Section 8).

The US-APWR HFE program is divided into three phases.

1. Phase 1 yields the US-Basic HSIS. This generic design is applicable to the US-APWR and US plant modernizations, as defined by Reference 18.1-1. The US-Basic HSIS does not include a specific plant HSI inventory of alarms, displays and controls. Phase 1 culminates in NRC approval of the topical report that defines the US-Basic HSIS design, Reference 18.1-1.

2. Phase 2 develops the US-APWR inventory of alarms, displays and controls, and combines that with the US-Basic HSIS to yield the US-APWR HSIS. The US-APWR HSIS is a generic design applicable to all US-APWRs. The US-APWR encompasses the total plant, including portions of the plant that are defined by the DCD as site-specific, such as the switchyard and ultimate heat sink. For these portions, plant system design assumptions are made that are either confirmed or changed in Phase 3. Phase 2 culminates with integrated system validation (ISV) of the US-APWR HSIS using a full scope dynamic simulator, as described in Section 18.10.

3. Phase 3 makes changes to the US-APWR HSI inventory, as may be needed to reflect site-specific systems. These changes yield a site-specific HSIS. There are no changes to the US-APWR inventory for generic portions of the plant, and no changes to the US-Basic HSIS. Phase 3 includes development of a full scope site-specific dynamic simulator. Phase 3 culminates with training and licensing of site-specific operators.

The general development process, is shown in Figure 18.1-4.

In Phase 1, the US-asic HSI is verified and validated as documented in Reference 18.1-13, Part 1 and Reference 18.1-12, Part 3. Phase 1a also includes an Operating

Experience Review (OER) to ensure the design includes features that encompass resolutions to nuclear industry issues and issues from other industries that also employ digital HSI. The OER results summary report is documented in Reference 18.1-13 Part 2.

In Phase 2, the US-APWR HSIS inventory is developed. The inventory is based on:

- OER, whose results summary report is documented in Reference 18.13, Part 2.
- FRA/FA and HRA, whose results summary reports are documented in Reference 18.1-12, Part 2
- TA (for risk important human actions), whose results report is documented in 18.1-12, Part 2.
- TA (for remaining human actions), whose implementation plan is documented in Reference 18.1-12, Part 2
- MCR minimum staffing, which is a US-APWR design constraint that is also confirmed through the Staffing and Qualifications Implementation Plan, Reference 18.1-18
- HSI Design, whose implementation plan is documented in Reference 18.1-14
- Procedure Development, whose implementation plan is documented in Reference 18.1-15

Also in Phase 2, the complete US-APWR HSIS, US-APWR inventory combined with US-Basic HSIS is verified and validated. The V&V implementation plan is documented in Reference 18.1-15.

In Phase 3, operators are trained, the US-APWR HSIS is implemented, and a human performance monitoring program is established, all for the site-specific plant. The implementation plans for these activities are documented in References 18.1-16 and 18.1-17, respectively.

The program’s eleven HFE elements are:

- Operating experience review (OER)
- Functional requirements analysis and function allocation
- Task analysis
- Staffing and qualifications
- HRA
- HSI design

- Procedure development
- Training development
- Human factors verification and validation
- Design implementation
- Human performance monitoring

The HFE standards and specifications, which are sources of HFE requirements imposed on the design process, are identified and described in Reference 18.1-1, Chapter 3.0, “Applicable Codes, Standards and Regulatory Guidance”.

The HSI design activities rely on the development of dynamic models for evaluating the overall plant response as well as the performance of individual control systems, including operator actions. The dynamic models are used to:

- Analyze steady state and transient behavior
- Confirm the design of the advanced alarm system concepts
- Confirm the adequacy of control schemes
- Confirm the allocation of control functions to a system or an operator
- Validate plant operating procedures
- Develop full-scope and part-task simulators for ISV and operator training

Part-task or engineering modeling/simulation is used to develop an initial set of plant control parameters, including the development of associated graphical user interfaces. The part-task simulator is used in the preliminary US-APWR design and then expanded to include specific US-APWR design features. As the US-APWR design progresses, the part-task simulator proceeds through a series of iterative evaluations, resulting in the development of a full-scope control room simulator. The simulator facility is the focal point for HFE development, engineering design verification, and operator evaluations/validation throughout the HSI design process.

Modifications to the approved US-APWR HSIS design will meet current regulations, except where specific exemptions are requested under 10 CFR 50.12 (Reference 18.1-8) or 10 CFR 2.802 (Reference 18.1-9), and are controlled as described in Reference 18.1-6.

Modifications to the approved US-APWR HSIS design will not compromise defense-in-depth. Defense-in-depth is one of the fundamental principles upon which the plant will be designed and built. Defense-in-depth is important in accounting for uncertainties in equipment and human performance, and for ensuring that some protection remains even when significant breakdowns occur in particular areas.

Defense-in-depth elements may be changed, but are maintained overall. The following important aspects of defense-in-depth, as identified in Regulatory Guide (RG) 1.174 (Reference 18.1-10), maintained throughout the US-APWR design are:

- A reasonable balance is preserved among prevention of core damage, prevention of containment failure, and consequence mitigation.
- There is no over-reliance on programmatic activities to compensate for weaknesses in plant design. This may be pertinent to changes in credited human actions (HAs).
- System redundancy, independence, and diversity are preserved commensurate with the expected frequency, consequences of challenges to the system, and uncertainties (e.g., no risk outliers).
- Defenses against potential common cause failures are preserved, and the potential for the introduction of new common cause failure mechanisms is assessed. Caution is exercised in crediting new HAs to verify that the possibility of significant common cause errors is not created.
- Independence of barriers is not degraded.
- Defenses against human errors are preserved. For example, procedures are established for providing a second check or independent verification for risk-important HAs to determine that they have been performed correctly.
- The intent of general design criteria (GDC) in 10 CFR Part 50, Appendix A (Reference 18.1-11), are maintained. The relevant GDC are:
    - GDC 3 – Fire Protection
    - GDC 13 – Instrumentation and Control
    - GDC 17 – Electric Power Systems
    - GDC 19 – Control Room
    - GDC 34 – Residual Heat Removal
    - GDC 35 – Emergency Core Cooling System
    - GDC 38 – Containment Heat Removal
    - GDC 44 – Cooling Water
- Safety margins are often used in deterministic analyses to account for uncertainty and incorporate added margin to provide adequate assurance that the various limits or criteria important-to-safety are not violated.

18.1.6 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.1(1) Deleted

COL 18.1(2) Deleted

18.1.7 References

18.1-1 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 5, November 2011.

18.1-2 Conditions of Licenses, NRC Regulations Title 10, Code of Federal Regulations, Part 50.54.

18.1-3 Wood, R. T., et al., Advanced Reactor Licensing: Experience with Digital I&C Technology in Evolutionary Plants, NUREG/CR-6842, March 2004.

18.1-4 Operators' Licenses, NRC Regulations Title 10, Code of Federal Regulations, Part 55.

18.1-5 Training and Qualification of Nuclear Power Plant Personnel, NRC Regulations Title 10, Code of Federal Regulations, Part 50.120.

18.1-6 Quality Assurance Program (QAP) Description for Design Certification of the US-APWR, PQD-HD-19005, Revision 5, Mitsubishi Heavy Industries, Ltd., May 2013.

18.1-7 Human Factors Engineering Program Review Model, NUREG-0711, Revision 2, U.S. Nuclear Regulatory Commission, Washington, DC, February 2004.

18.1-8 Specific Exemptions, NRC Regulations Title 10, Code of Federal Regulations, Part 50.12.

18.1-9 Petition for Rulemaking, NRC Regulations Title 10, Code of Federal Regulations, Part 2.802.

18.1-10 An Approach for Using Probabilistic Risk Assessment in Risk-Informed Decisions on Plant-Specific Changes to the Licensing Basis, Regulatory Guide 1.174, Revision 1, November 2002.

18.1-11 General Design Criteria for Nuclear Power Plants, NRC Regulations Title 10, Code of Federal Regulations, Part 50, Appendix A.

18.1-12 US-APWR HSI Design, MUAP-09019-P (Proprietary) and MUAP-09019-NP (Non-Proprietary), Revision 2, September 2012.

18.1-13 US-APWR Human System Interface Verification and Validation (Phase 1a), MUAP-08014-P (Proprietary) and MUAP-08014-NP (Non-Proprietary), Revision 1, May 2011.

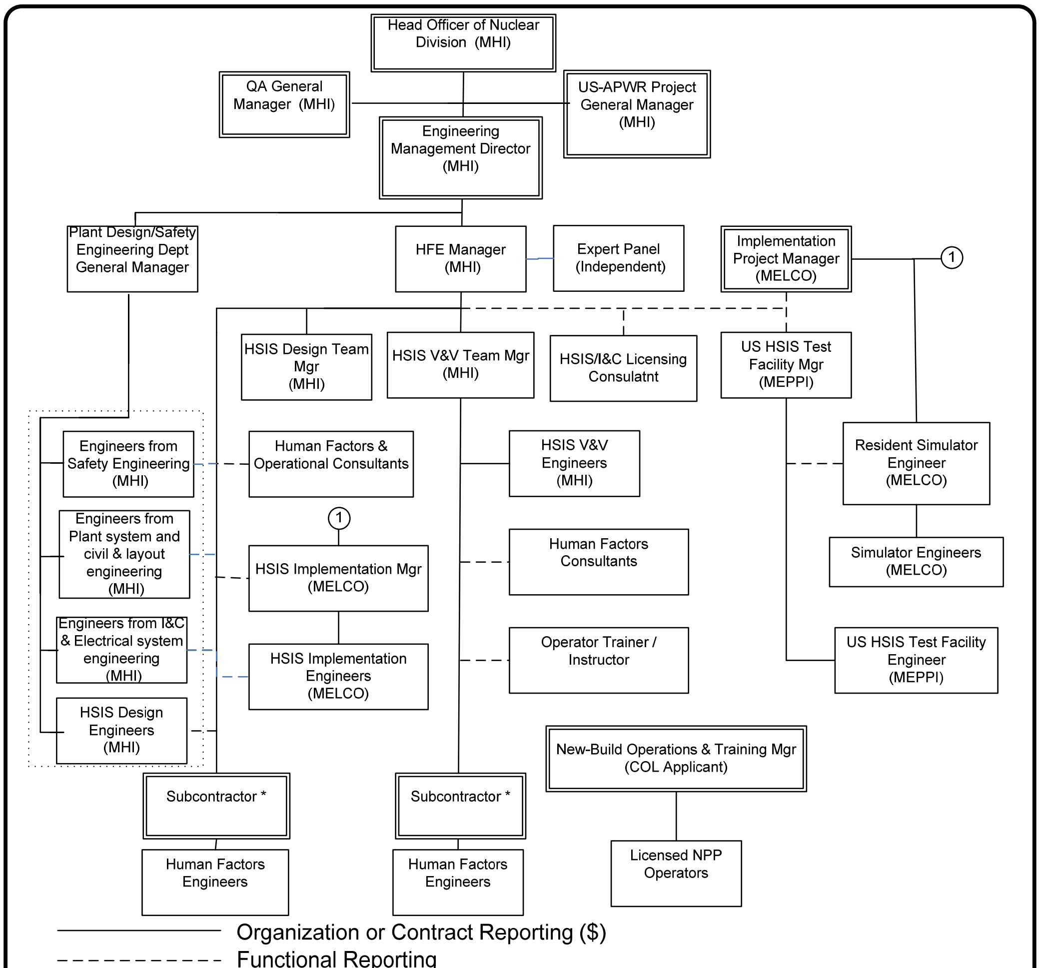
18.1-14 US-APWR HSI Design Implementation Plan, MUAP-10009, Revision 2, September 2012.

18.1-15 Verification and Validation implementation plan, MUAP-10012, Revision 2, September 2012.

18.1-16 Design Implementation, MUAP-10013, Revision 2, September 2012.

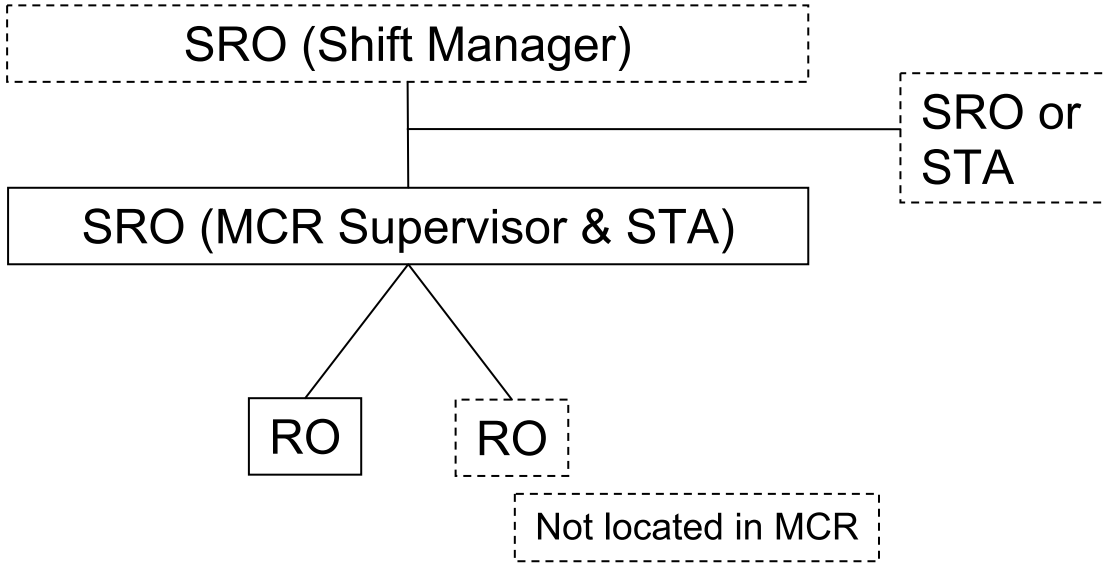
18.1-17 Human Performance Monitoring Implementation Plan, MUAP-10014, Revision 2, September 2012.

18.1-18 US-APWR Staffing & Qualifications Implementation Plan (MUAP-10008), Revision 2, September 2012.



* Responsibilities are delegated to subcontractors at the discretion of MHI's HSIS Design and V&V Managers and by contractual agreement.

Figure 18.1-1 HFE Team Organization



Note: STA: shift technical advisor

Figure 18.1-2 Operations Personnel Staffing and Organization (Minimum)

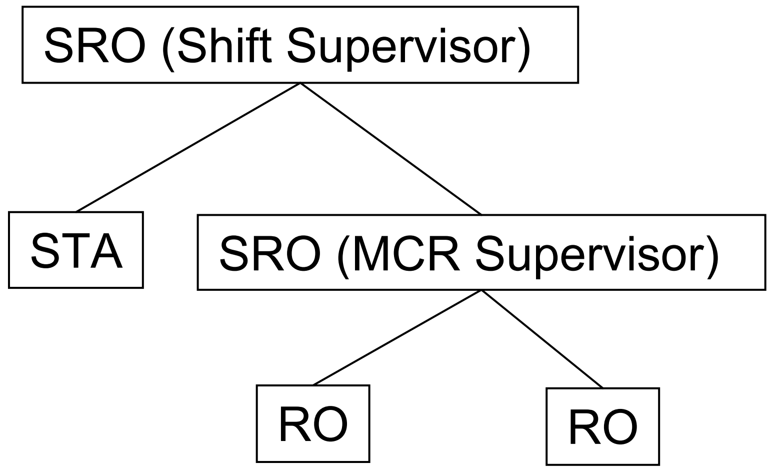


Figure 18.1-3 Operations Personnel Staffing and Organization (Maximum)

Note: MCR also accommodates several active observers, see Reference 18.1-18

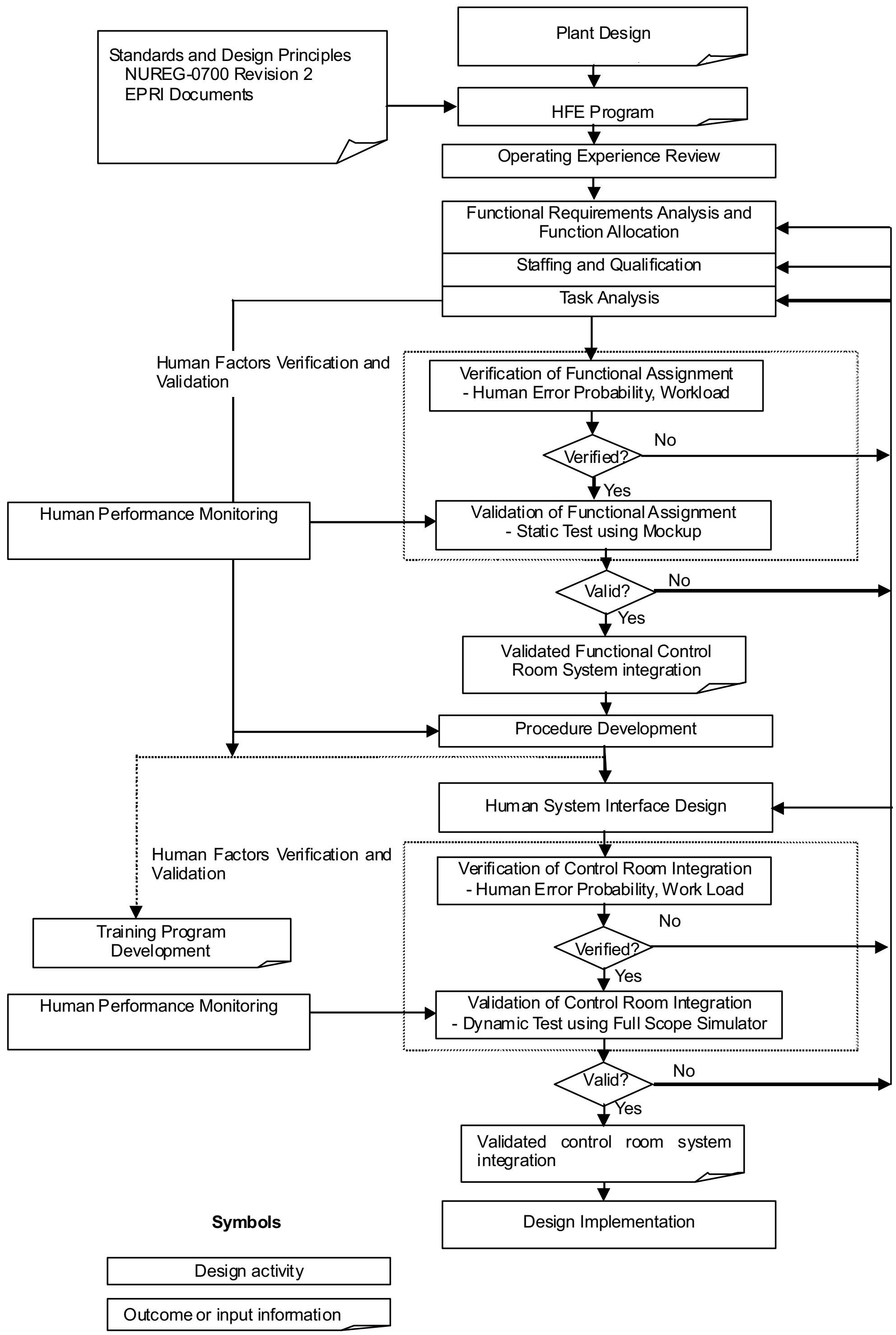


Figure 18.1-4 Overall HFE Design Process

18.2 Operating Experience Review

18.2.1 Objectives and Scope

The objective of the HFE Operating Experience Review (OER) is to identify and analyze HFE-related problems and issues encountered in previous nuclear plant designs that are similar to the US-APWR, so that the negative features are not repeated and positive features are retained. Since the nuclear industry lacks significant experience with the modern HSI technology used in the US-APWR, the OER also encompasses the utilization of similar digital HSI technologies from other process industries.

This review includes information pertaining to the human factors issues related to the predecessor plant(s) or highly similar plants and plant systems. Recognized nuclear industry HFE issues and the issues related to HFE technology are included in the review. Issues related to advanced reactor design, as contained in Reference 18.2-1, are addressed. Personnel interviews with US licensed plant operators, conducted during Phase 1a V&V testing, were used to determine operating experience related to predecessor plants or systems. The OER identifies where risk-important human errors have occurred.

The OER is documented in US-APWR operating experience results report, Reference 18.2-3 (Part 2). The methodology for performing the HFE OER and integrating it into the HFE analyses is described below.

18.2.2 Methodology

18.2.2.1 OER Process

OER is the examination and evaluation of specific industry-operating experience related to system and human performance for systems similar to the system under review. The technique entails the review of the following data sources:

- Licensee event reports (LERs)
- Significant event reports (SERs)
- Significant operating experience reports (SOERs)
- Plant corrective action reports (see Section 18.2.2.2)
- Operational and maintenance logs and records (see Section 18.2.2.2)
- Data from interviews with experienced plant personnel

A structured evaluation is conducted to determine the applicability of the operational data to each human factors issue. This evaluation is performed by an HFE team of subject matter experts drawn from the technical disciplines described in Section 18.1. The evaluation data and process are recorded on the form shown in Reference 18.2-3, Table 5. Issues identified during the OER were evaluated to identify:

- Human performance issues, problems, and sources of human error
- Design elements that support and enhance human performance

Each operating experience item is evaluated to determine if the issue is applicable to the US-Basic HSIS, the US-APWR HSIS or the US-APWR plant design, and if the issue is already addressed in these designs. Each operating experience item determined to be appropriate for incorporation in the design (but not already addressed in the design) is documented in the HFE issues tracking system, as described in Section 18.1.4. HFE issues are resolved through design changes, procedure changes or training changes (or a combination of changes) as described in Sections 18.7, 18.8, and 18.9, respectively.

18.2.2.2 Predecessor Plants and Systems

The HSI for the US-APWR is based on the following predecessor plant designs:

- Japanese conventional 3-loop PWR with full digital I&C and HSI: this plant is operating
- Japanese 4-loop APWR with full digital I&C and HSI: this plant is under licensing
- Japanese conventional 2-loop PWR with full digital I&C and HSI modernization: this plant is operating

All of these plants utilize the Japanese Basic HSIS design, which is the starting point for development of the US-Basic HSIS design. The US-Basic HSIS design is the foundation of the US-APWR HSIS design. The OER process for this standard HSI design and the expanded OER that led to the HSI design for the US-APWR is shown in Figure 18.2-1.

The contribution of the OER process to the standard Japanese Basic HSIS design includes two major operating experience inputs:

- LERs and SERs from the currently operating Japanese PWRs
- Plant corrective action systems, operating logs, and maintenance logs from the currently operating Japanese PWRs

The standard Japanese Basic HSIS design is the predecessor of the US-APWR HSI design. The US-APWR also reflects an expansion of the OER that includes:

- LERs for US nuclear reactors, as described in Reference 18.2-1 (described in Subsection 18.2.2.5)
- LERs and SERs for US nuclear reactors that have been issued since the issuance of Reference 18.2-1
- Data from interviews with experienced plant personnel from US plants currently operated by anticipated US-APWR licensees.

The following are the key differences between the standard Japanese Basic HSIS and the HSI for the US-APWR:

- Arrangement of the main control room operator console to accommodate the change from one to two reactor operator stations
- Accommodating the change from two-train to four-train design
- HSI details to accommodate specific plant mechanical and electrical systems
- Japanese to English language conversion
- Metric to English unit conversions
- Ergonomics changes to operator consoles to accommodate American personnel
- Additional safety visual display units to improve situation awareness during degraded HSI conditions
- Addition of automatic data checking to computer-based procedure (CBP) system. It is noted that this is a US-APWR specific change from the CBP system of the US-Basic HSIS described in Reference 18.2-2. Automated data checking has been added to specifically reduce human performance errors when executing procedures. The potential for these errors and this resolution was identified during evaluation of HFE issues from Phase 1b V&V, Reference 18.2-4 (Part 3, Section 5.1).

The HFE design aspects incorporated in the US-APWR from previous or predecessor plant designs are clearly identified in the US-APWR operating experience review report. The HFE-related problem resolutions, including supporting analysis and corrective designs are provided. In addition, a discussion of positive HFE features that were identified, evaluated, and retained is provided.

18.2.2.3 Risk-Important Human Errors

The OER identifies risk important human errors from predecessor plants that are also applicable to the US-APWR. The OER provides justification for risk-important human errors from predecessor plants that are not applicable.

18.2.2.4 HFE Technology

The OER addresses related HFE technology. For example, touch screen interfaces, large-screen wall panel displays, electronic maintenance tagging systems, and computerized procedures are utilized in the standard Japanese Basic HSIS and the US-APWR HSI, as described in Reference 18.2-2. HFE issues associated with their use are reviewed, including HFE design aspects used in other industries. There are no technology differences between the standard Japanese Basic HSIS and the US-Basic HSIS.

Within this context, technology refers to the human interface aspect of the technology, not the hardware or software. For example, the use of rear projection video technology or flat screen plasma or liquid crystal display technology would not affect the human interface. Therefore these are considered the same technology. Alternately, due to parallax issues, the use of infrared touch screen technology vs. surface acoustic touch screen technology would affect the human interface. Therefore these are considered human interface technology differences.

18.2.2.5 Recognized Industry Issues

The recognized industry issues contained in Reference 18.2-1 and issues subsequent to the publication of Reference 18.2-1 are addressed. These issues are organized into the following categories:

- Unresolved safety issues/generic safety issues
- Three Mile Island issues
- NRC generic letters and information notices
- Reports of the former NRC Office for Analysis and Evaluation of Operational Data
- Low power and shutdown operations
- Operating plant event reports

18.2.2.6 Issues Identified by Plant Personnel

Personnel interviews were conducted to determine operating experience related to predecessor plants or systems. Interview feedback was provided in the following topics or areas:

- Plant Operations
    - Normal plant evolutions (e.g., startup, full power, and shutdown)
    - Instrument failures (e.g., safety-related system logic and control unit, fault tolerant controller (nuclear steam supply system), data network bus system, network bus controller, and break in data network line)
    - HSI equipment and processing failure (e.g., loss of video display units, loss of data processing, or loss of large overview display)
    - Transients (e.g., turbine trip, loss of offsite power, station blackout, loss of all feedwater, loss of service water, loss of power to selected buses or control room power supplies, and safety/relief valve transients)
    - Accidents (e.g., main steam line break, positive reactivity addition, control rod insertion at power, control rod ejection, anticipated transients without scram, and various-sized loss-of-coolant accidents)

- Reactor shutdown and cooldown using remote shutdown system

- HSI Design Topics
  - Alarm and annunciation
  - Display
  - Control and automation
  - Information processing and job aids
  - Real-time communications with plant personnel and other organizations
  - Procedures, training, staffing/qualifications, and job design

18.2.2.7 Issue Analysis, Tracking, and Review

Issues identified during the OER are entered into the HFE issues tracking system. Each OER issue that is determined to be unresolved by the US-Basic HSIS, the US-APWR HSI Inventory or the US-APWR plant design is documented in the HFE issues tracking system, as described in Section 18.1.4. The HFE issues tracking system provides the appropriate level of reviews to ensure that issues are tracked to completion.

18.2.3 Results

The results from the HFE OER analysis are documented in the US-APWR operating experience review results summary report (Reference 18.2-3, Part 2). Issues applicable to the US-APWR are documented along with descriptions of how those issues are resolved by the US-APWR HSIS. Unresolved HFE issues identified during the OER are documented and tracked for subsequent resolution. (Reference 18.2-3)

18.2.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

18.2.5 References

18.2-1 Higgins, J. and Nasta, K., HFE Insights For Advanced Reactors Based Upon Operating Experience, NUREG/CR-6400, December 1996.

18.2-2 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 5, November 2011.

18.2-3 Human System Interface Verification and Validation (Phase 1a), MUAP-08014-P (Proprietary) and MUAP-08014-NP (Non-Proprietary), Revision 1, May 2011.

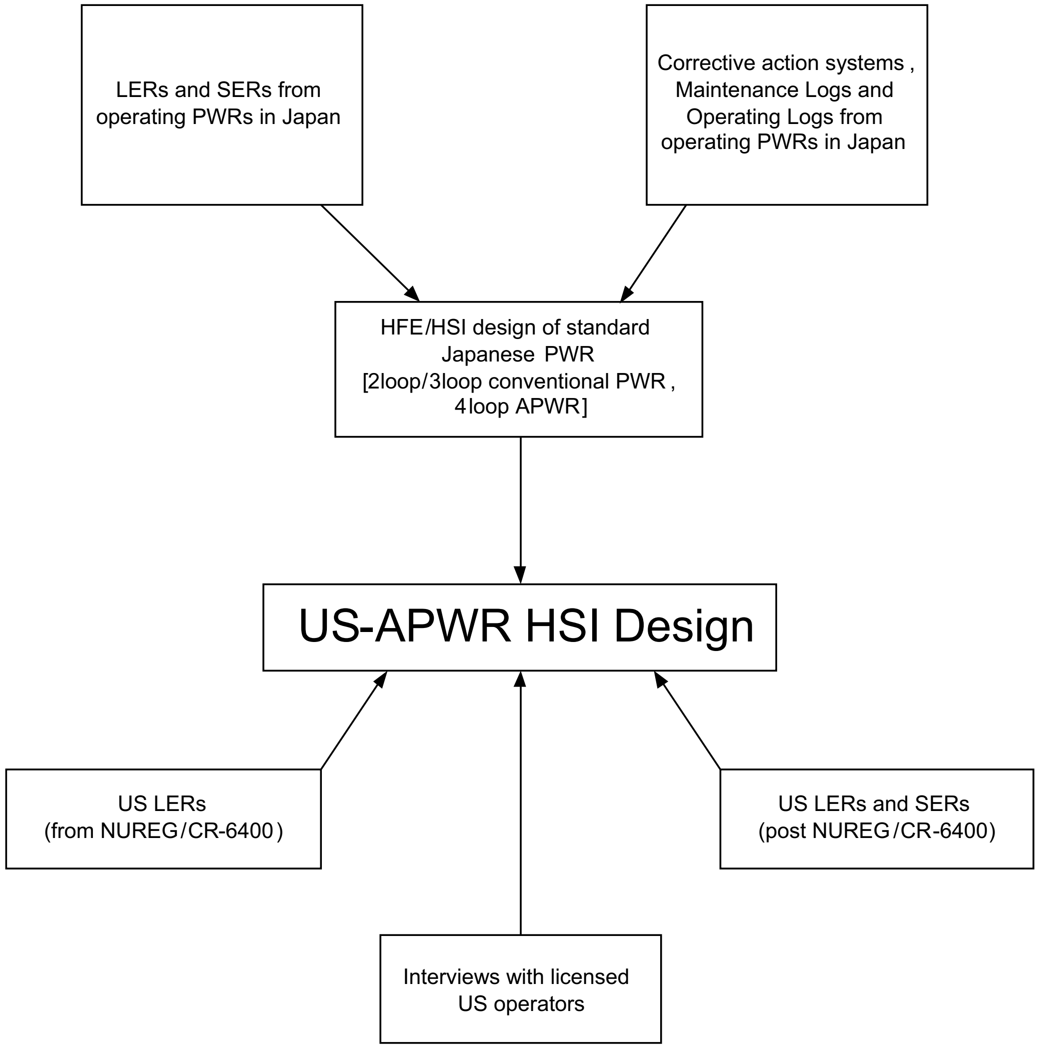


Figure 18.2-1 US-APWR OER Process

Table 18.2-1 Examples of Issues and Resolutions from US-APWR OER Report (Sheet 1 of 3)

No.	Item	Issue/Scope	Human Factor Aspect Issue	Human Factor Issue addressed by US-APWR
1	A-44	Station blackout (SBO)	This is a large and significant issue with many human factors-related aspects, including controls, displays, training, and procedures.	In US-APWR, safety I&C system allows operators to maintain longer term hot shut down condition and transition and maintain cold shutdown. Safety grade HSI system provides all safety component controls and monitoring of safety functions, and provides all safety related plant information to operators. Safety I&C system power, including safety grade HSI system, is supplied by a class 1E safety grade voltage line which power on at least one train cannot be lost under SBO condition. Safety HSI system is located at the operator console in the MCR and at the remote shutdown console outside of MCR. In addition, though it is not necessary to maintain the power supply for safety shutdown transition, non safety HSI system is also available for thirty minutes under SBO condition.
2	A-47	Safety implications of control systems	This issue relates to the implications of failures of non safety-related control systems and their interaction with control room operators.	MUAP-07004-P, "Safety I&C System Description and Design Process" Subsection 5.1.8 ensures non safety system failure does not affect the safety system which credits plant safety functions. The implications of failures of non safety-related control systems and their interaction with control room operators are addressed in "HSI System Description and HFE Process" Section 4.11, "Response to HSI Equipment Failures".
3	B-17	Criteria for safety-related operator actions	This issue involves the development of a time criterion for safety-related operator actions including a determination of whether automatic actuation is required. This issue also concerns some current pressurized water reactor designs requiring manual operations to accomplish the switchover from the injection mode to the recirculation mode, after a loss-of-coolant accident (LOCA).	Defense-in-depth and diversity coping analysis provides a time criterion for safety-related operator actions. In accordance with this analysis, if actions are needed earlier than 10 minutes, the function is generally automated. Any operator actions credited prior to 30 minutes are justified based on EOP and task analysis. Transfer actions from the injection mode to the recirculation mode after LOCA are generally automated.

Table 18.2-1 Examples of Issues and Resolutions from US-APWR OER Report (Sheet 2 of 3)

No.	Item	Issue/Scope	Human Factor Aspect Issue	Human Factor Issue addressed by US-APWR
4	B-32	Ice effects on safety-related water supplies	The buildup of ice on service water intakes can occur gradually and can require improved instrumentation to allow operators to detect its occurrence before it causes system inoperability.	The service water temperature is monitored and alarmed in MCR at low temperature setpoint.
5	GI-2	Failure of protective devices on essential equipment	A large number of licensee event reports have noted the incapacitation of safety-related equipment because of the failure of protective devices such as fuses and circuit breakers. Operators are not always aware of the failure of the equipment because of the design of the instrumentation.	To minimize the effects of failures of safety-related equipment, the following measures are applied: - I&C systems including non-safety system are extensively distributed and digitalized. These digital I&C systems have a self-diagnosis function for their failures. - Redundant safety equipment power is supplied by independent power source. In addition, their failure is monitored and alarmed in the MCR.
6	GI-23	Reactor coolant pump seal failures	This is a multifaceted issue, which includes a number of proposed resolutions. One sub issue is the provision of adequate seal instrumentation to allow the operators to take corrective actions to prevent catastrophic failure of seals (see Subsection 7.3.1 for more detail).	RCP seal flow and boundary on each RCP seal are monitored and alarmed at abnormal status in MCR. RCP seal leak and rupture event is analyzed and the procedures are prepared.

Table 18.2-1 Examples of Issues and Resolutions from US-APWR OER Report (Sheet 3 of 3)

No.	Item	Issue/Scope	Human Factor Aspect Issue	Human Factor Issue addressed by US-APWR
7	GI-51	Improving the reliability of open cycle service water (SW) systems	The buildup of clams, mussels, and corrosion products can cause the degradation of open cycle SW systems. Added instrumentation is one means of providing operators with the capability to monitor this buildup and take corrective action before loss of system functionality occurs.	SW system has instrumentation that detects its flow degradation. The low flow alarm informs operators of service water system degradation and operators can take corrective actions.

18.3 Functional Requirements Analysis and Function Allocation

18.3.1 Objectives and Scope

The objective of the functional requirements analysis and function allocation (FRA/FA) is to ensure success paths which are used to control the safety critical functions and power production critical functions of the US-APWR are assigned properly as HAs or to automated systems. The safety and power production functional requirements are defined in such a way that the functional allocations take advantage of human strengths and avoid allocating functions that would be negatively influenced by human limitations. Safety is the primary consideration of the FRA/FA. To ensure safety can always be maintained, the analysis also considers power production functions. The FRA/FA ensures humans are not overloaded while trying to maintain power production, and thereby have the capacity to concurrently maintain overall plant situational awareness and control of all plant safety functions. The function allocations from the FRA/FA are compared to the automation and manual controls defined in the US-APWR system designs that are based largely on Japanese and US predecessor PWRs. Where discrepancies exist, the FRA/FA identifies HEDs. The HED database is used to track the evaluation and resolution of all HEDs.

18.3.1.1 Functional Requirements Analysis

The scope of the functional requirements analysis includes the identification of functions that must be performed to satisfy plant safety and power production objectives; that is, to maintain safe power production and to prevent or mitigate the consequences of postulated accidents that could damage the plant or cause undue risk to the health and safety of the public. Both objectives require maintaining critical safety functions under all plant conditions. A functional requirements analysis is conducted to:

- Determine the objectives, performance requirements, and constraints of the design
- Define the high-level critical power production and critical safety functions that have to be maintained to meet the design's objectives and desired performance
- Define the relationships between the critical functions and the success paths needed to maintain those functions or restore them to normal during plant upsets. Success paths are comprised of sub-functions, systems, key components and actions needed to control the critical functions. Each success path, including the action, is allocated to human or machine during FA.
- Provide a framework for understanding the role of controllers (whether personnel or system elements) for controlling the plant

18.3.1.2 Function Allocation

The scope of the function allocation activity includes the analysis of the requirements for plant control and the assignment of control functions for the following:

- Personnel (e.g., manual control)

- System elements (e.g., automatic control or passive, self-controlling phenomena)
- Combinations of personnel and system elements (e.g., shared control). It is noted that for the FRA/FA automatic systems are assumed to require human monitoring and occasional manual adjustment. Specific manual actions associated with automation failure are considered in task analysis, not FRA/FA.

Plant safety and reliability are enhanced by exploiting the strengths of personnel and system elements, including improvements that can be achieved through the assignment of control to these elements with overlapping and redundant responsibilities. In addition to technological and economic considerations, function allocation should be based on HFE principles using a structured and well-documented methodology that seeks to provide personnel with logical, coherent, and meaningful tasks. Function allocation should not be based solely on technology considerations that allocate to plant personnel everything the designers cannot automate, because such an approach results in an ad hoc set of activities that may negatively affect operator performance.

The FA includes evaluation of human or machine assignments for credited actions identified in the plant accident analysis. This encompasses alignment actions that may be necessary during emergency core cooling. The FA compares the HFE allocation to the assignments assumed in the accident analysis (e.g. Section 6.3 Emergency Core Cooling Systems, Subsection 6.3.2.8 “Manual Actions”). HEDs are generated for discrepancies.

18.3.2 Methodology

The detailed methodology for conducting the functional requirements analysis and function allocation and integrating it into the HFE analyses is documented in this section.

The FRA/FA is conducted by US licensed operators who are considered subject matter experts (SME). The FRA/FA process includes oversight and approval from HFE and HSI design experts, and from plant system design experts.

Functional requirements analysis and function allocation are performed using a structured, documented methodology reflecting HFE principles, as described in Reference 18.3-1, Section 3, 18.3-5, and 18.3-6 which provide general guidance on conducting the functional design of a nuclear power plant control room. Detailed guidance on the analytical methodology used, is provided in Reference 18.3-1, Appendix A.3. The function allocation methodology also reflects the additional guidance from Reference 18.3-2, which supplements the guidance in Reference 18.3-1. Reference 18.3-4, Part 2, Subsection 1.4.3, provides the criteria that Mitsubishi Heavy Industries, Ltd. (MHI) employed in determining function allocation for the US-APWR.

The functional requirements hierarchical decomposition for the US-APWR is determined for full power, low power and shutdown, and for normal and abnormal plant conditions. . The hierarchy shows the functions essential to plant safety and power production, and the success paths that are used to control those functions. Success paths are identified based on SME experience and US-APWR system design documentation. SME experience has been incorporated into the US-APWR function allocation.

The functional requirements analysis and function allocation consider the following:

- The degree to which the success paths of the new design differ from those plants which establish the SME experience base

- The extent to which difficulties related to plant functions or success paths identified by the SMEs are addressed in the new design

The functional requirements analysis and function allocation are kept current over the life cycle of design development and are maintained until decommissioning, so that they can be used as design base when modifications are considered. Control functions are re-allocated in an iterative manner, in response to developing design specifics, operating experience, and the outcomes of ongoing analyses and trade studies, if required.

The OER (Section 18.2) is used to identify problems with historical function allocations. If problematic allocation issues are identified through the OER, then the FRA/FA:

- Justifies maintaining the historical human-machine allocation and identifies solutions such as improved HSI design (eg. alarms), training, personnel selection, and/or procedure design to address the OER issues.

- Changes the human-machine allocation.

- Identifies solutions such as training, personnel selection, and procedure design that is to be implemented to address the OER issues

The function allocation analysis considers not only the concurrent workload associated with all critical safety and power production functions for the primary allocations to personnel, but also personnel responsibilities to monitor automatic functions and make routine periodic manual adjustments to automatic control functions (eg. control setpoint changes). This workload evaluation, which considers concurrent power production and safety functions, ensures the allocation supports the highest level safety goal during all plant conditions.

The FRA/FA does not consider the additional workload needed to backup automation failure, because these very infrequent and burdensome actions would incorrectly skew the allocation decisions for most success paths to automation, leaving the operator role to serve only as an automation backup. This is a conservative approach because in the digital control systems all automation is fully redundant, therefore a complete automation function failure is unlikely. For the FRA/FA it is assumed that automation failure conditions are addressed by Emergency Operating Procedures and Abnormal Operating Procedures and operators will stop other less important tasks to execute these procedures. The specific tasks needed to backup automation failure are addressed in the TA.

The functional requirements analysis and function allocation verifies the following:

- All high-level functions necessary for the achievement of safe operation are identified.

- All requirements of each high-level function are identified.

- The allocations of functions result in a coherent role for plant personnel.

The FRA/FA is kept current with design changes and the HFE issues tracking program, as described in Subsection 18.10.2.4 and Section 18.11.

18.3.3 Results

The results report of the functional requirements analysis and function allocation is documented in Reference 18.3-4 (Part 2, Section 1).

Each critical safety function and critical power product function is identified. The safety functions include functions needed to prevent or mitigate the consequences of postulated accidents that could cause undue risk to the health and safety of the public. For each safety and power production function, the set of plant system configurations or success paths that are used to control the function are clearly defined. Function decomposition starts at “top-level” functions where a very general picture of major functions is described, and continues to lower levels until a specific critical end-item requirement emerges (e.g., a piece of equipment, software, or HA). The functional decomposition addresses the following levels:

- Plant goals (i.e. Safety and Power Production).
- Critical functions that must be maintained to achieve each goal (e.g., Reactor Coolant System integrity).
- Success paths used to control (i.e., maintain or restore) each critical function. Success paths include subfunctions, systems, key components and actions.

A description is provided for each critical function and includes:

- Critical function purpose.
- Conditions indicating the critical function is deviating from normal, and therefore that a success path deployment or adjustment is needed.
- Parameters indicating the success path is available.
- Parameters indicating the success path is operating (e.g., flow indication).
- Parameters indicating the success path is achieving its purpose (e.g., the critical function is returning to normal).
- Parameters indicating operation or adjustment of the success path can or should be terminated.

Parameters may be described qualitatively (e.g., high or low) since specific data values setpoints are not necessary at this stage.

The major FA changes for the critical safety functions of the US-APWR as compared to a conventional four loop US and Japanese PWR plants are:

- Automatic isolation of a faulted SG resulting from a main steam line break or feedwater line break

  - The purpose of the FA changes is to reduce plant operator workload and potential human error when responding to a faulted SG. Emergency feedwater isolation valves should be closed for the faulted SG in case the SG main steam line pressure reaches the low setpoint. The SG levels and pressures are significant parameters for monitoring the SG conditions.

- Automatic establishment of recirculation for ECCS

  - The purpose of the FA changes is to allocate establishment of long-term core cooling after the LOCA from manual to automatic action. In the design of a present day PWR plant, a containment recirculation sump water level is an essential parameter in changing recirculation mode. The US-APWR refueling water storage pit inside containment enables ECCS recirculation to be established automatically.

The technical basis for each function allocation is documented, including the allocation criteria, rationale, and analyses method. The technical basis for functional allocation can be any one or a combination of evaluation factors (Reference 18.3-4, Section 1.4.2). For example, the performance demands to successfully control the success path, such as the control complexity, time available to take the action compared to the time required for a human to take the action manually, or the frequency of a recurring response, may be such that it would be difficult or error prone for personnel to accomplish. HFE evaluation factors such as these establish the basis for the FA result. HEDs are identified where the FA result does not match the US-APWR system design. Technical feasibility, regulator design constraints and cost factors for automation will also be considered in the final HED resolution.

18.3.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.3(1) Deleted

COL 18.3(2) Deleted

18.3.5 References

18.3-1 Design for Control Rooms of Nuclear Power Plants, IEC 964, International Electrotechnical Commission, 1989.

18.3-2 Pulliam et al., A Methodology for Allocation of Nuclear Power Plant Control Functions to Human and Automated Control, NUREG/CR-3331, June 1983.

18.3-3 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 5, November 2011.

18.3-4 HSI Design, MUAP-09019-P (Proprietary) and MUAP-09019-NP (Non-Proprietary), Revision 2, September 2012.

18.3-5 Nuclear power plants – Control Rooms – Design, IEC 60964 ed2.0, International Electrotechnical Commission, February 2009.

18.3-6 Nuclear power plants – Design of control rooms – Functional analysis and assignment, IEC 61839 ed1.0, International Electrotechnical Commission, July 2000.

18.4 Task Analysis

18.4.1 Objectives and Scope

The objective of the task analysis is to identify the specific tasks that are needed for function accomplishment and the associated information, control, and task-support requirements.

Scope of the task analysis includes:

- Selected representative and important tasks from the following areas:
  - Operations
  - Maintenance (analysis is limited to equipment restoration to operability after maintenance)
  - Test
  - Inspection
  - Surveillance
- Full range of plant operating modes, including:
  - Startup
  - Normal operations
  - Abnormal and emergency operations
  - Transient conditions
  - Low-power and shutdown conditions
- HAs that have been found to affect plant risk by means of probabilistic risk assessment (PRA). Internal and external initiating events and actions affecting the PRA Level I and II analyses are considered when identifying risk-important actions.
- Where the control of critical functions are automated, the analyses consider all human tasks, including monitoring of the automated system and execution of backup actions if the automation fails.
- The task analysis identifies information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls.

The task analysis also addresses issues such as the following:

- The US-APWR design constraint of minimum operator staffing (i.e., one RO and one SRO in the MCR)
- Operating personnel skill requirements
  - Job formation and training
  - Physical workload
  - Cognitive workload
  - Other workload tasks that may need to be executed concurrently with the specific task being analyzed.

The scope of the task analysis encompasses the MCR, RSC, TSC and LCSs that fall into the categories identified in Section 18.1.1.2.

Task analysis for the EOF that is within the scope of the US-APWR HFE program is limited to (1) the information needed on displays at the EOF and (2) the EOF communication requirements with the MCR. Task analysis to address the complete EOF will be conducted in accordance with the site-specific HFE program for compliance with NUREG-0696.

Task analysis for the CAS and SAS that is within the scope of the US-APWR HFE program is limited to the information that shall be communicated between the CAS/SAS and the operators in MCR.

18.4.2 Methodology

The detailed methodology for conducting the task analysis and integrating it into the HFE analyses is documented in this section and in Part 2, Section 3 of Reference 18.4-4. This methodology is applicable to (1) the TA for Risk Important Human Actions, whose results report is documented in Part 2 Section 3 of Reference 18.4-4, and (2) the TA for other actions, whose implementation plan is documented in Part 2, Section 3 of Reference 18.4-4.

Task analyses begin at a high level and involves the development of detailed narrative and tabular descriptions of what personnel have to accomplish. The analyses define the nature of the input, process, and output needed by and from personnel.

Detailed narrative and tabular task descriptions address (as appropriate) the following topics:

- Information requirements
- Decisions making requirements
- Response requirements
- Communication requirements

- Workload
- Task support requirements
- Workplace factors
- Situational and performance shaping factors (PSFs)
- Hazard identification

The task analysis is conducted for plant systems that are in various stages of design. For some plant systems, the TA may be based on preliminary system design information. For these cases, the TA will be verified when the system design information matures. In all cases, the TA is detailed enough to identify information and control requirements to enable specification of detailed requirements for alarms, displays, data processing, and controls for human task accomplishment. The task analysis addresses the following issues:

- The number of crew members, with consideration of minimum staffing design constraints
- Crew member skills
- Allocation of monitoring and control tasks for the following purposes:
    - Definition of a meaningful job scope
    - Management of crew member's physical workload
    - Management of crew member's cognitive workload

The TA will analyze the Success Path Actions identified by FRA on the basis of their allocation from FA. If the allocation is to machine, the TA is limited to the tasks needed to supervise the automation. If the allocation is to man, the TA decomposes the Action to tasks that encompass all required manual control actions. The TA will also perform a separate analysis for manual actions to accommodate automation failure.

18.4.2.1 Description of the Methods Used to Analyze Tasks

The general task analysis methodology is described in Part 2, Section 3 of Reference 18.4-4. The operational sequence diagram (OSD) method is used to conduct functional-based task analysis. The goals, operators, methods, and selection (GOMS) method (Reference 18.4-2) is used to conduct cognitive skills task analysis.

18.4.2.2 General Task Analysis Methods

The OSD method is applied for analysis of US-APWR operations. OSD is used as it is applicable from the initial facility design phase to the final design phase. An OSD represents operator and computer tasks in graphical scheme sequentially and indicates actions, data transmitted or received, inspections, operations, decisions, and data storage. The information flow is shown in relation to both time and space. This method is used to develop and present the system reaction to specific inputs and display the interrelationship between operators and equipment. Detailed task analysis tools (e.g., task description method or functional flow diagram, Reference 18.4-3) are employed to supplement OSD, as needed.

HEDs may be identified during TA. The following are examples of where HEDs may be identified:

- Manual allocations from FA that are determined from TA to require staffing that exceeds the minimum staffing design constraint.

- Information or control requirements defined by TA, but are not included in the system designs.

18.4.2.3 Detailed Cognitive Task Analysis Methods

In order to evaluate a crewmember's cognitive workload, an interaction analysis between human and computer systems is necessary. GOMS is a method for the analysis of the cognitive skills involved in human-computer tasks. GOMS is based upon an information-processing framework that assumes a number of different stages or types of memory and separate perpetual, motor, and cognitive processing times. Selected scenarios are analyzed using this method and detailed quantitative metrics are obtained. This information is then used to develop the HSI design.

18.4.3 Results

The task analysis results report for Risk Important Human Actions and the task analysis implementation plan for remaining tasks are documented in the Technical Report (Reference 18.4-4). The task analysis results provide input to the design of HSIs, procedures, and personnel training programs.

18.4.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.4(1) Deleted

COL 18.4(2) Deleted

COL 18.4(3) Deleted

18.4.5 References

18.4-1 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 5, November 2011.

18.4-2 Card, S., Moran, T.P., and Newell, A, The Psychology of Human-Computer Interaction, Part II, Lawrence Erlbaum Associates, Hillsdale, NJ, 1983.

18.4-3 Burgy, D, Lempges, C., Miller, A., Schroeder, Van Cott, L.H., Paramore, B., Task Analysis of Nuclear Power Plant Control Room Crews, NUREG/CR-3371, Volumes 1 and 2, September 1983.

18.4-4 HSI Design, MUAP-09019-P (Proprietary) and MUAP-09019-NP (Non−Proprietary), Revision 2, September 2012.

18.5 Staffing and Qualifications

18.5.1 Objectives and Scope

The objective of the staffing and qualifications analysis (SA) is to determine the number and qualifications of personnel required for safe and efficient plant operation in a systematic manner that includes a thorough understanding of task requirements and applicable regulatory requirements. The detailed staffing and qualification analysis process is described in Reference 18.5-12, the US-APWR Staffing & Qualifications Implementation Plan (MUAP-10008).

18.5.2 Methodology

The staffing analysis determines the number and background of personnel for the full range of plant conditions and tasks including all modes of operation (normal, abnormal, and emergency), plant maintenance, plant surveillance and testing.

The plant personnel who are addressed by the HFE program include licensed control room operators (ROs and SRO) as defined in 10 CFR 55 (Reference 18.5-4), and the following categories of personnel defined in 10 CFR 50.120 (Reference 18.5-5):

- Non-licensed operators (Note 1)
- Shift managers
- Shift technical advisor
- I&C technicians (Note 1)
- Electrical maintenance personnel (Note 1)
- Mechanical maintenance personnel (Note 1)
- Radiological protection technicians (Note 1)
- Chemistry technicians (Note 1)
- Engineering support personnel (Note 1)

Note 1: Tasks directly related to plant safety are addressed in this analysis for the full range of plant operating modes, including the following:

- Startup / Shutdown
- Normal operations
- Abnormal and Emergency operations
- Transient conditions

The scope of tasks covered by the analysis includes operational tasks, plant maintenance tasks and plant surveillance and testing.

In addition, any other plant personnel that perform tasks directly related to plant safety are addressed in the staffing analysis.

The minimum and maximum MCR staffing are design constraints of the US-APWR, as defined in Section 18.1.1.1. The maximum staffing establishes the basis of the MCR physical design. The minimum staffing establishes an input to all HFE program elements, including TA. Minimum staffing is ultimately confirmed through V&V. HEDs are generated if a program element identifies any challenges to the minimum staffing design constraint.

The initial US-APWR staffing levels and qualifications for non-operating staff are based on predecessor PWR plants. The staffing analysis begins by identifying changes to the US-APWR from predecessor plants (i.e., similar PWR plants) in system designs, technologies or operating practice assumptions. Analyses are then conducted to identify where US-APWR plant changes can lead to, or require, changes in staffing numbers or personnel qualifications. The analysis will be conducted by a multidisciplinary team that includes expertise in:

- US-APWR plant design, including reactor system design, turbine system design, and HSI and I&C design
- Plant operations in a typical U.S. PWR plant across all modes of operation including, outage, startup, low power and normal operation
- Plant maintenance and plant surveillance and testing practice in a typical U.S. PWR plant
- PWR Operator training
- Human Factors

The team makeup will vary depending on the tasks being analyzed.

The staffing analysis is iterative where initial staffing levels are reviewed and modified as the analyses associated with other elements are completed.

The staffing and qualifications analysis addresses the following issues associated with each HFE program element:

- OER
  - Operational problems and strengths that result from staffing levels in predecessor systems
  - Initial staffing goals and their bases, including staffing levels of predecessor systems and a description of significant similarities and differences between predecessor and current systems
  - Staffing considerations described in NRC Information Notice 95-48, “Results of Shift Staffing Study” (Reference 18.5-7)

  - Staffing considerations described in NRC Information Notice 97-78, “Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times” (Reference 18.5-8)

- Functional requirements analysis and function allocation

  - Mismatches between functions allocated to personnel and their qualifications

  - Changes to the roles of personnel due to plant system and HFE modifications

- Task analysis

  - Knowledge, skills, and abilities needed for personnel tasks addressed by the task analysis

  - Personnel response time and workload

  - Personnel communication and coordination, including interactions between them for diagnosis, planning, and control activities, and interactions between personnel for administrative, communications, and reporting activities

  - Job requirements that result from the sum of all tasks allocated to each individual, both inside and outside of the control room

  - Decreases in the ability of personnel to coordinate their work due to plant and HFE modifications

  - Availability of personnel considering other activities that may be ongoing and for which operators may take on responsibilities outside the control room (e.g., fire brigade)

  - Actions identified in 10 CFR 50.47 (Reference 18.5-9), NUREG-0654 (Reference 18.5-10), and the procedures to meet an initial accident response in key functional areas, as identified in the emergency plan

  - Staffing considerations described by the application of American National Standards Institute (ANSI)/American Nuclear Society (ANS) 58.8-1994, ”Time Response Design Criteria for Safety-Related Operator Actions“ (Reference 18.5-11)

- HRA

  - Effect of overall staffing levels on plant safety and reliability

  - Effect of overall staffing levels and crew coordination for risk-important HAs

  - Effect of overall staffing levels and the coordination of personnel on human errors associated with the use of advanced technology

- HSI Design

- Staffing demands resulting from the locations and use (especially concurrent use) of controls and displays
- Coordinated actions between individuals
- Decreases in the availability or accessibility of information needed by personnel due to plant system and HFE modifications
- Physical configuration of the control room and control consoles
- Availability of plant information from individual workstations and group-view interfaces

• Procedure Development

- Staffing demands resulting from requirements for concurrent use of multiple procedures
- Personnel skills, knowledge, abilities, and authority identified in procedures

• Training Program Development

- Crew coordination concerns that are identified during the development of training

18.5.3 Results

The staffing and qualifications analysis methodology is documented in the Staffing and Qualifications Implementation Plan, Reference 18.5-12. The staffing and qualification analysis is developed and documented in the staffing and qualifications analysis results summary report. The staffing and personnel qualifications required for the US-APWR are demonstrated by the V&V process to be adequate for operating plant personnel. Those staffing and qualification program issues that negatively impact human performance are identified as HEDs and are tracked and dispositioned. For MCR operator staffing, the SA results summary report summarizes the staffing-related HEDs generated in other HFE program elements and their resolution.

The result of staffing and qualifications analysis is used as input to other HFE elements including Human-System Interface Design, Procedure Development and Training program development.

18.5.4 Combined License Information

No additional information is required to be provided by a COL Applicant In connection with this section.

COL 18.5(1) Deleted

COL 18.5(2) Deleted

18.5.5 References

18.5-1 Conditions of Licenses, NRC Regulations Title 10, Code of Federal Regulations, Part 50.54.

18.5-2 U.S. Nuclear Regulatory Commission, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, NUREG-0800, Subsections 13.1.2 – 13.1.3 “Operating Organization”, March 2007.

18.5-3 U.S. Nuclear Regulatory Commission, Human Factors Engineering Program Review Model, NUREG-0711, Revision 2, February 2004.

18.5-4 Operators’ Licenses, NRC Regulations Title 10, Code of Federal Regulations, Part 55.

18.5-5 Training and Qualification of Nuclear Power Plant Personnel, NRC Regulations Title 10, Code of Federal Regulations, Part 50.120.

18.5-6 Selection, Qualification, and Training of Personnel for Nuclear Power Plants, ANSI/ANS 3.1, 1993.

18.5-7 Results of Shift Staffing Study, Information Notice 95-48, 1995.

18.5-8 Crediting of Operator Actions in Place of Automatic Actions and Modifications of Operator Actions, Including Response Times, Information Notice 97-78, 1997.

18.5-9 Emergency Plans, NRC Regulations Title 10, Code of Federal Regulations, Part 50.47.

18.5-10 U.S. Nuclear Regulatory Commission, Criteria for Preparation and Evaluation of Radiological Emergency Response Plans and Preparedness in Support of Nuclear Power Plants, NUREG-0654, October 1980.

18.5-11 Time Response Design Criteria for Safety-Related Operator Actions, ANSI/ANS 58.8, 1994.

18.5-12 US-APWR Staffing & Qualifications Implementation Plan (MUAP-10008), Revision 2, September 2012.

18.6 Human Reliability Analysis

18.6.1 Objectives and Scope

The objective of the human reliability analysis program element (HRA) is to (1) ensure that the assumptions of the HRA/PRA, as documented in DCD Chapter 19 regarding risk important human actions, are consistent with the US-APWR HSI and are consistent with expected human performance, and (2) document the HRA/PRA results that must be thoroughly incorporated into the HFE analysis and HSI design. The HFE analysis and HSI design process interacts iteratively with the HRA/PRA. The proper interaction of HFE design and HRA/PRA most effectively contributes to minimizing personnel errors, allowing human error detection, and providing human error recovery capability.

During the HRA, the HSI design and human performance assumptions of the HRA/PRA are confirmed based on the known characteristics of the HSI design, including design basis constraints, as defined in Section 18.1.1.1, and the resulting human performance expectations. The HSI design and human performance assumptions of the HRA/PRA are confirmed in more detail as the detailed HFE analysis and HSI design progresses as part of the task analysis, HSI design, procedure and training development, and the V&V program elements. The assumptions of the HRA/PRA are considered inputs to these program elements. HEDs are generated if any challenges to the HRA/PRA assumptions are identified.

The scope of the HRA/PRA incorporation into the HFE effort encompasses risk-important HAs as described in Reference 18.1-12, Part 2 Section 2. The iterative nature of the interaction of HFE design and the HRA/PRA continues as the design progresses. The primary influence of the HRA/PRA on the HFE process manifests itself in the task analysis where accurate estimates of workload and task completion times for risk-important human actions (RIHA) are developed. These TA results confirm the HRA/PRA assumptions at a more detailed level than initially performed during the HRA. The TA results for risk-important human actions (RIHAs) are described in Section 18.4.

18.6.2 Methodology

The methodology for conducting the HRA program element (ie. integrating the HRA/PRA into the HFE analyses) is described below.

Incorporating HRA/PRA results into the HSI design process involves identifying risk-important HAs, addressing the HAs in the HFE analysis and design process, and validating the HSI design supports the human performance assumptions of the HRA/PRA. The guidelines for incorporating the HRA/PRA into the HFE analysis, as contained in Reference 18.6-1, are used to achieve the integration. The following specific activities are conducted during the HRA:

- Risk-important HAs are identified from the PRA/HRA. These actions are extracted from the Level 1 (core damage) PRA and Level 2 (release from containment) PRA, including both internal and external events. RIHAs are developed using several important measures and HRA sensitivity analyses to provide reasonable assurance that an important action is not overlooked because of the selection of the measure or the use of a particular assumption in the analysis. The HRA methodology is described in Subsection 19.1.4.1.1, “Description of the Level 1 Probabilistic Risk Assessment for Operations at Power” and Subsection 19.1.6.1, “Description of Low-Power and Shutdown Operations.” The categorization of the RIHAs is described in Subsections 19.1.4.1.1 and 19.1.6.1.

- The HFE design team characterizes risk-important human-system interactions by the performance shaping factors (PSF) described in Reference 18.6-2, Subsection 4.5.2, as specifically stated in or inferred from the HRA/PRA.
- HRA assumptions such as decision-making and diagnosis strategies for dominant sequences are confirmed by personnel with US nuclear plant operational experience using table top walk-throughs.

18.6.3 Results

The HRA results summary report (Reference 18.6-3 Part 2, Section 2) documents the following:

- Risk-important HAs
- Consistency between the HSI design and the PRA/HRA assumptions

All RIHAs that have been identified in the PRA, have been evaluated in the "Human Reliability Analysis" HFE program element. The results of that program element are documented in Part 2 Section 2 of Reference 18.1-12. This document reflects the RIHAs identified in the US-APWR Probabilistic Risk Assessment (Reference 18.1-20). As part of the US-APWR philosophy, all RIHAs that were identified and that have been typically located outside the MCR for previous generation plants, were moved into the MCR for the US-APWR. Therefore the RIHA list contained in the attachment to Reference 18.1-12 Part 2 Section 2 only contains HAs within the MCR.

However, the HFE process, as described in Reference 18,1-12 Part 1, is iterative, If additional RIHAs are identified in the future, these will be similarly evaluated, with preference, as practical based on the design status, given to location within the MCR.

All RIHAs at LCS, if they are identified in the future, and all HAs located at LCS that fall into the categories identified in Section 18.1.1.2 (risk-important or not), will be evaluated and designed in accordance with the remaining HFE Implementation Plans (Reference 18.1-14, 18.1-15, 18.1-16 and 18.1-17).

RIHAs and their associated tasks and scenarios, as identified in the HRA, are specifically addressed during task analyses, HSI design, procedure development, and training development. Proper consideration of RIHAs helps verify that these tasks are well supported by the design and within acceptable human performance capabilities (e.g. within time and workload requirements). The HFE team applies HFE guidelines to the HSI design to optimize the PSFs, thereby enhancing the overall human success probability. Final reviews of the HSI design and integrated system validation, conducted during HFE V&V process, confirm the HSI design supports the human performance assumptions of the HRA/PRA for all RIHAs.

18.6.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.6(1) Deleted

COL 18.6(2) Deleted

18.6.5 References

18.6-1 U.S. Nuclear Regulatory Commission, Guidance for the Review of Changes to Human Actions, NUREG-1764, December 2002.

18.6-2 IEEE Guide for Incorporating Human Action Reliability Analysis for Nuclear Power Generating Stations, IEEE Std 1082-1997, Institute of Electrical and Electronics Engineers, NY, September 1997.

18.6-3 HSI Design, MUAP-09019-P (Proprietary) and MUAP-09019-NP (Non−Proprietary), Revision 2, September 2012.

18.6-4 Swain, A.D. and Guttmann H.E., Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications, NUREG/CR-1278, August 1983.

18.7 Human-System Interface Design

18.7.1 Objectives and Scope

The objective of the Human-System Interface Design program element is to document the design process with the resulting US-Basic HSI design, and the plan for translating the US-APWR HFE analysis outputs into the US-APWR inventory of alarms, displays and controls, through the systematic application of HFE principles and criteria. A key output of the HSI Design program element is a complete US-APWR HSIS that will be implemented in a full scope simulator for subsequent verification and validation. The simulator includes the functions of the MCR, RSR and TSC.

This program element will also generate complete HSI designs for safety-significant local controls, and detailed communications and information requirements for the EOF. The HSI Design program element will also generate the design of the HSI that will be used by the operators in the MCR to communicate with the EOF and with the CAS/SAS.

18.7.2 Methodology

Reference 18.7-1 provides a detailed description of the design of the US-Basic HSIS control room, control consoles, and user interfaces, and the methodology used to develop this design. The Japanese and international standards, Japanese nuclear power plant operating experience, and NRC-directed operating considerations are applied to the US-Basic HSIS design discussed in Reference 18.7-1, Appendices A and B and supporting references. The Japanese Basic HSIS design underwent a V&V process conducted in accordance with Japanese requirements. This control room and HSI configuration are the basis for the US-Basic HSIS design that is the foundation of the US-APWR HSIS design. However, the US-APWR HSIS is to comply with all NRC regulations as stated in the Abstract of Reference 18.7-1, by full implementation of the analyses described in Sections 18.2, 18.3, 18.4, 18.5, and 18.6 above. The verification of the US-Basic HSIS is evaluated with respect to the guidelines in Reference 18.7-2 described in this Section; and a full V&V of the fully integrated US-APWR HSIS is conducted, as described in Section 18.10. HEDs identified during any program element are resolved prior to completion of the HFE program.

18.7.2.1 HSI Design Inputs

The Japanese Basic HSIS design is the initial design input for the US-Basic HSIS design, which is the foundation of the US-APWR HSIS design, discussed above. The following sources of the US-APWR information, described in Sections 18.2 through 18.6, provide input to the US-APWR HSI design process:

- Analysis of Personnel Task Requirements – The analyses performed in earlier stages of the design process are used to identify requirements for the HSIs. These analyses include the following:
    - Operating experience review – Lessons learned from other complex human-machine systems, especially predecessor designs and designs involving similar HSI technology are used as an input to HSI design. The OER is described in Section 18.2.

- Functional requirement analysis and function allocation – The HSIs support the operator’s role in the plant (e.g., appropriate levels of automation and manual control). The FRA and FA are described in Section 18.3.

- Task analysis – The set of requirements to support the role of personnel is provided by task analysis. The task analysis is described in Section 18.4. The task analysis identifies the following:

  - Tasks that are necessary to control the plant in a range of operating conditions for normal through accident conditions

  - Detailed information and control requirements (e.g., requirements for display range, precision, accuracy, and units of measurement)

  - Task support requirements (e.g., special lighting and ventilation requirements)

- Human reliability analysis – Risk-important HAs and their associated power shaping factors, as identified through HRA, are given special attention in the HSI design process. The HRA integration into the HSI design process is described in Section 18.6.

- Staffing and qualificationsanalysis – The results of staffing and qualifications analyses provide input for the layout of the overall control room and the allocation of controls and displays to individual consoles, panels, and workstations. This establishes the basis for the minimum and maximum number of personnel to be accommodated and requirements for coordinating activities between personnel. The staffing/qualifications and job analyses are described in Section 18.5.

• US-APWR design constraints – As defined in Section 18.1.1.1 the US-Basic HSIS is the starting point for the US-APWR HSIS. In addition, the US-APWR HSIS must accommodate the minimum and maximum MCR staffing. Challenges to these design constraints result in HEDs.

• System Requirements – Constraints imposed by the overall I&C system, such as redundancy, equipment qualification, and coping with common mode failures are significant inputs for the HSI design and are considered throughout the HSI design process

• Regulatory and Other Requirements – Applicable regulatory requirements and industry standards, including those identified in Reference 18.7-1 Section 3.0 “Applicable Codes, Standards, and Regulatory Guidance,” are inputs to the HSI design process.

18.7.2.2 Concept of Operations

The concept of operations for the US-APWR is as described in Reference 18.7-1, Section 4.1, and includes:

- Crew composition (see Reference18.7-1 Subsection 4.1.f) - As defined in Section 18.1.1.1, for the US-APWR the minimum crew composition is supplemented with one more SRO or STA qualified person present at the facility during operation. During emergency conditions, this person can relieve the MCR Supervisor of either the supervisor or STA responsibilities. This person can be shared by multiple units.

- Roles and responsibilities of individual crewmembers (see Reference 18.7-1, Subsection 4.1.g) - This information will be supplemented by the results of the Staffing and Qualifications analysis, see Section 18.5.

- Personnel interaction with plant automation (see Reference 18.7-1, Subsections 4.1.a, 4.1.b, 4.1.e, 4.1.h) - Operators can enable or disable automatic control functions, and override automatic interlock functions, as defined in Reference 18.7-6, Section 4.2.

- Use of control room resources by crewmembers (see Reference 18.7-1, Sections 4.1.c and 4.1.d)

- Methods used to ensure good coordination of crewmember activities, including non-licensed operators, technicians, and maintenance personnel. These coordination tools/methods include:

  - Large display panel (LDP) (see Reference 18.7-1, Section 4.9)

  - Local Control Stations (LCS) (see Reference 18.7-1, Subsection 4.2.5)

  - Tagging (see Reference 18.7-1, Section 4.5)

In addition, distribution of plant data via the unit bus and the plant station bus is described in Section 7.9, with voice communications systems for the US-APWR described in Subsection 9.5.2.

18.7.2.3 Functional Requirements Specification

Reference 18.7-3 and 18.7-9 identify the key principles of functional requirements specification in Chapter 4, “Functional Design Specification,” with additional analytical detail provided in Appendix A, “Design Guide for Control Rooms,” Section A.4. These basic functional requirements for all HSI resources are reflected in the HSI design described in Reference 18.7-1. During the detailed design process additional functional requirements for HSIs are added reflecting the output from the task analysis, including alarm, information and control content for specific displays.

18.7.2.4 HSI Concept Design

The US-APWR HSI design is a direct evolution of the predecessor standard Japanese Basic HSIS design, as described in Reference 18.7-1 and shown in Reference 18.7-1, Appendix B, Figure B-2. The development of the standard Japanese Basic HSIS design from concept phase through final design is described in Reference 18.7-1, Appendix A. Figure 7.1-7 in Section 7.1 shows the conceptual MCR layout of the US-APWR. The final

US-APWR MCR layout, resulting from all phases of the HSI design process, will be described in the HSI Design results summary report.

- The primary changes from the Japanese Basic HSIS design and conventional US and Japanese PWRs that are reflected in the US-APWR HSIS design are described in Sections 18.2 and 18.3. These include:

  - Automating channel checks (i.e. automated cross checking of redundant sensor measurements)

  - Automatic isolation of a faulted SG (the function is to be implemented inside the Protection and Safety Monitoring System (PSMS))

  - Elimination of manual actions required to establish ECCS recirculation (this is a change from conventional US PWRs)

  - Arrangement of the main control room operator consoles to accommodate the control actions and monitoring by one or two reactor operators (the Japanese Basic HSIS design accommodates control by one operator)

  - Conversion from two-train to four-train design for safety systems

  - HSI modified to accommodate the US-APWR specific plant mechanical and electrical systems

  - Japanese-to-English language conversion

  - Metric-to-English units conversion

  - Ergonomics changes to accommodate the expected range of US operating personnel, in accordance with Reference 18.7-2

  - Console designs to accommodate modern HSI technology (e.g., flat panel displays versus cathode-ray tube displays)

  - Control devices to accommodate advances in technology (e.g., mouse, touch screens and other pointing devices)

- The functional requirement specification for the Japanese Basic HSIS design serves as the initial source of input to the US-Basic HSIS design effort. As a result, the US-APWR HSIS design, which is built upon the US-Basic HSIS design, is a direct evolution from the predecessor standard Japanese PWR. The following criteria in this section were considered during the development of the standard Japanese PWR and the HSI design.

  - Alternative approaches for addressing HSI functional requirements were considered. Evaluation methods included operating experience, literature analyses and engineering evaluations. A survey of the state-of-the-art in HSI technologies was conducted to:

        - Support the development of concept designs that incorporate advanced HSI technologies
        - Provide assurance that proposed designs are technically feasible
        - Support the identification of human performance concerns and tradeoffs associated with various HSI technologies

    - Alternative concept designs were evaluated so that one can be selected for further development. The evaluation provides reasonable assurance that the selection process is based on a thorough review of design characteristics and a systematic application of selection criteria. Tradeoff analyses, based on the selection criteria, provide a rational basis for the selection of concept designs.

    - HSI design performance requirements were identified for components of the selected HSI concept design. These requirements were based on the functional requirement specifications and were refined to reflect HSI technology considerations identified in the survey of the state of the art in HSI technologies and human performance considerations identified in human performance research and evaluations.

- Human performance issues identified from operating experience with the predecessor design are resolved.

18.7.2.5 HSI Detailed Design and Integration

The HSI detailed design and integration for the US-APWR HSIS is based on the Japanese Basic HSIS design. The standard Japanese Basic HSIS design employs a style guide that is used in establishing the generic display methods for all aspects of the design. The style guide was used as the starting point for the US-Basic HSIS style guide. The US-Basic HSIS style guide is described in the Topical Report (Reference 18.7-1), including the scope, contents, and procedures. The HFE guidelines utilized in the design of the HSI features, layout, and environment is provided in the style guide. The style guide design guidance was primarily developed in accordance with Reference 18.7-2; guidelines from other sources were incorporated and identified by reference. Key aspects of the style guide are as follows:

- The content of the style guide is derived from (1) the application of generic HFE guidance to the specific application, and (2) the development of situation-specific guidelines based upon design-related analyses and experience. Guidelines that are not derived from generic HFE guidelines may be justified based on an analysis of recent literature, analysis of current industry practices, operational experience, tradeoff studies and analyses, and the results of design engineering experiments and evaluations. The guidance is tailored to reflect design decisions made to address specific goals and needs of the HSI design.

- The topics in the style guide address the scope of HSIs included in the design and address the form, function, and operation of the HSIs as well as environmental characteristics relevant to human performance.

- The individual guidelines are expressed in concrete, easily observable terms. Generic HFE guidelines are used in their abstract form. Such generic guidance is translated into more specific design guidelines that can, as much as possible, provide unambiguous guidance to designers and evaluators. The design guidelines are detailed enough to permit their use by design personnel to achieve a consistent and verifiable design that meets the HFE guideline.

- The style guide is used in developing procedures for use in determining where and how HFE guidance is used in the overall HSI design process. The style guide is written in a manner so it can be readily understood by designers. The style guide supports the interpretation and comprehension of design guidance by supplementing text with graphical examples, figures, and tables.

- The guidance is maintained in a form that is readily accessible and usable by designers and facilitates modification when the contents require updating as the design matures. Each guideline included in the guidance documentation includes a reference to the source upon which it is based (as applied in Reference 18.7-2).

The standard Japanese Basic HSIS style guide was updated for the US-Basic HSIS style guide to address HSI modifications for the US-APWR described in the section above. The US-Basic HSIS style guide specifically addresses consistency in design across the HSIs.

The HSI detailed design and integration described in Reference 18.7-1 is applicable to the US-APWR. The HSI System Description and HFE Process describes (including the references that fully define the US-Basic HSIS):

- How the design supports personnel in their primary role of monitoring and controlling the plant, while minimizing the demands associated with interface management. The operational visual display units (VDUs) provide access to all information and controls, both Safety and Non safety. The LDP provides a continuous display to support situation awareness and crew interaction for all modes of operation.

- How the design addresses the safety parameter display system (SPDS) parameters referenced in 10 CFR 50.34(f)(2)(iv) (Reference 18.7-4). The LDP provides continuous display for the status of all critical safety functions and the plant systems used to control those safety functions. The electronic procedure system supports execution of the functional recovery EOPs.

- How the design minimizes the probability of error in the performance of risk-important HAs and provides the opportunity to detect errors, if they should occur:

    - Two actions, which means two touch operations, are required to activate any controls. The first action enables the soft control popup window. The second action activates the desired control. Since most control windows are normally not visible, additional touch operations are normally required to navigate to the appropriate video display and the appropriate control window.

- For the operational VDU, the soft control popup window is selected by touching an icon that represents the component to be controlled. The icon is presented in a graphical display that depicts the component within a system mimic diagram. Thereby, promoting correct component selection.

- The soft control pop-up face plate contains clearly labeled English descriptors, and tag numbers that uniquely distinguish safety and non-safety components, and identify safety division designations.

- Soft control pop-up windows show component status feedback in real time, allowing operators to immediately detect control errors. Operators can take immediate corrective actions (e.g., mid-travel valve reversal), without needing to wait for components to fully respond to the previously demanded control action.

- If an operator action erroneously disables a safety function or erroneously creates a condition that threatens a critical safety function, Bypassed or Inoperable Status Indication and Critical Safety Function alarms are provided on the LDP.

• The basis for allocation of HSI functions to either the main control room or LCS. All control functions are accessible in the main control room and no LCS controls are credited for normal operation or design basis accident condition operator response.

• The basis for the MCR layout, and the organization of HSIs within consoles, panels, and workstations – the MCR is designed to support the range of crew tasks and staffing (MCR layout is discussed in Reference 18.7-1 Subsection 4.3.1). Operational VDUs used during all normal and emergency modes of operation are centrally located.

• How the control room supports a range of anticipated staffing situations. The design accommodates minimum and maximum staffing, as described in Section 18.5. In addition, sufficient space is available to accommodate shift turnover.

• How the HSI characteristics mitigate excessive fatigue. Lighting, is described in Subsection 9.5.3, and ergonomics is described in Reference 18.7-1, Section 4.3, Layout Design.

• How the HSI characteristics support human performance under a full range of environmental conditions. Normal as well as credible extreme conditions, including emergency lighting is discussed in Subsection 9.5.3. Ventilation is discussed in Section 9.4, and control room habitability is discussed in Section 6.4.

• How the inspection, maintenance, tests, and repair of HSIs is accomplished without interfering with other control room tasks. Reference 18.7-1, Section 4.11 “Response to HSI Equipment Failures” describes how HSI equipment failures are responded to without impacting plant control functions.

- Reference 18.7-1, Section 4.8 provides a detailed description of the US-APWR CBP design, including user interfaces and the methodology used in developing the design. The US-APWR CBP design is based on the US-Basic HSIS design. NRC- directed operating considerations have been applied to the US-Basic HSIS design as discussed in Reference 18.7-1. US-APWR CBP design and procedures are demonstrated to comply with NRC regulations, as described in the HSI Design IP (Reference 18.7-6).

Overall HFE issues associated with the central alarm station (CAS) and the secondary alarm station (SAS) are discussed in Section 13.6, Security. The HSI Design and V&V program elements encompass the communications interface from the MCR to the CAS and SAS.

18.7.2.6 HSI Tests and Evaluations

The development of the Japanese Basic HSIS design described in Reference 18.7-1 Appendix A, includes trade-off evaluations and performance-based tests. This work was conducted in conjunction with Japanese nuclear utilities that provided nuclear plant operating staff to support the test efforts. The performance of the operating staff was evaluated and is described in Reference 18.7-1 Appendix B with the associated references. .

The US-Basic HSIS design was developed from the Japanese Basic HSIS design based on known differences needed to accommodate US operations, and based on additional testing that was conducted in Phases 1a and 1b of the US-APWR HFE program (see Section 18.1.5). These tests are described in Reference 18.7-8 Part 1 and Reference 18.7-5 Part 3. These reports describe the tests methods, results and HEDs identified during the process. HEDs will be resolved within the HSI Design program element described in Reference 18.7-7. HED resolution includes design changes and design testing, as deemed appropriate by the HSI Design Team and independent Expert Panel. The details of the HED resolution process are described in Section 18.1.4.

18.7.3 Results

The US-Basic HSIS design results and description are documented in the HSI/HFE Topical Report (Reference 18.7-1). The US-APWR HSIS design results and description combines the generic US-Basic HSIS design with the specific HSI inventory for the US-APWR, and will be documented in the "US-APWR HSIS Design Specification.” The US-APWR HSIS Design Specification will be referenced from the design implementation results summary report. The results summary report will demonstrate that all aspects of the US-APWR HSIS design have been developed and tested in accordance with Reference 18.7-6.

18.7.3.1 Overview of US-Basic HSIS Design and Key Features

The HSI/HFE Topical Report (Reference 18.7-1) describes the overall US-Basic HSIS design concept and its rationale. This description is applicable to the MCR, remote shutdown console (RSC), and TSC. Key features of the design, such as information display, “soft” controls, CBPs, alarm processing, and control room layout, are provided. The HSI Topical Report (Reference 18.7-1) includes:

- The detailed HSI description, including its form, function and performance characteristics
- The basis for the HSI requirements and design characteristics with respect to operating experience and literature analyses, tradeoff studies, engineering evaluations and experiments, and benchmark evaluations
- The basis of any design changes from the Japanese Basic HSIS design
- The outcomes of tests and evaluations performed in support of HSI design

18.7.3.2 Safety Aspects of the HSI

The HSI/HFE Topical Report (Reference 18.7-1) describes the US-Basic design implementation of the following safety aspects of the HSI, which are coordinated with the I&C design, are applicable to the US-APWR and will be documented in the "US-APWR HSI Design Specification":

- Safety function monitoring
- Periodic testing of protection system actuation functions
- Bypassed and inoperable status indication for plant safety systems
- Manual initiation of protective actions
- Instrumentation required to assess plant and environmental conditions during and following an accident
- Setpoints for safety-related instrumentation
- HSIs for the TSC

The information needed to be displayed at the EOF is identified through the US-APWR HFE program. However, the actual design of HSIs for the site-specific EOF is outside the scope of the US-APWR HFE program. These HSIs will be designed in accordance with the site-specific HFE program for complying with NUREG-0696.

In addition, the HSI/HFE Topical Report (Reference 18.7-1) describes the minimum Inventory of HSIs for the US-Basic HSI Design, that are applicable to the US-APWR and will be documented in the "US-APWR HSI Design Specification." This includes:

- Fixed position continuously visible HSI provided by:
    - The fixed area of the LDP (Table 18.7-1) - Section 4.9 “Large Display Panel” of Reference 18.7-1 provides the design basis and description of all LDP indications and alarmsand includes:
        - Bypassed and inoperable status indication (BISI) parameters

        - Type A and B post-accident monitoring (PAM) variables (Section 7.5, Table 7.5-3)
        - Safety parameter displays including status of critical safety functions and performance of credited safety systems and preferred non-safety systems
        - Prompting alarms for credited manual operator actions and risk-important HAs identified in the HRA
    - PAM displays for Type A and B variables on the safety VDUs (Subsection 7.5.1.1)
    - Conventional switches on the MCR operator console for system level actuation of safety functions such as reactor trip, engineering safety features actuation system (ESFAS) actuation, etc. (Tables 7.2-6 and 7.3-5)
- Class 1E HSI for control of all safety-related components and monitoring of all safety-related plant instrumentation provided on the safety VDUs, located on the MCR operator console and the remote shutdown console (Section 7.1).
- Minimum inventory for degraded HSI conditions - Section 4.11 “Response to HSI Equipment Failures” of Reference 18.7-1 provides the design basis and description of redundant and diverse HSI that supports the following degraded operating conditions:
    - Degraded operations based on loss of non-safety HSI. The plant is maintained in a stable condition through continued operation of normal automatic control systems and monitoring and controlling of critical safety functions through safety VDUs.
    - Degraded operations based on loss of safety and non-safety HSI due to common cause failure. HSI for accident mitigation and achieving safe shutdown is provided by the DHP (Subsection 7.8.3).
    - Degraded operations based on evacuation of the MCR. Safe shutdown is achieved through HSI at the RSC (Subsection 7.4.1.5).
    - Degraded operations based on single HSI failures. All information and controls are available to continue normal plant operation, manage accidents and achieve safe shutdown through alternate HSI devices (Reference 18.7-1, Subsection 4.11.2).

The safety VDUs provide backup HSI to accommodate complete failure of the non-safety HSI. The safety VDUs provide the following operational capabilities:

1. Maintain continued stable plant operation without exceeding the licensed thermal power limit, while maintaining all critical safety functions. Stable plant operation is capable of being maintained for a reasonable duration that permits non-safety HSI to be restored (ie. approximately 12 hours).

2. Manage AOOs and PAs identified in the safety analysis (Section 15) with the defined malfunctions and within the defined acceptance criteria.

3. Achieve safe shutdown (ie. cold shutdown) from the stable or abnormal plant conditions defined above.

Compliance to the safety VDU design basis defined above shall be demonstrated through validation test scenarios that include concurrent failure of all non-safety HSI. Validation testing is described in Section 18.10. Demonstrating compliance to the safety VDU design basis defined above does not require consideration of the following additional failures:

1. A concurrent safety VDU failure.

2. Beyond design basis events, such as Station Blackout.

3. Beyond design basis malfunctions, such as failure of multiple ESF trains/systems or additional non-safety failures that would lead to beyond design basis events.

18.7.3.3 HSI Change Process

The HFE Design Report (Reference 18-7-5) and HSI Design Implementation Plan (Reference 18.7-6) documents the process for the following HSI changes:

- Topical Report (Reference 18.7-1 Subsection 4.5.2 “Operation Method”) describes HSI for setpoints that are expected to be changed by operators during normal operations.

- HSIs designs that are modified and updated on a permanent basis (see Section 18.11).

- Temporary setpoint modifications. These changes are made through changes in the protection and safety monitoring system (PSMS) or plant control and monitoring system (PCMS) software. The software management life cycle process is described in Subsection 7.1.3.17.

- Configuration of operator-managed trend displays and operator-managed alarms. Operators can configure new trend displays and new alarms that are not pre-configured in the HSI design. The configuration tools ensure consistency with the HSI style guide. The operator-configured HSI does not change any pre-configured HSI. Operator-managed trend displays and operator-managed alarms are controlled through administrative procedures.

- Data entry into the PCMS for maintenance related work order management (Reference 18.7-1 Subsection 4.5.3). This function is administratively controlled.

18.7.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.7(1) Deleted

18.7.5 References

18.7-1 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 5, November 2011.

18.7-2 U.S. Nuclear Regulatory Commission, Human-System Interface Design Review Guidelines, NUREG-0700, Revision 2, May 2002.

18.7-3 Design for Control Rooms of Nuclear Power Plants, IEC 964, International Electrotechnical Commission, 1989.

18.7-4 Post-TMI Requirements, NRC Regulations Title 10, Code of Federal Regulations, Part 50.34.

18.7-5 HSI Design, MUAP-09019-P (Proprietary) and MUAP-09019-NP (Non−Proprietary), Revision 2, September 2012.

18.7-6 HSI Design Implementation Plan, MUAP-10009, Revision 2, September 2012.

18.7-7 US-APWR Verification and Validation Implementation Plan, MUAP-10012, Revision 2, September 2012.

18.7-8 US-APWR Human System Interface Verification and Validation (Phase 1a) MUAP-08014-P (Proprietary) and MUAP-08014-NP (Non-Proprietary) Revision 1, May 2011.

18.7-9 Nuclear power plants - Control rooms - Design, IEC 60964 ed2.0, International Electrotechnical Comission, February 2009.

Table 18.7-1 Parameters on LDP (Sheet 1 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm(Note 1)	OK Monitor(Note 2)	SPDS
Reactor Thermal Power	X							
Turbine Power	X							
Generator Power	X							
Nuclear Instrumentation System (NIS) Power	X	X						
Pressurizer Pressure	X	X				X		
Pressurizer Water Level	X	X			X	X		X
Pressurizer Reference Water Level	X							
RCS Average Temperature	X	X						
RCS Reference Temperature	X	X						
RCS Delta-Temperature	X	X						
RCS Hot Leg Temperature (Wide Range)					X			X
RCS Cold Leg Temperature (Wide Range)					X			X
RCS Subcooling (Loop)					X			X
RCS Subcooling (TC)					X			X
Core Outlet Temperature					X			X
RCS Pressure					X	X		X
Power Range Neutron Flux	X	X						
Intermediate Range Neutron Flux	X	X	X	X	X			X
Source Range Neutron Flux	X	X	X	X	X	X		X
Intermediate Range Neutron Flux Change Rate		X	X	X				X
Source Range Neutron Flux Change Rate		X	X	X				X
SG Water Level (Narrow Range)	X	X			X	X		X
SG Water Level (Wide Range)					X			X

Table 18.7-1 Parameters on LDP (Sheet 2 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm(Note 1)	OK Monitor(Note 2)	SPDS
SG Reference Water Level	X	X						
Main Steam Line Pressure	X	X			X	X		
Main Steam Line Flow	X	X						
Main Feed Water Flow	X	X				X		X
Main Steam Tie Line Pressure	X	X						
Main Feed Water Head Pressure	X	X						
Turbine First Stage Pressure	X	X						
Charging Water Flow	X	X						
Letdown Water Flow	X	X						
Boric Acid Tank Water Level								
Component Cooling Water Surge Tank Water Level								
Service Water Supply Line Pressure								
Containment Vessel (C/V) Pressure					X	X		X
C/V Temperature								X
C/V Annulus Pressure								
Class 1E Electrical Room Pressure								
Reactor Vessel Water Level					X			
Safety Injection Water Flow								
Residual Heat Removal (RHR) Flow								
Emergency Feed Water (EFW) Flow					X			X
C/V Spray Cooler Outlet Flow								X
Spent Fuel Pit Water Level								
Refueling Water Storage Pit (RWSP) Water Level					X			

Table 18.7-1 Parameters on LDP (Sheet 3 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm(Note 1)	OK Monitor(Note 2)	SPDS
EFW Pit Water Level					X	X		
C/V Sump Water Level						X		
C/V High Range Radiation Monitor								
C/V Dust Radiation Monitor						X		
C/V Gas Radiation Monitor						X		
Condenser Ejection Gas Radiation Monitor						X		
SG Blow Down Radiation Monitor						X		
Main Steam Radiation Monitor						X		
N-16 Main Steam Radiation Monitor						X		
Exhaust Duct Gas Radiation Monitor						X		
Control Room Emergency HVAC System Status								
Emergency Power Generator				X				
Reactor Trip Breaker Status		X	X	X			X	X
Control Rod Position	X	X	X			X	X	X
Pressurizer Depressurization Valve	X	X						
Pressurizer Depressurization Valve Shutdown Valve	X	X						
Pressurizer Spray Valve	X	X						
Pressurizer Back Up Heater	X	X						
Pressurizer Control Heater	X	X						
MFW Control Valve	X	X		X			X	
MFW Bypass Control Valve	X	X		X			X	
SG Makeup Water Line Valve		X					X	
MFW Isolation Valve	X	X		X			X	

Table 18.7-1 Parameters on LDP (Sheet 4 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm(Note 1)	OK Monitor(Note 2)	SPDS
EFW Isolation Valve				X			X	
Turbine Bypass Valve	X	X						
Main Steam Depressurization Valve	X	X						
Main Steam Relief Valve Isolation Valve	X	X						
Main Steam Isolation Valve	X	X		X			X	
Reactor Coolant Pump	X	X						
Charging Pump	X	X						
Component Cooling Water Pump		X		X			X	
Service Water Pump		X		X			X	
Safety Injection Pump				X			X	
C/V Spray/RHR Pump				X			X	
Emergency Feedwater Pump				X			X	
Instrument Air Compressor				X			X	
C/V Recirculation Fan				X			X	
Bearing Cooling Water Pump		X						
Main Turbine Stop Valve	X	X	X					
Main Turbine Control Valve	X	X	X					
Reheat Stop Valve	X	X	X					
Interceptor Valve	X	X	X					
Turbine Rotation Rate	X	X						
Deaerator Pressure	X	X						
Deaerator Tank Water Level	X	X						
Condenser Vacuum Rate	X	X						

Table 18.7-1 Parameters on LDP (Sheet 5 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm(Note 1)	OK Monitor(Note 2)	SPDS
Condensate Pump	X	X						
Condensate Booster Pump	X	X						
Circulating Water Pump	X	X						
Power Factor	X	X						
Generator Frequency	X	X						
Generator Voltage	X	X						
Generator Current	X	X						
Turbine Shaft Vibration	X	X						
Feed Water Pump	X	X						
Feed Water Booster Pump	X	X						
Transmission Voltage	X	X		X				
Class 1E 6.9kV Bus Voltage	X	X		X				
Non Class 1E 6.9kV Bus Voltage	X	X		X				
Main Transformer Circuit Breaker	X	X	X	X				
Generator Load Break Switch	X	X	X				X	
Generator Field Circuit Breaker	X	X	X				X	
Reserve Auxiliary Transformer Circuit Breaker	X			X			X	
Class 1E Emergency Power Generator Incoming Breaker	X	X		X			X	
Unit Auxiliary Transformer Incoming Breaker		X					X	
Class 1E 6.9kV Bus Power Receive Circuit Breaker	X			X				
Non Class 1E 6.9kV Bus Power Receive Circuit Breaker	X			X				
Switchyard Circuit Breaker		X						
Class 1E Direct Current Bus Voltage								

Table 18.7-1 Parameters on LDP (Sheet 6 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm (Note 1)	OK Monitor (Note 2)	SPDS
Reactor Trip Status			X				X	
Turbine Trip Status			X				X	
Generator Trip Status			X				X	
ECCS Status (ECCS Line-Up Valves)				X			X	
ECCS Sequence Components				X			X	
LOOP Sequence Components				X			X	
C/V Spray Sequence Components				X			X	
Main Control Room Isolation Sequence Components				X			X	
C/V Isolation Phase A (T Signal) Actuating Valves				X	X		X	X
C/V Spray Signal Actuating Valves				X			X	
C/V Isolation Phase B (P Signal) Actuating Valves				X	X		X	X
C/V Isolation Phase A (T Signal) & Emergency Bus Under Voltage Signal Actuating Valves				X			X	
Safety Injection Signal & Emergency Bus Under Voltage Signal Actuating Valves				X			X	
C/V Purge Isolation Signal Actuating Valves				X			X	
Main Control Room Ventilation Isolation Signal Actuating Valves				X			X	X
Automatic Activation Block				X				
Main Steam Bypass Start Up Valve				X			X	
EFW Pump Outlet Flow Control Valve			X				X	
EFWP Drive Steam Inlet Valve			X				X	
SG Sampling Line C/V Outside Isolation Valve				X			X	
SG Blow Down C/V Outside Isolation Valve				X			X	
SG Blow Down Stop Valve				X			X	

Table 18.7-1 Parameters on LDP (Sheet 7 of 7)

	Plant Power	Cause of Reactor Trip	Plant Trip	ESFAS Actuation	PAM	SDCV Alarm(Note 1)	OK Monitor(Note 2)	SPDS
Safety Interlock Bypass (BISI Component level)							X	

Note 1: SDCV: specially dedicated continuously visible

Note 2: Prior to safety system actuation, the OK Monitors indicate operability status (i.e., BISI). After safety system actuation, OK Monitors indicate actuation status.

18.8 Procedure Development

The objective of the procedure development program is to produce procedures that support and guide human interactions with plant systems and control plant-related events and activities. HFE principles and criteria are applied along with all other design requirements to develop procedures that are technically accurate, comprehensive, explicit, easy to use, and validated.

The scope of the procedures program for the US-APWR is described in Chapter 13 (Section 13.5). As described in Section 13.5, operational program procedure development is the responsibility of the COL Applicant, and is consistent with the development of other operational programs. The development and implementation of operational programs is the responsibility of the COL Applicant in accordance with SECY-05-0197 (Reference 18.8-8), as described in Section 13.4. .

18.8.1 Combined License Information

No additional information is required to be provided by a COL Applicant In connection with this section.

COL 18.8(1) Deleted

18.9 Training Program Development

The objective of the training program is to develop training for plant operations personnel, and personnel who maintain safety-related equipment. The scope of the training program for the US-APWR is described in Chapter 13 (Section 13.2). As described in Section 13.2, Training Development is an operational program. Consistent with the development of other operational programs, Training Development is the responsibility of the COL Applicant. The development and implementation of operational programs is made in accordance with SECY-05-0197 (Reference 18.9-5) as described in Section 13.4. The training program for safety-related operations and maintenance activities are developed in accordance with the HFE program described in this section. The training program:

- Evaluates personnel knowledge and skill requirements;
- Coordinates training program development with other elements of the HFE design process; and
- Implements training in an effective manner that is consistent with human factors principles and practices.

The US-APWR Training Program complies with the applicable requirements of NUREG-0800, Subsection 13.2.1 (Reference 18.9-1) and ensures operations and maintenance personnel maintain plant safety and respond to abnormal plant conditions.

The training of plant personnel addresses applicable guidance in Reference 18.9-1, Section 13.2 (“Training”, 13.2.1), as defined in 10 CFR 55.4 (Reference 18.9-2), and as required by 10 CFR 52.78 (Reference 18.9-3) and 10 CFR 50.120 (Reference 18.9-4).

18.9.1 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.9(1) Deleted

18.9.2 References

18.9-1 U.S. Nuclear Regulatory Commission, Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants, NUREG-0800, Subsection 13.2.1 “Reactor Operator Requalification Program; Reactor Operator Training,” March 2007.

18.9-2 Definitions, NRC Regulations Title 10, Code of Federal Regulations, Part 55.4,

18.9-3 Contents of Applications; Training and Qualification of Nuclear Power Plant Personnel, NRC Regulations Title 10, Code of Federal Regulations, Part 52.78.

18.9-4 Training and Qualification of Nuclear Power Plant Personnel, NRC Regulations Title 10, Code of Federal Regulations, Part 50.120.

18.9-5 Staff Requirements-SECY-05-0197-Review of Operational Programs in a Combined License Application and Generic Emergency Planning Inspections, Tests, Analyses, and Acceptance Criteria. SRM-SECY-05-0197, U.S. Nuclear Regulartory Commission, Washington, DC, February 2006.

18.10 Verification and Validation

18.10.1 Objectives and Scope

V&V evaluations comprehensively determine that the US-APWR design conforms to HFE design principles and that it enables plant personnel to successfully perform their tasks to achieve plant safety and other operational goals. Successful completion of integrated system validation is a critical design acceptance milestone for the US-APWR HSIS.

The scope of the V&V activity encompasses the MCR, RSC, TSC and LCSs that fall into the categories identified in Section 18.1.1.2. V&V of the EOF is outside the scope of the US-APWR V&V program; V&V will be conducted in accordance with the site specific HFE program to confirm compliance to NUREG-0696. However, communications between the MCR and the EOF, and between the MCR and other off-site entities (eg. emergency officials) are included in the V&V for the MCR. All aspects of the MHI US-APWR V&V program are controlled by the appropriate sections of Reference 18.10-1.

18.10.2 Methodology

The V&V methodology addresses the following topics:

- Operational conditions sampling: the selection of operational scenarios to be used in ISV
- HSI design verification: the evaluation of the HSI design for meeting tasks requirements and HFE guidelines
- Integrated system validation: the evaluation of whether the integrated system (hardware, software, and crew) meets performance requirements
- HED resolution: the resolution of potential human performance issues identified in V&V evaluations

US-APWR Verification and Validation Implementation Plan, Reference 18.10-5, provides a description of the US-APWR HFE V&V program, including the methodology used to develop that program. The US-APWR HFE V&V program is based on the HFE V&V program for the Japanese plants that have or will employ the Japanese Basic HSIS. The Japanese HFE V&V program encompasses the HSI design and procedure development. The Japanese and international standards, Japanese nuclear power plant operating experience, and NRC directed operating considerations have been applied to the US-APWR HFE V&V program and are discussed in Reference 18.10-5.

The US-APWR HSIS, including procedures, is based on the Japanese Basic HSIS, including procedures for conventional Japanese PWRs. The changes to HSI and procedures are described in Sections 18.7 and 18.8, respectively. The US-APWR HFE V&V program encompasses the completely integrated HSIS, including aspects of the design that are the same as the Japanese Basic HSIS and changes that are unique to the US-Basic HSIS or unique to the US-APWR HSIS.

18.10.2.1 Operational Conditions Sampling

This portion of the V&V process identifies a sample of operational conditions that are to be used as the basis for ISV activities. This sample:

- Includes conditions that are representative of the range of events that could be encountered during operation of the plant. This includes normal plant evolutions, design basis AOOs and PAs, and beyond design basis events.

- Reflects the characteristics that are expected to contribute to system performance variation including degraded HSI conditions, such as loss of all non-safety HSI and loss of digital HSI due to common cause failure.

- Considers the safety performance of HSI components. For example, safety VDUs have limited functionality to accommodate design basis events, therefore they cannot be expected to provide sufficient functionality for beyond design basis conditions.

The operational scenarios, events, transients, and accidents used in V&V are based on their risk importance and the extent to which they encompass all aspects of the US-APWR HSIS. The complete basis for operational conditions sampling and samples of selected operational conditions are described in the US-APWR V&V implementation plan, Reference 18.10-5.

18.10.2.2 Design Verification

All aspects of the US-APWR HSI are verified, including HSI that is needed for scenarios that are not included in the ISV. The verification activities are conducted using actual HSI displays generated by system software and actual HSI control panels. The aspects of the Design Verification that are addressed are discussed below. The task analysis is used as the principal source for verifying the HSI inventory contained in alarms, displays and controls. The US-Basic HSI Style Guide (see Section 18.7.2.5) is used as the principle source for verifying the detailed HSI implementation. The Design Verification:

- Confirms that the inventory and characterization of all HSI components (alarms, controls, displays and related equipment) meet the HSI inventory and characterization requirements defined in the task analysis. This activity is sometimes referred to as HSI Task Support Verification

- Confirms that the characteristics of the HSI, and the environment in which it is used, conform to HFE guidelines, as defined in the US-Basic HSI design style guide. The US-Basic HSI style guide was verified against Reference 18.10-3 during its development. Reference 18.10-3 is also used for confirmation of detailed characteristics that may not be included in the HSI design style guide

- Identifies any inventory or characterization non-conformance and documents those as HEDs. HEDs are resolved as described in Section 18.10.2.4.

Verification for the US-APWR HSIS is conducted in two phases, as follows:

- Phase 1 (References 18.10-6) - This phase verifies the US-Basic HSIS.
  - For this phase, the US-Basic HSIS is developed based on the Japanese Basic HSIS, as described in Reference 18.10-2.
  - Verification confirms the complete US-Basic HSI style guide conforms to Reference 18.10-3.
  - Verification includes a sampling of the HSI inventory (alarms, displays and controls) which are included in the simulator used for Phase 1 validation.
  - Verification is documented in Reference 18.10-6 (Part 1).
- Phase 2 (Reference 18.10-5) - This phase verifies the US-APWR HSIS.
  - Verification encompasses 100% of the US-APWR HSI inventory for conformance to the US-Basic HSI style guide.
  - Any aspects of the US-Basic HSIS that are affected by the detailed design of the US-APWR HSIS will be re-verified.
  - Verification in this phase is conducted in accordance with Reference 18.10-5.
  - Verification in Phase 2 may be subdivided into (1) HSI needed to support the scenarios selected for ISV (2) the remaining HSI.

18.10.2.3 Integrated System Validation

The integrated system validation is the process by which an integrated system design (i.e., hardware, software, and personnel elements) is evaluated to determine whether it acceptably supports safe operation of the plant. This process evaluates the acceptability of those aspects of the design that cannot be determined through such analytical means as HSI task-support verification and HFE design verification.

Integrated system validation is conducted using actual dynamic HSI with high fidelity plant model simulation of the operational conditions samples. Reference 18.10-5, describes the process for the integrated system validation methodology.

The methods for integrated system validation include the following aspects of the validation methodology:

- Test objectives
- Validation test beds
- Plant personnel
- Scenario definition including initial plant conditions, plant transients or accidents and complicating equipment malfunctions

- Performance measurement
  - Measurement characteristics
  - Performance measure selection
  - Performance criteria
- Test design
  - Coupling crews and scenarios
  - Test procedures
  - Test personnel training
  - Participant training
  - Pilot testing
- Data analysis and interpretation
- Pass/fail Acceptance Criteria
- Validation conclusions

Plant personnel performing operational events for the validation use a simulator or other suitable representation of the system (referred to as a test bed) to determine its adequacy to support safety operations. The test bed of the MCR is a full-scope US-APWR control room simulator which as been demonstrated consistent with the validation test bed criteria specified in NUREG 0711, Rev. 2, Section 11.4.3.2.2, Validation Testbeds, using ANSI/ANS 3.5-1998, Reference 18.4-10, as a guide. Other test beds modeling locations outside the MCR are represented by part task or limited scope simulations, meeting the guidelines of Reference 18.10-4, Appendix D, or by mockups or analysis. Deviations from the requirements of Reference 18.10-4 that are judged to be acceptable for the purposes of HSI validation, as compared to operator training, are documented and justified in the HSI V&V procedure.

The validation is undertaken after significant HEDs that were identified in verification reviews have been resolved, since these can negatively affect performance and the results of validation. A description of HEDs identified during the validation and their resolution is documented.

The US-APWR HSIS, including procedures, is based on the Japanese Basic HSIS design and procedures that were validated, as described in Reference 18.10-2, Appendices A and B. Validation for the US-APWR HSIS is conducted in two phases, as follows:

- Phase 1 (References 18.10-6 and 18.10-7) - This phase validates the US-Basic HSIS design.

- The US-Basic HSIS is developed based on the Japanese Basic HSIS, as described in Reference 18.10-2
- This phase is conducted by a sample of US operations crews who are previously trained on the utilization of the Japanese HSI and procedures, and operation of the Japanese standard 4-loop PWR
- Operational conditions samples used during this phase are those that assist with validation of the basic HSI design for cross-cultural differences and population stereotypes
- This testing was divided into Phase 1a and 1b. The test reports for each phase are documented in Reference 18.10-6 (Part 1) and 18.10-7 (Part 3), respectively.
- Design changes resulting from HEDs generated during Phase 1a that have not been fully validated in Phase 1b or design changes resulting from HEDs generated during Phase 1b are encompassed in the validation testing of Phase 2.

• Phase 2 (Reference 18.10-5) - This phase validates the US-APWR HSIS.

  - This phase is conducted by US operations crews who are trained on the utilization of the US-APWR HSIS, including procedures, and operation of the US-APWR plant systems. This phase integrates the US-Basic HSIS with the HSI inventory for a complete US-APWR plant, to yield the US-APWR HSIS. The complete US-APWR is defined based on assumptions for the portion of the US-APWR that are site-specific (e.g. switchyard and ultimate heat sink).
  - Operational conditions samples used during this phase conform to all of the selection criteria in Subsection 18.10.2.1
  - Validation in this phase is conducted in accordance with Reference 18.10-5.

Phases 1 and 2 are non-recurring validation activities. HEDs that pertain to Phase 2 ISV Acceptance Criteria will be resolved prior to completing Phase 2. Changes needed to resolve other HEDs, or changes to site specific assumptions that are needed to accommodate actual site specific differences, are addressed through the Design Implementation program element, as described in Section 18.11.

18.10.2.4 Human Engineering Discrepancy Resolution

HED resolution is performed iteratively throughout all V&V activities. HEDs identified during a V&V activity are evaluated to determine if they must be resolved prior to conducting other V&V activities. The purpose of the HED resolution is to verify the adequate completion of the following tasks:

• Evaluation of HEDs to determine the need for corrective action, assigning appropriate priority, and assigning an organization to be responsible for resolution

- Identification of design solutions to address significant HEDs along with an indication of their current status (implemented or scheduled to be implemented)
- Determination of the HFE Program activities that must be re-performed to satisfy the requirements of the limited reapplication of the HFE analysis processes, as described in Sections 18.3 through 18.6
- Verification of the implementation of the design solutions resolving HEDs including how the change complies with the V&V evaluation criteria

HEDs are not considered in isolation and, to the extent possible, their potential for interaction with other HED disposition activities are considered when developing and implementing solutions. For example, if the HSI for a single plant system is associated with many HEDs, then the set of design solutions are coordinated to enhance overall performance and avoid incompatibilities between individual solutions. Approaches that develop design solutions to some HEDs before all have been identified from a particular verification or validation activity are acceptable provided that the potential interactions between HEDs are specifically considered prior to implementing the design solutions.

18.10.3 Results

The V&V Phase 1 results are documented in Reference 18.10-6 Part 1, and Reference 18.10-7, Part 3. The Phase 2 results, which include V&V program staffing and resources, the detailed procedures for conducting the V&V program, the V&V program data, analysis, and results, identification, and resolution of HEDs, and the major conclusions from these activities along with their bases, will be documented in a results summary report in accordance with Reference 18.10-5.

Phase 1 verification and validation activities for the US-Basic HSIS, as documented in References 18.10-6 and 18.10-7, are not credited for the US-APWR HSIS verification and validation, as required by NUREG-0711 Section 11. Phase 1 V&V activities are considered part of the US-Basic HSIS design process. Compliance to NUREG-0711 Section 11, relies on the Phase 2 V&V program which will be conducted in accordance with Reference 18.10-5.

18.10.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.10(1) Deleted

COL 18.10(2) Deleted

18.10.5 References

18.10-1 Quality Assurance Program (QAP) Description for Design Certification of the US-APWR, PQD-HD-19005, Revision 5, Mitsubishi Heavy Industries, Ltd., May 2013.

18.10-2 HSI System Description and HFE Process, MUAP-07007-P (Proprietary) and MUAP-07007-NP (Non-Proprietary), Revision 5, November 2011.

18.10-3 U.S. Nuclear Regulatory Commission, Human-System Interface Design Review Guidelines, NUREG-0700, Revision 2, May 2002.

18.10-4 Nuclear Power Plant Simulators for Use in Operator Training, ANSI/ANS 3.5, 1998.

18.10-5 US-APWR Verification and Validation Implementation Plan, MUAP-10012, Revision 2, September 2012.

18.10-6 US-APWR Human System Interface Verification and Validation Phase 1a, MUAP-08014, Revision 1, May 2011.

18.10-7 US-APWR Human System Interface Design, MUAP-09019, Revision 2, September 2012.

18.11 Design Implementation

18.11.1 Objectives and Scope

The objective of the design implementation program element is to demonstrate that the design that is implemented (i.e., the "as-built" design) accurately reflects the design that has been verified and validated in the V&V program element, Section 18.10. In addition, the design implementation program element will identify and evaluate aspects of the design that were not addressed in the V&V program. These may be site-specific aspects that were not included in V&V or design changes that occur after V&V. It is noted that while successful ISV marks the end of the V&V program element, Section 18.10, the HSI design will continue to be challenged during Phase 3 of the HFE program, which includes operator training (see Section 18.1.5). HEDs generated during the V&V program that do not affect the ISV acceptance criteria or conclusions, and any HEDs generated after completion of the V&V program element, will be resolved during the Design Implementation program element.

In this section, the referenced changes after V&V apply to any changes made to the US-APWR design following the V&V program element, Section 18.10, but prior to fuel load. HSI changes that occur after fuel load are managed by the COL holder as plant design changes.

18.11.2 Methodology

The detailed HSI design implementation process is performed and documented as described below.

The design implementation methodology includes the following features:

- Aspects of the design that were not addressed in the design V&V are evaluated by the HFE team. For HSIs that were included in the V&V program, but have been modified to accommodate site-specific design features, a regression analysis will be conducted to determine what aspects of prior HFE program elements must be repeated. The regression analysis will assess the modified HSIs individually. as well as the effects on the completely integrated HSI.

- For HSI features that have been included within each HFE program element but were not evaluated in the V&V program element, a specific method of V&V will be determined. V&V methods include the use of table-top walkthroughs, mock-ups, part task simulators and plant walk-downs. This is expected to apply to HSI features that (1) are outside the scope of a typical MCR simulator (eg. HSI for local equipment testing) or whose detailed implementation was not available in time to support ISV, and (2) are evaluated to have no impact on the ISV.

- Completely new HSI features will be evaluated in accordance with each HFE program element. If the evaluation concludes the HSI has no impact on ISV, then a specific V&V method will be determined as explained above. Otherwise, the aspects of ISV that are impacted by the new HSI feature will be repeated.The potential impact on HAs is assessed and a risk significance level is assigned in accordance with the criteria in Reference 18.11-1

- All HFE-related issues documented in the issue tracking system are verified to be adequately addressed

The detailed implementation process is described in the Design Implementation Plan (MUAP-10013, R0), Reference 18.11-2.

18.11.3 Results

The activities conducted during the Design Implementation program element are described in the Design Implementation result summary report. The result summary report includes:

- The configuration control identification methods used to confirm both as-built hardware and software are equivalent to that tested during the V&V program element.

- Changes from the V&V test bed, and the HFE methods used to determine the acceptability of those changes.

18.11.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.11(1) Deleted

COL 18.11(2) Deleted

18.11.5 References

18.11-1 U.S. Nuclear Regulatory Commission, Guidance for the Review of Changes to Human Actions, NUREG-1764, Revision 1, September 2007.

18.11-2 US-APWR Design Implementation Plan, MUAP-10013, Revision 2, September 2012.

18.12 Human Performance Monitoring

18.12.1 Objectives and Scope

Human performance monitoring applies after the HSI has been turned over to the COL holder for fuel load, and continues throughout plant operation. Human performance monitoring within the scope of this program specifically applies to the following:

- Time critical operator actions
- Correct diagnosis of abnormal plant events
- Accuracy of procedure execution

Monitoring of human performance in other areas is within the scope of other plant programs (such as, "Fitness for Duty").

Human performance during the ISV of the V&V program element is a key factor in determining the acceptance of the US-APWR HSIS. Human performance monitoring is intended to detect degradation in operator performance compared to the performance observed during ISV. Degradation may be due to many factors that occur over the life of the plant, including changes in personnel, changes in plant culture, changes in training methods, or changes in the HSI design itself. The Human Performance Monitoring program is a catalyst for corrective actions that are managed within the corrective actions program.

18.12.2 Methodology

A human performance monitoring (HPM) strategy is developed and documented. The US-APWR HPM process guides human performance monitoring for the life of the plant. It guides the process for identification and disposition of human performance issues. The Human Performance Monitoring program element is applicable after the completion of integrated HSI validation and operator training.

This process evaluates the impact of facility design and operating changes and addresses the following topics:

- Confirmation of the following criteria:
  - Effectiveness of HSIs
  - Personnel performance impacts of HSI, procedure, and training changes
  - Operator actions meet time and performance criteria
  - Maintenance of human performance criteria which are established during integrated system validation
- Human performance trending of the following elements:

  - Performance degradation
  - Failures
  - Detection sensitivity
  - Safety Importance
- Human performance evaluation criteria, including the following:
  - Specific cause determination
  - Safety Importance
  - Feedback of information
  - Corrective actions

The US-APWR relies on a robust set of computer based recording systems to collect and store plant data that may help to understand trends and the sequence of events and conditions leading up to a problem such that the role the human played in the problems initiation, progression, consequence, and recovery can be determined, in most anticipated cases. This plant data is expected to directly support the plants corrective action tracking system. Human performance will be monitored and documented based on actual plant conditions during plant commissioning and commercial operation. This is accomplished through review of computer event logs, which include process parameter and component status history along with computer based procedure execution history, and post event personnel debriefings. Evaluation techniques are used (see References 5-16, 17 and 18) to gather the required information from these data systems to evaluate trend and determine problem causes and corrective actions.

However, in some cases when human performance under actual plant conditions cannot be monitored, measured or simulated, such as for local control stations or manual actions outside of the main control room, available information that is determined by judgment to most closely approximate performance data under actual conditions will be used. In these cases, a hierarchical and systematic logic (see MUAP-10014, References 5-16, 17, and 18) will be applied to the evaluation, selection and documentation of the appropriate surrogate data.

18.12.3 Results

HPM implementing procedures are developed and documented in accordance with the HPM Implementation Plan, Reference 18.12-1. Human performance issues are tracked and dispositioned in a timely manner by the implementation procedures. Disposition of the human performance issues is documented in a periodic status report.

18.12.4 Combined License Information

No additional information is required to be provided by a COL Applicant in connection with this section.

COL 18.12(1) Deleted

18.12.5 References

18.12-1 Human Performance Monitoring Implementation Plan, MUAP-10014, Revision 2, September 2012.