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.: **383-8458**

SRP Section: **18 – Human Factors Engineering**

Application Section:

Date of RAI Issue: **02/01/2016**

Question No. 18-107

NUREG-0711, Criterion 8.4.5(1), states that an applicant should identify degraded HIS conditions.

The Basic HSI TeR, Section 3.1.3, “Safety Console,” says that the Safety Console (SC) will have one information flat panel display (IFPD). DCD Tier 2, Figure 7.1-1, “APR1400 I&C System Overview Architecture,” includes a drawing of the SC, but the staff did not see an IFPD or an interface with the Information Processing System (IPS) included in the graphic. Also, the Control System CCF Analysis Technical Report (APR1400-Z-J-NR-14012-P, Rev. 0), Section 4.4.4.2, "Design Features to Cope with Spurious Component Selection Commands," indicates that IFPDs are not on the SC.

Clarify whether or not an IFPD is available on the Safety Console. Revise the submittal as necessary.

Response

There is no Information Flat Panel Display (IFPD) on the Safety Console (SC) in the APR1400 design.

Section 4.1.1, “Basic HSI Design,” and Section 4.1.3.1, “Failure of Individual HSI Components,” of the HSI Design Implementation Plan (HD IP) will be revised to match DCD Tier 2, Figure 7.1-1, “APR1400 I&C System Overview Architecture.”

Also, Section 3.1.3, “Safety Console,” of the Basic Human-System Interface Technical Report (TeR) will be revised to delete the sentence which indicates there is an IFPD on the Safety Console.

Impact on DCD

There is no impact on the DCD.

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-NP, Rev. 0, “HSI Design Implementation Plan,” Section 4.1.1 and 4.1.3.1, and technical report APR1400-E-I-NR-14011-P/NP, Rev. 0, “Basic Human-System Interface,” Section 3.1.3 will be revised, as indicated in the attachment associated with this response.

TS

TS

4.1.1 Basic HSI Design

TS

4.1.3 Basic HSI Concept for Degraded I&C and HSI Conditions

The APR1400 Basic HSI accommodates the following degraded HSI conditions:

- Failure of individual HSI components
- Loss of all non-safety HSI
- CCF of all digital safety systems
- MCR evacuation

The design basis and design features of the APR1400 Basic HSI to cope with each condition are described in Subsections 4.1.3.1 through 4.1.3.5.

4.1.3.1 Failure of Individual HSI Components

TS

TS

3.1.3 Safety Console

TS

3.1.4 Facility

TS

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.: **383-8458**

SRP Section: **18 – Human Factors Engineering**

Application Section:

Date of RAI Issue: **02/01/2016**

Question No. 18-109

NUREG-0711, Criterion 8.4.5(1), states that the applicant should identify the effects of automation failures and degraded conditions on personnel and plant performance.

The staff reviewed the HD IP, Section 4.1.3.5, “Failure of I&C Components;” the Basic HSI TeR; DCD Tier 2, Chapter 7, Table 7.7-1, "Control Groups for the NSSS Control Functions,"; the Control System CCF Analysis; and the CCF Coping Analysis. The staff did not find where the application addresses the effects of automation failures and degraded conditions (in automated control processes) on personnel performance.

Provide a description of how automation failures and degraded I&C conditions identified in DCD Tier 2, Chapter 7 and associated technical reports effect personnel performance. Revise the submittal as necessary.

Response

The effects on APR1400 personnel performance due to automation failures and degraded HSI conditions are unknown at this time. However, these effects are determined and assured acceptable through various HFE program activities, which are documented in the following HFE program elements:

DCD:

18.2.2.4 Issues Identified by Plant Personnel

Plant personnel interviews are conducted to determine operating experience related to predecessor plants and systems. OER issues obtained during the interviews are reviewed and documented by the HFE design team. The following topics are included in the interviews:

a. Plant operation …

2) Instrument failures (e.g., safety system logic and control unit, fault-tolerant controller, communication systems)

3) HSI equipment and processing failure (e.g., loss of displays, loss of information processing system, loss of large display panel)

b. The interviews will include structured questions regarding: …

2) Failure modes and degraded conditions of the instrumentation and control (I&C) systems

3) Degraded conditions of the HSI

18.3.2.2 Methodology for Function Allocation

The FA generates not only the primary allocations to personnel, but also considers their responsibilities to monitor automatic functions and to assume manual control in event of an automatic system failure. The operator's role in executing safety functions is summarized as follows:

b. Detect degradations and failures

18.4.1 Objectives and Scope

The TA scope includes:

a. TA is implemented for plant operations tasks…This encompasses … the following degraded HSI conditions:

1) Continued stable operation with loss of all non-safety HSI

2) Accident mitigation and safe shutdown with only safety HSI

3) Accident mitigation and plant stabilization with concurrent common-cause failure (CCF) in digital I&C systems (as defined by the D3CA)

4) Safe shutdown from the RSR

18.7.2.1 HSI Design Input

The analyses that are conducted prior to HD are used to identify HSI requirements. The analyses include the following:

c. TA – HSI requirements to support the role of personnel are provided by TA. TA encompasses tasks that are necessary to control the plant for the full range of operating conditions, from normal through accident conditions, during normal and degraded HSI conditions.

18.10.2.2 Integrated System Validation

The pass or fail performance evaluation measures include directly observable performance data such as the execution time of operator tasks, frequency of human error, and measurable plant performance data collected by the test bed simulator. The diagnostic measures also include indirectly measurable performance data such as operator task load, situational awareness, and collaboration between operators. The validation includes operator interaction with the emergency operating procedures (EOPs) and other operating sequences to meet the following objectives:

f. Operation with HSI and instrumentation and control (I&C) equipment failures

OER IP:

4.3 Operator Interviews as a Source of Operating Experience

The interviews will include structured questions regarding:

- Normal plant evolutions
- Failure modes and degraded conditions of the instrumentation and control (I&C) systems
- Degraded conditions of the HSI …

4.10 Important Human Actions

The OE reviewer identifies OE that involves actions similar to the IHAs …These human actions shall be any action, including backup manual actions (including actions taken owing to the failure of an automatic system) that the reviewer regards as needed for accident mitigation. The OE reviewer will determine if there are aspects of the design (from the OE) that ensure or deter success of the human action. If errors occurred in the execution of the human action, these OEs will also be captured as lessons learned and therefore HEDs. These HEDs will be tracked to resolution in the ITS.

TA IP:

4.1 Task Selection

The TA task selection methodology ensures that the TA encompasses:

4. Tasks related to monitoring of automated systems that are important to power production
5. Tasks that involve the use of automated support aids for personnel, such as computer-based procedures
6. Tasks related to identifying the failure or degradation of automation, and implementing backup responses

4.2.2.1 Process Monitoring

13. Backup: All parameters are displayed on non-safety HSIs. If that is all that is required, “none” is entered. If the parameter is credited for a degraded HSI condition, “safety” is entered if the parameter is needed for loss of all non-safety HSI or “diverse” is entered if the parameter is needed to cope with accidents with a concurrent CCF.

TIHA IP:

2 SCOPE

These APR1400 analyses encompass actions taken by operators from the Main Control Room (MCR) and other plant areas. Abnormal and accident conditions include both normal and degraded HSI conditions as defined in the analysis.

3.4.1 Operating Experience Review

The HFE Operating Experience Review (OER) PE identifies past human performance (HP) issues in operating plants. OER highlights any HP issues that describe actions ‘similar’ to the RIHAs or DIHAs documented in the TIHA ReSR…

The OER evaluates the HFE characteristics for each ‘similar’ action to identify any HFE characteristic that may adversely affect human performance. If an HFE characteristic that may adversely affect human performance is identified and is not correctly included in the PRA, TAA or D3CA, as documented in the TIHA ReSR, a Human Engineering Discrepancy (HED) is generated.

V&V IP:

4.1.1 Sampling Dimensions

A. Plant Conditions

Operational conditions consist of normal operation that commonly takes place during the life of the plant, abnormal operation due to an equipment failure or a system failure, and emergency operation resulting from an unexpected event that may lead to radiation release. …

Abnormal operation includes operation with the following failures present (including a design bases accident (DBA) in progress):

- I&C system failure and degraded conditions, including sensor, monitoring, automation, and control/communications subsystem failures and malfunctions (e.g., safety system logic and control unit, fault tolerant controller)
- Common cause failure of the I&C system during a design basis accident (Reference 5)
- HSI failure including, loss of processing or display capabilities for alarms, displays, controls, and computer-based procedures

Impact on DCD

There is no impact on the DCD.

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

There is no impact on any Technical, Topical, or Environmental Report.

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.: **383-8458**

SRP Section: **18 – Human Factors Engineering**

Application Section:

Date of RAI Issue: **02/01/2016**

Question No. 18-110

NUREG-0711, Criterion 8.4.5(2), states that the applicant should specify the alarms and other information personnel need to detect degraded I&C and HSI conditions in a timely manner, and to identify their extent and significance.

The staff reviewed the HD IP, Section 4.1.3.5, “Failure of I&C Components,” which includes a general statement that alarms and other information will be used to inform the operators of degraded I&C conditions. However, the HD IP does not include a detailed method for how these alarms and information will be designed and presented to the operator. Additionally, some of the alarms appear to be identified in other sections of the application (e.g., the Control System CCF Analysis Technical Report, Table 5.1-2, “Multiple Failure due to a Single Failure of Shared Signals”).

Provide a detailed method in the HD IP to ensure that the alarms and other information that personnel will need to detect and identify the extent and significance of degraded I&C systems, automation failures, and degraded HSI conditions will be specified. If the alarms and other information have already been identified in another section of the application, then the HD IP should include this information or identify where it can be found in the application.

Revise the submittal as necessary.

Response

The HSI inventory requirements are generated through the TA program element and plant system designs, not the HSI Design program element. HD determines how to present that HSI inventory, including alarm context and prioritization. The HSI Design Implementation Plan (HD IP), APR1400-E-I-NR-14007, Rev. 0, ABSTRACT, Sections 1, 3.2.3, 3.2.5, 3.5.3, 4.2.5 and 4.1.3.1, and the Task Analysis Implementation Plan (TA IP), APR1400-E-I-NR-14004, Rev. 0, Sections 4.2.1 and 4.2.2 will be revised to clarify that the HSI inventory requirements, which are

an input to HD, support degraded I&C systems, automation failures, and degraded HSI conditions, as indicated in the attachment associated with this response.

Impact on DCD

There is no impact on the DCD.

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-NP, Rev. 0, “HSI Design Implementation Plan,” ABSTRACT, Sections 1, 3.2.3, 3.2.5, 3.5.3, 4.2.5 and 4.1.3.1, and Technical Report APR1400-E-I-NR-14004-NP, Rev. 0, “Task Analysis Implementation Plan,” Sections 4.2.1 and 4.2.2 will be revised, as indicated in the attachment associated with this response.

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:

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.

The integration of the APR1400 HSIS and APR1400 HSI Facilities is referred to as the APR1400 HSI Design. This includes HSI inventory requirements to support degraded I&C systems, automation failures, and degraded HSI conditions.

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

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:

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

Abnormal conditions include degraded I&C systems, automation failures, and degraded HSI conditions.

TS

3.2.1 Critical Safety Function Displays

TS

3.2.2 System Displays

TS

3.2.3 Task Displays

TS

3.2.4 Application Displays

TS

TS

3.2.5 Alarms

TS

3.2.6 Computer-Based Procedures

TS

3.2.7 Performance-Based Tests

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

TS

4.2.5 Alarms

TS

TS

TS

4.2.2. Human-System Interface Inventory

Page intentionally blank

TS

TS

4.2.2.1. Process Monitoring

TS

TS

4.2.3. Task Evaluation

Page intentionally blank