REVISED RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.:	**502-8647**
SRP Section:	**07.07 – Control Systems**
Application Section:	**7.7.1.1**
Date of RAI Issue:	**07/01/2016**

Question No. 07.07-17

Regulatory Basis:

10 CFR 52.47(a)(3)(i) requires compliance with 10 CFR 50, Appendix A, "General design criteria [GDC]." GDC 19 requires in part that, "Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown...."

10 CFR 52.47(a)(8) requires compliance with parts of 10 CFR 50.34(f). 10 CFR 50.34(f) requires in part that, "...each applicant for a design certification,...under part 52 of this chapter shall demonstrate compliance with the technically relevant portions of the requirements in paragraphs (f)(1) through (3) of this section..." 10 CFR 50.34(f)(2)(iii) requires, "...a control room design that reflects state-of-the-art human factor principles..."

10 CFR 52.47(a)(9) requires, "For applications for light-watercooled nuclear power plants, an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application...."

10 CFR 52.47(a)(28) requires compliance with 10 CFR 50.150. 10 CFR 50.150 states, in part, “using realistic analyses, the applicant shall identify and incorporate into the design those design features and functional capabilities to show that, with reduced use of operator actions: (i) The reactor core remains cooled, or the containment remains intact; and (ii) Spent fuel cooling or spent fuel pool integrity is maintained.” SRP Section 19.5 states in part, “the staff shall consider…use of operator action to be reduced when (1) all necessary actions to control the nuclear facility can be performed in the control room, or at an alternate station containing equipment specifically designed for control purposes, and (2) a reduced amount of active operator intervention, if any, is required to meet the assessment criteria in 10 CFR 50.150(a)(1).”

Information in the Design Certification Application:

DCD Tier 2, Section 7.7.1.1.o.3.c states, “The RCC [Remote Control Center] is designed against aircraft impact to meet the requirements of 10 CFR 50.150…The operator can shut down the reactor from the MCR [Main Control Room] 10 minutes before aircraft impact upon the MCR in the auxiliary building, and the control and monitoring is transferred to the RCC using a transfer switch located in the MCR.”

Additionally, the response to RAI 356-7881, Question 07-5 (ADAMS Accession No. ML16126A066), states, "The RCC provides manual control and monitoring means to bring the plant to hot standby under accident conditions. The RCC is manipulated by one reactor operator who monitors and controls the plant." Further, the response states that "the controls and displays available at the RCC have been designed according to the guidelines in NUREG-0700, “Human-System Interface Design Review Guidelines.” The RCC has not been specifically described in Chapter 18; however, design of the RCC will follow the NUREG-0711, human factors engineering process as a local control station facility."

Questions:

1. Describe any design features and functional capabilities that will provide operators with advance notification of an aircraft impact event such that they will be able to perform necessary actions before leaving the MCR (e.g., trip the reactor and transfer control to the RCC from the MCR) and transit to the RCC before aircraft impact occurs. Also, provide a description of the design features and functional capabilities in the DCD.

2. Explain why 10 minutes is a sufficient amount of time for operators to transfer control from the MCR to the RCC and walk to the RCC before aircraft impact occurs.

3. The application describes the RCC as an alternative to the main control room, and therefore it is akin to the remote shutdown room (RSR), not a local control station. Therefore, the design of the RCC should conform to the design method described in NUREG-0711 in the same way that the RSR conforms to this method. Provide direction in the "HSI Design Implementation Plan," APR1400-E-I-NR-14007, Section 4.2.8, "Central Facilities," for the RCC to follow the design process described in NUREG-0711.

Response – (Rev. 1)

Response to Question 1:

The operators are provided with advance notification of a potential aircraft impact event from the government or military agencies. The offsite communication system, including a dedicated hot line to the MCR, is used to communicate with government or military agencies, as described in DCD Tier 2, Section 9.5.2.2.2.3. Steps that the operators will take once notified will be detailed in procedures that are to be developed by the COL applicant.

The COL applicant is to provide the emergency offsite communication system including a dedicated hotline, local law enforcement radio equipment, and a wireless communication system as specified in COL Item 9.5(9).

Response to Question 2:

Five minutes is an approximate time based on practical estimations of time to trip the reactor, transfer control from the MCR to the RCC, and the walking distance and path to the RCC that it would take operators once notified of a potential impact event. The appropriateness of the time to trip the reactor and transfer the control from the MCR to the RCC will be verified during the Task Analysis process using the simulator.

After the control actions are complete from the MCR (i.e., tripping the reactor and transferring controls from the MCR to the RCC), the operators will transition to the RCC through the plant corridors and the stairs. Since the pathway at elevation 137 ft 6 in is blocked by the pipe lines, it is anticipated that the operators would go down to elevation 120 ft and then up to elevation 137 ft 6 in using the adjacent stairs.

The estimated time for taking control actions and relocating to the RCC, including the selected path, are as follows:

TS

TS

Table 1 Estimated Time for Control Actions and Movements

	Description	Distance (ft)	Time (min:sec)
Control Action	Reactor Trip	10	0:40
	Transfer Control from MCR to RCC	10	1:00
Moving Path	MCR to “A” (Corridor)	115	0:32
	El. 156’-0” to El. 120’-0” (Stair)	72	0:40
	“B” to “C” (Corridor)	213	1:00
	El. 120’-0” to El. 137’-6” (Stair)	32	0:18
	“D” to RCC (Corridor)	165	0:46
Total		**617**	**4:56**

Notes:

1) The performance times for tripping the reactor and transferring control from the MCR to the RCC are representative times based on operator training observation
2) The walking speed is assumed to be 3.6 ft/sec for corridor and 1.8 ft/sec for stairs. (See DCD Tier 2, Table 12.4-8 (2 of 11))

The total predicted time is estimated to be less than 5 minutes to take the appropriate control actions and for operators to transition to the RCC. Based on the above analysis, DCD Tier 2, Section 7.7.1.1.o.3.c will be changed to reflect the capability to shutdown the reactor and take control from the RCC within 5 minutes.

Response to Question 3:

The design of the RCC conforms to the design method described in NUREG-0711 in the same way that the RSR conforms to this method. The "HSI Design Implementation Plan," APR1400-E-I-NR-14007 will be revised to include the RCC as indicated in the attachment associated with this response.

Impact on DCD

DCD Tier 2 Section 7.7.1.1.o.3.c will be revised as shown in Attachment 1 associated with this response.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Technical report APR1400-E-I-NR-14007-P/NP, Rev. 0, “HSI Design Implementation Plan,” will be revised, as indicated in Attachment 2 associated with this response.

the sump provides an alarm in the MCR to alert the operator of the presence of water in that area.

b) Hydrogen mitigation system

The HMS allows adiabatic, controlled burning of hydrogen at low concentrations during degraded core accident conditions. Divisionalized HMS igniters are manually actuated from the MCR.

The HMS controls and instrumentation are described in Subsection 6.2.5. Electrical power distribution is described in Section 8.3.

c) Remote control center

The RCC is designed against aircraft impact to meet the requirements of 10 CFR 50.150 (Reference 11). The minimum equipment needed to maintain the reactor for 24 hours is provided to accomplish hot standby plant condition. The operator can shut down the reactor from the MCR ~~10~~ five minutes before aircraft impact upon the MCR in the auxiliary building, and the control and monitoring is transferred to the RCC using a transfer switch located in the MCR. The RCC is located separately from the MCR so that aircraft impact to the MCR does not adversely affect the RCC operation integrity.

The RCC panel consists of divisionalized safety control and non-safety controls to achieve plant hot shutdown. The signals from the RCC are routed from the RCC to the I&C equipment room as well as to the motor control center (MCC) through multiplexers.

Insert "A" on following page

7.7.1.2 Main Control Room Facility

The MCR facilities are composed of the following major functional units:

a. The MCR includes the MCR operator consoles, a large display panel (LDP), safety console, and an adjacent meeting room.

b. The computer room contains the IPS that monitors plant performance, drives various display units, and logs plant data.

"A"

The remote control center (RCC) is designed with the following design features:
- The RCC provides manual control and monitoring means to bring the plant to hot standby under accident conditions.
- The RCC is manipulated by one reactor operator who monitors and controls the plant.
- For control and monitoring, the RCC provides four divisionalized engineered safety features (ESF) component control system (CCS) soft control modules (ESCMs) for safety component control and process monitoring. Conventional hardwired switches, related indicators, and non-safety component control are also provided.
- The ESCMs and conventional switches in the RCC are physically separated from the MCR and RSR. These ESCMs are connected to the ESF-CCS loop controller (LC) in the remote multiplexer (MUX) room through a dedicated route which is separated from the routes of the main control room (MCR) and the remote shutdown room (RSR). The conventional switches are connected to the P-CCS cabinets in the remote MUX room through a dedicated route. This route also is separated from the routes of the MCR and the RSR.
- In normal conditions, the MCR/RCC transfer switch is in MCR mode and the signals from the control channel gateway (CCG) of the RCC are disconnected. When the MCR/RCC transfer switch is switched to the RCC mode, the signals from the CCG of the RCC are connected to the ESF-CCS LC and the signals from CCG of the MCR are disconnected.
- No single credible event that would require the concurrent evacuation of the MCR and the RSR (or fire damage in the MCR and RSR) would make the RCC inoperable.
- The ESF-CCS LCs and P-CCS LCs that are related with plant hot shutdown are interfaced with the RCC panel.
- MCR/RCC transfer switches are located in the MCR. MCR/RCC transfer switches are provided for safety division A, B, C, D, and the non-safety division. One transfer switch is provided for each division of ESF-CCS LC and each division of P-CCS LC, respectively. These transfer switches disconnect signal paths between the ESCMs in the MCR and the RSR and ESF-CCS LC in the remote MUX room.
- The RCC panel room is located on the opposite side of the plant from the MCR and the RSR so that an aircraft impact cannot affect the MCR, RSR, and the RCC panel.
- The ESCMs on the RCC are seismically and environmentally qualified as class 1E.
- The ESCMs on the RCC have same design features as those on the MCR and the RSR. The ESCMs are verified to meet independence, physical separation, and EMI/RFI requirements as described in DCD Tier 1, Section 2.5.4.1, Items 2 and 16 and as detailed in the corresponding ITAAC.

The I&C system architecture for the RCC panel is shown in Figure 7.7-14.

ABSTRACT

This document provides the implementation plan (IP) for the human factors engineering (HFE) human-system interface design (HD) program element (PE), one of 12 PEs in the Advanced Power Reactor 1400 (APR1400) HFE Program. This IP governs the technical activities conducted in the HD PE by defining the scope, methodology, output products, and the qualifications of the personnel who conduct the PE.

The main purpose of the HD PE is to create functional designs for the following:

, and remote control center (RCC)

,

1. The detailed design for the APR1400 Basic Human-System Interface (HSI), which establishes the generic indication, alarm, control, and procedural methods applied to all systems and functions controlled from the main control room (MCR) ~~and the~~ remote shutdown room (RSR). The same HSI methods apply to the safety parameter display system (SPDS) indications in the MCR and the technical support center (TSC). The APR1400 Basic HSI also defines indication, alarm, and control methods for local control stations (LCSs) used for important human actions (IHAs). The detailed design for the APR1400 Basic HSI is an extension of the conceptual design described in APR1400 Basic Human-System Interface Technical Report (TeR) (Reference 2); the conceptual design of the APR1400 Basic HSI is based on the Basic HSI of the predecessor design (Shin Kori Nuclear Power Plant Units 3 and 4 [SKN 3&4]).
2. The APR1400 HSI System (HSIS), which establishes soft and conventional indications, alarms, controls and operating procedures that encompass the HSI inventory in the task analysis (TA) HFE PE and APR1400 plant system designs, within the generic HSI methods defined in the APR1400 Basic HSI.
3. APR1400 HSI Facilities, which include the ARP1400 MCR, RSR, and TSC. The facility designs accommodate the APR1400 HSIS as well as storage, communication, meeting, and other habitability features important to support required operations crew performance during all facets of plant operation.

RCC,

The integration of the APR1400 HSIS and APR1400 HSI Facilities is referred to as the APR1400 HSI Design.

This HD IP controls the HSI design process and scope, including the translation of HSI inventory requirements from the TA PE into the detailed designs of alarms, displays, controls, and other aspects of the HSI. Key HD outputs include soft graphical displays, soft and conventional controls, alarm prioritization and applicability logic, computer-based operating procedures, control consoles and the configuration of control rooms. This IP provides reasonable assurance that these functional designs reflect the systematic application of HFE principles and criteria through the generation of design documents, prototypes, part-task simulators and focused design tests.

HD uses input from the following APR1400 HFE PEs to create its outputs: functional requirements analysis and function allocation (FRA/FA), treatment of important human actions (TIHA), TA, staffing and qualifications (S&Q), and procedure development (PD). The end product of the HD is the functional design of the APR1400 HSI (i.e., the APR1400 HSI Design), which is incorporated into the detailed designs of HSI hardware, software, and physical facilities. The APR1400 HSI design is then formally verified and validated in the human factors verification and validation (V&V) HFE PE through high fidelity simulation.

The HD for the APR1400 Basic HSI may be conducted at any time because it does not depend on the output of other APR1400 HFE PEs, which are incorporated primarily to generate the APR1400 HSI inventory. The HD for the APR1400 HSIS is conducted after the Basic HSI is documented (as defined herein) after the APR1400 HSI inventory is identified through the HFE PEs identified above and after the instrumentation and control (I&C) design requirements are established by the mechanical and I&C system designers for each APR1400 plant system. The piping and instrumentation diagrams (P&ID) are the starting point for creating HSI indication and control designs during the HD PE. The APR1400

OPR	Optimized Power Reactor
P-CCS	process- component control system
PE	program element
PD	procedure development
P&ID	piping & instrumentation diagram
PPS	plant protection system
PRA	probabilistic risk assessment
QIAS-N	qualified indication and alarm system-non-safety
QIAS-P	qualified indication and alarm system-p
RCC	remote control center
ReSR	results summary report
RG	Regulatory Guide
RO	reactor operator
RSR	remote shutdown room
RT	reactor trip
S&Q	staffing and qualifications
SDCV	spatially dedicated and continuously visible
SKN 3&4	Shin-Kori Nuclear Power Plant Units 3 and 4
SLI	system level initiation
SME	subject matter expert
SPDS	safety parameter display system
SPM	success path monitoring
SS	shift supervisor
STA	shift technical advisor
TA	task analysis
TAA	transient and accident analysis
TeR	technical report
TIHA	treatment of important human actions
TO	turbine operator
TS	trade secret
TSC	technical support center
V&V	verification and validation
VDU	visual display unit

1 PURPOSE

This document provides the implementation plan (IP) for the human factors engineering (HFE) human-system interface design (HD) program element (PE), which is one of 12 PEs in the APR1400 HFE Program. This IP governs the technical activities conducted in the HD PE by defining the scope, methodology, output products, and the qualifications of the personnel who conduct the PE.

The HD PE creates the functional designs of the APR1400 Human-System Interface (HSI Design), which includes:

, , and remote control center (RCC),

1. The detailed design of the APR1400 Basic HSI, which establishes the generic indication, alarm, control, and procedural methods applied to all systems and functions controlled from the main control room (MCR) ~~and the~~ remote shutdown room (RSR). The same HSI methods apply to the safety parameter display system (SPDS) indications provided in the technical support center (TSC). The APR1400 Basic HSI also defines indication, alarm, and control methods for local control station (LCSs) used for important human action (IHAs). The HD uses the APR1400 Basic HSI to provide reasonable assurance that the HSI design is consistently applied throughout the APR1400 plant systems and at the HSI locations credited for controlling the critical safety functions (CSFs) and critical power production functions (CPPFs) defined by the functional requirements analysis / function allocation (FRA/FA), during normal and degraded HSI conditions.

   The conceptual design of the APR1400 Basic HSI is described in “APR1400 Basic Human-System Interface” (Reference 2) and APR1400 Basic HSI Style Guide (Reference 4). The Basic HSI concept includes the HSI accommodations for the plant’s operations staff, such as the ergonomic designs of operator consoles, the safety console, and their architectural configurations to provide reasonable assurance of visibility and audibility for crew coordination.

   The Basic HSI concept also defines the criteria and methods for spatially dedicated and continuously visible (SDCV) HSI, the methods for Class 1E and diverse HSI, and the strategies for managing degraded HSI. This IP governs the evolution of the APR1400 Basic HSI concept into APR1400 Basic HSI detailed design through the documentation of detailed functional designs, prototype development, and design tests using U.S. licensed reactor operators.

2. The APR1400 HSIS, which refers to the soft and conventional indications, alarms, controls and operating procedures that encompass the HSI inventory defined by the TA and plant system designs, within the HSI methods defined in the APR1400 Basic HSI. The APR1400 HSIS encompasses all plant operating modes, including shutdown and refueling, for both normal and abnormal conditions.

   While the TA and plant system designs define the HSI inventory using text descriptions and characterizations, the HD reflects the inventory in graphical displays, soft controls, and conventional controls that integrate multiple, related inventory components. The HD integration is based on the inventory component relationships within plant systems, operator tasks, and plant functions using the generic techniques defined in the APR1400 Basic HSI Style Guide. The HD also expands the alarm inventory from the TA and plant system designs, to establish prioritization of and applicability to plant and system operating modes. The HD results in a hierarchical structure of alarms, displays, controls, and procedures that promote a mental model of the plant and plant-wide situation awareness, from the highest level functions to the success path actions needed to maintain these functions.

   The HD process for the APR1400 HSIS starts with the APR1400 Basic HSI and the HSI inventory defined in Chapter 7 of the APR1400 Design Control Document (DCD) (Reference 11) to fulfill regulatory guidance, such as indications, alarms, and controls for credited manual actions, controls for manual initiation of automated protective functions, indications on the SPDS, and

indications and controls for common cause failure (CCF) conditions. HD creates graphic displays, soft controls and conventional controls to fulfill that DCD inventory and to fulfill the expanded HSI inventory defined by the TA and plant system designs. , RCC,

3. The APR1400 HSI , which are the MCR, RSR and TSC, which accommodate the APR1400 HSIS as well as storage, communication, meeting, and other habitability features important to facilitating required operations crew performance during all facets of plant operation. The HD establishes the architectural configuration of operations crew offices, kitchen, and restroom facilities; meeting areas; and facility lighting requirements. It provides reasonable assurance that the HSI facilities accommodate face-to-face interaction between the operations crew and other plant staff without interfering plant operations. The HD also establishes the functional design of voice communications and paging throughout the plant and in designated offsite facilities for emergency plan coordination during abnormal events. The HD generates the three-dimensional plant model for the MCR and the functional aspects of the MCR simulator specification for the integrated system validation (ISV), which is conducted during V&V.

The integration of the APR1400 HSIS and APR1400 HSI Facilities is referred to as the APR1400 HSI Design. This HD IP defines the activities that are necessary to develop the APR1400 HSI Design. The activities include the incorporation of HFE design standards and guidance applicable to the APR1400 HSIS, as defined in the APR1400 Basic HSI Style Guide and NUREG-0700 (Reference 5), into the APR1400 HSI Facilities. This IP provides a systematic approach to integrating the HFE design standards, guidance, and results of other HFE PEs into a comprehensive HSI design process. The integration provides reasonable assurance that the resulting HSI resources and facilities effectively support performance of operational functions and tasks.

The end product of the HD PE is the functional design of the APR1400 HSI (i.e., the APR1400 HSI Design), which is implemented into the detailed designs of HSI hardware, software, and physical facilities by APR1400 engineers in multiple disciplines. The APR1400 HSI Design is formally verified and validated during the V&V through high-fidelity simulation.

A key purpose of the HD is to provide reasonable assurance that the end product (i.e., APR1400 HSI Design) reflects the resolutions of all human engineering discrepancies (HEDs) generated in previous HFE PEs and the resolutions of any HEDs that may have been generated during the HD. While the APR1400 HSI Design must reflect all HED resolutions, closure of all HEDs is not required for completion of the HD because some HEDs may require resolution to be successfully demonstrated during the ISV of the V&V.

As demonstrated in Appendix A, this IP conforms to the review criteria in Section 8 of NUREG-0711, “Human Factors Engineering Program Review Model,” Rev. 3 (Reference 10).

This document defines the qualifications of the subject matter experts (SMEs) required to conduct HD and the independent review of its output products. This document also defines the required content of the HD ReSR, which demonstrates that the HD was conducted in accordance with this IP.

2 SCOPE

RCC, , RCC,

The scope of the HD includes the facility design of the MCR, RSR, and TSC. The scope also includes the HSIS design of the MCR and a subset of the HSIS, which is applied to the RSR and TSC. For the emergency operation facility (EOF), the scope of the HD is limited to the HSI inventory for the SPDS. For the LCSs, the scope of the HD is limited to the HSI used for IHAs.

The HD scope is divided into the following areas:

- APR1400 Basic HSI
- APR1400 HSI System
- APR1400 HSI Facilities

The scope of each area is defined in Subsections 2.1, 2.2, and 2.3.

2.1 APR1400 Basic HSI

The APR1400 Basic HSI encompasses the physical design of the MCR, which includes operator consoles, the safety console, the large display panel (LDP), and furnishings such as book cases and work tables. The APR1400 Basic HSI defines the generic methods for controls, alarms, information displays, and procedure displays. These generic HSI methods are applied to Basic HSI functions, such as CBPs, critical function monitoring (CFM), success path monitoring (SPM), accident monitoring instrumentation (AMI), and bypassed and inoperable status indication (BISI). All Basic HSI functions are seamlessly integrated through Basic HSI features such as the information display hierarchy, single point alarm acknowledgment, intuitive diagnostic drill down and inter-function navigational hyperlinks. These physical and functional resources constitute the APR1400 Basic HSI, within which the HSI inventory for the APR1400 plant system designs is implemented.

The HD initially expands the APR1400 Basic HSI concept, which is described in the APR1400 Basic HSI Description technical report (TeR) in conjunction with the APR1400 Basic HSI Style Guide. The scope of the APR1400 Basic HSI includes:

1. The design basis (i.e., the HSI inventory selection criteria) for SDCV indications and alarms to be displayed on the non-safety LDP and safety related displays. SDCV alarms and indications promote plant level situation awareness.
2. The design basis for SDCV controls and their location within the HSI facilities.
3. The methods (e.g., dynamic video symbols, conventional HSI components) for all displays, alarms and controls, including distinctions required to accommodate Class 1E HSI, diverse HSI, and LCS HSI, and for providing operator feedback to control actions.
4. Criteria for alarm applicability and prioritization and the display and control methods for alarm states and priorities.
5. Design criteria for graphic displays including density, graphic symbol and character size, line thickness, and information orientation.
6. The video display hierarchy, including the function, task, and system design content of each hierarchical level.
7. The navigation methods between and within hierarchical display levels and between alarms, displays, controls, and CBPs and methods for providing operator feedback to screen selection actions.
8. CBP methods, including navigation within and among procedures, place keeping, annotations and bookmarks, multiple procedure usage, independent step verification, archiving, automated data checking, and provisions for continuous action steps.
9. Configuration of operator consoles and the safety console and their arrangement within the HSI facilities.
10. Methods for control transfer between HSI facilities.

11. Nomenclature and labeling standards for all elements of both soft and conventional HSI, including abbreviations and syntax for labels and alarm messages.

The APR1400 Basic HSI also establishes standard functional specifications for the indications and controls associated with plant instrumentation and components, referred to as the basic component control and instrumentation design guide. The guide provides reasonable assurance of HSI consistency across all APR1400 plant systems.

2.2 APR1400 HSIS

The HD implements the HSI inventory defined by the TA and plant system designs in the Basic HSI methods described above, which encompass both video and conventional devices. For plant systems that are site specific, such as the switchyard and ultimate heat sink, the HD is based on generic assumptions that are made to establish a complete plant design that is reflected in the complete APR1400 HSIS. These generic assumptions are modified as necessary for each plant-specific application of the APR1400 during the design implementation (DI) HFE PE.

The scope of the APR1400 HSIS encompasses soft displays and controls, and conventional displays and controls for all aspects of the APR1400 Basic HSI, as follows:

1. Large display panel (LDP); SDCV sections
2. Information flat panel displays (IFPDs); selectable displays with soft controls, including SPDS (displays are also applicable to the selectable sections of the LDP)
3. Engineered safety features control modules (ESCMs); selectable soft controls
4. Qualified indication and alarm system –- non-safety (QIAS-N); SDCV and selectable displays
5. Qualified indication and alarm system – post accident monitoring (QIAS-P); SDCV and selectable displays
6. Plant protection system (PPS) and core protection calculator (CPC) operator modules; selectable displays with soft controls
7. Reactor trip (RT) and engineered safety features (ESF) system-level initiation (SLI) controls; conventional SDCV controls
8. Minimum inventory controls (MICs); conventional SDCV controls
9. Diverse manual actuation (DMA) controls; conventional SDCV controls
10. Diverse indication system (DIS); selectable displays
11. Safety console configuration (encompassing all items above, except LDP and IFPD)
12. Alarms that are displayed on the LDP, IFPDs, and QIAS-N displays
13. LCS; conventional indications and controls

For all items in the above list, the HD generates pictorial design drawings with a database that correlates each pictorial element to a unique instrumentation or control item in the plant system designs. The pictorial designs integrate the HSI inventory defined by the TA and plant system designs in the information hierarchy of the APR1400 Basic HSI, using the conventions established by the APR1400 Basic HSI Style Guide.

, RCC,

As for all computer driven displays, the HD graphical design output for the SPDS is implemented in software for the MCR, RSR and TSC. However, for the EOF the HD output for the SPDS is provided only to define the HSI inventory requirements and to provide guidance for graphical implementation of the SPDS within the EOF. The EOF HSI system is provided by the combined license (COL) applicant. Therefore, the COL applicant provides the actual graphical design and software for the SPDS in the EOF, in accordance with the EOF HSI system style guide to provide reasonable assurance of conformance with the HFE criteria for the EOF.

The HD PE also includes the CBPs that are used for the scenarios conducted during the ISV. Other procedures that are unrelated to the V&V scenarios are not within the scope of the HD PE because they have their own development and verification program through the procedure development (PD) PE.

Placeholders for the additional procedures are included in the APR1400 HSIS to provide reasonable assurance of completeness of the information inventory and to avoid operator bias during the ISV.

2.3 APR1400 HSI Facilities

RCC,

The APR1400 HSI Facilities included in this HD PE are the MCR, RSR, TSC, and LCSs. The EOF facility is in the scope of the COL applicant; therefore, the EOF is outside the scope of the APR1400 HD PE (except for the HSI inventory requirements and implementation guidance for the SPDS, as described above).

RCC,

For the MCR, RSR, and TSC, the HD generates functional designs or design requirements that address the follow facility characteristics:

1. Arrangement of operator consoles, safety console, and LDP
2. Arrangement of meeting tables and chairs, desk areas and laydown areas for plant drawings, documents, and procedures
3. Location and functional configuration of communications devices for paging, plant announcements, and telecommunications
4. Location of personal computers, printers, and other components of the plant's information technology system
5. Storage facilities for documents, drawings, operating procedures and equipment for the plant's emergency plan
6. Location of entries and exits, kitchen, and restroom facilities
7. Location of offices for plant personnel and meeting rooms with an emphasis on their visibility and accessibility into the control areas
8. Ambient noise requirements, and facility features to minimize noise and provide reasonable assurance that normal voice communications are audible in required locations
9. Lighting requirements, and facility features to provide reasonable assurance that lighting minimizes glare on visual display units and conventional control devices and that facility features provide reasonable assurance that lighting is adequate in areas where documents and drawings must be read.
10. Requirements for environmental conditions that promote comfortable working conditions.

For LCSs, the HD provides reasonable assurance of timely area accessibility, adequate task lighting and a non-hazardous environment that does not require onerous personnel hazard protection.

3.2.8 Safety Console

TS

3.2.9 Local Control Stations

TS

3.3 APR1400 Facilities

TS

3.3.1 Central Facilities

TS

3.5.3 Task Analysis

TS

3.5.4 Treatment of Important Human Actions

TS

3.5.5 Staffing and Qualifications

TS

3.5.6 Procedure Development

TS

3.5.7 Training Program Development

TS

4 IMPLEMENTATION

This section describes the HD implementation plan for:

- APR1400 Basic HSI (Subsection 4.1)
- APR1400 HSIS and APR1400 Facilities (Subsection 4.2)

4.1 APR1400 Basic HSI

TS

TS

4.1.1.1 LDP

TS

4.1.1.2 Soft Control

TS

4.1.1.3 Information Display Hierarchy

TS

4.1.6.1 Functional Specifications

TS

4.1.6.2 Basic HSI Style Guide

TS

TS

4.2.8 Central Facilities

TS

8 DEFINITIONS

, , and RCC,

APR1400 Basic Human-System Interface (HSI): Generic indication, alarm, control and procedure methods applied to all systems and functions controlled from the MCR ~~and the~~ RSR. The same HSI methods apply to the SPDS indications provided in the MCR and the TSC. The APR1400 Basic HSI also defines indication, alarm, and control methods for LCSs used for IHAs.

APR1400 HSI Design: Complete integration of the APR1400 HSIS and APR1400 HSI Facilities (see definitions below).

RCC,

APR1400 HSI Facilities: ARP1400 MCR, RSR, TSC and LCSs. The facility designs accommodate the APR1400 HSIS (see definition below) as well as storage, communication, meeting and other habitability features important to support required operations crew performance during all facets of plant operation.

APR1400 Human-System Interface System (HSIS): The soft and conventional indications, alarms, controls, and operating procedures that encompass the HSI inventory defined by the TA PE and APR1400 plant system designs within the generic HSI methods defined by the APR1400 Basic HSI.

Independent reviewer: Person with qualifications equivalent to the originator of a product but not engaged in preparing the product.

Known aspect: An aspect of the APR1400 plant design or APR1400 Basic HSI design that is documented at the time of the HFE analysis.

Performance-based testing: Testing using dynamic simulation and plant operators that includes scenarios targeted to confirm the design of specific HSI features.

Preferred emergency success path: The first set of plant structures, systems, and components, defined by the EOPs for event mitigation. EOPs may define alternate success paths if the preferred success path does not function as expected.