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.:	**356-7881**
SRP Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	
Date of RAI Issue:	**01/04/2016**

Question No. 07-18

Describe the mechanisms in place that would allow operators to determine whether the QIAS-N and IFPDs have undergone a failure.

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. The QIAS-N and IFPDs, located in the main control room (MCR) provide alarm, display and controls for operators. In Section 7.7.1.4 of APR1400 FSAR Tier 2, regarding the IFPDs, the applicant states that, “If a data communication error occurs, an appropriate message is generated.” For information displays, the applicant does not appear to state in the licensing documentation how an operator can determine whether a failure such as a common cause failure has occurred such that the displays are frozen up or affected by some other means. Therefore, it is not apparent that an appropriate error message could be generated to alert the operator(s) to a random or common cause failure, for non-safety or safety-displays. Failures of the IFPDs are addressed in Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.” However this document does not address how operators would make the initial determination that IFPDs have experienced a failure of some type.

Describe the mechanisms, procedures, or processes in place for the APR1400 design that would allow operators to be alerted to a failure of either the QIAS-N or the IFPDs (e.g. frozen displays or controls).

Response – (Rev. 2)

The applicant’s response to RAI 323-8281 07.03-19 provides the mechanisms that will alert operators when the information flat panel display (IFPD) is malfunctioning.

The QIAS-N processor receives safety system signals via the ITP. The QIAS-N MTP receives non-safety system signals via the multi-channel gateway. Isolation devices are used between the ITP and QIAS-N processor, and between the multi-channel gateway and QIAS-N MTP. The QIAS-N processor performs applicable calculations based on the data received from the safety systems and non-safety systems. The QIAS-N MTP provides maintenance and testing means of the QIAS-N, and a gateway function with the multi-channel gateway to provide communication from the non-safety P-CCS. The QIAS-N server contains the process database, updates the values and status of the database records, executes the alarm processing function, and functions as a gateway between the QIAS-N network and QIAS-N display network.

The data from the QIAS-N processor (safety system signals) and the data from the QIAS-N MTP (non-safety system signals) are broadcasted on the QIAS-N network. The QIAS-N server captures the data from the QIAS-N network and updates the QIAS-N process database. The QIAS-N server broadcasts them on the QIAS-N display network for indication on the QIAS-N displays (QIAS-N FPDs, mini-LDPs, and SODPs).

To inform operator of QIASN-N failure, the QIAS-N server provides system diagnostic functions as follows:

a. Monitor the QIAS-N MTP, QIAS-N processor, QIAS-N network, QIAS-N display network.

b. Detect QIAS-N trouble and generate QIAS-N trouble status signals.

c. Transfer the QIAS-N trouble status to the non-safety IPS for alarm purpose.

d. Transfer the QIAS-N trouble status to the QIAS-N MTP via QIAS-N network for indication on the QIAS-N MTP displays.

e. Transfer the QIAS-N trouble status to the QIAS-N FPDs, mini-LDPs, and SODPs via QIAS-N display network.

The operator controls the plant utilizing four ESCMs, four IFPDs, and the associated mouse on the operator console. An operator console is considered inoperable when one of the following occurs: 1) Three IFPDs and each mouse are unavailable, 2) Three ESCMs are unavailable, or 3) The workstation disable switch is switched to “disable mode”.

The workstation disable switch (WDS) is to disconnect the signal interface of the IFPD and peripheral devices (e.g., mouse, keyboard) from the node of the DCN-I network should these non-safety devices generate spurious signals.

The WDS is located on each operator console and is a hardwired two-position (enable/disable) type of cam switch. Therefore, there are five WDSs for the RO, TO, EO, SS, and STA console. The keyboard, monitor, and mouse of the operator console are connected to the keyboard/video/mouse (KVM) extender. The KVM extender sends signals over an internal communication cable between the KVM extender and the network switch. When the WDS is switched to the disable mode, the switch disconnects 120 Vac power that comes from the power branch of the non-safety vital bus power supply system (VBPSS) to the KVM extender on the corresponding operator console. The configuration of the WDS will be shown in APR1400 DCD Tier 2, Figure 7.7-15.

The WDS does not have any software and, therefore, is not subject to a software CCF. The failure of a WDS does not impact any safety devices, including ESCMs at the operator console, because the WDS does not have any interfaces with safety devices. If a single failure of a WDS occurs, the operator can use the IFPD and peripheral devices at another operator console. A multiple failure of all five WDSs occurring concurrently is highly unlikely because the WDSs are hardwired devices and each WDS is separated, which enables an operator to perform the required operator actions on the safety console.

Impact on DCD

The APR1400 DCD Tier 2, Rev. 0 has been revised to reflect the changes indicated in the Rev. 1 response to Subsection 7.5.1.1, Figure 7.5-2, and Figure 7.9-1.

The APR1400 DCD Tier 2, Rev. 1 Subsection 7.5.1.1 and Subsection 7.7.1.2 will be revised and Figure 7.7-15 will be added as indicated in the Attachment 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

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

RAI 356-7881 - Question 07-18_Rev.2

c. Transfer the QIAS-N trouble status to the non-safety IPS for alarm purpose.

d. Transfer the QIAS-N trouble status to the QIAS-N MTP via QIAS-N network for indication on the QIAS-N MTP displays.

e. Transfer the QIAS-N trouble status to the QIAS-N FPDs, mini-LDPs, and SODPs via QIAS-N display network.

The operator controls the plant utilizing four ESCMs, four IFPDs, and the associated mouse on the operator console. An operator console is considered inoperable when one of the following occurs: 1) Three IFPDs and each mouse are unavailable, 2) Three ESCMs are unavailable, or 3) The workstation disable switch is switched to "disable mode."

The detailed information of workstation disable switch is provided in Subsection 7.7.1.2.

~~The workstation disable switch on the operator console is a hardwired two-position type of cam switch. This switch can disconnect the non-safety power to the IFPD and peripheral devices by switching the mode to the "disable mode."~~

The QIAS-N is physically separated and electrically isolated from the IPS and QIAS-P so that the failure of QIAS-N does not cause a loss of the IPS or QIAS-P.

The QIAS-N is seismically qualified for physical and functional integrity to enhance information availability.

The block diagram for the QIAS-N is shown in Figure 7.5-2.

Information Processing System (IPS)

The IPS displays all AMI variables on the information flat panel display (IFPD) of the consoles in the MCR and RSR and provides permanent historical recordings of AMI variables. All information displayed and recorded within the IPS is provided and available upon the operator's demand. The IPS also displays AMI information on the IFPD and LDP. The IPS also includes a historical data storage, retrieval, and trending capability. The IPS design includes data links to the on-site TSC and to the EOF to provide the capability for monitoring plant conditions at these locations. The IPS is described in Subsection 7.7.1.4.

7.5.1.2 Inadequate Core Cooling Monitoring Instrumentation

The ICC monitoring instrumentations are designed to meet the requirements of NUREG-0737, Item II.F.2.

RAI 356-7881 - Question 07-18_Rev.2

1) All MCR circuits (e.g., flat panel displays, switches) are isolated from the electronics (e.g., controller cabinets, monitoring systems, instrumentations) to which they interface. Similarly, all RSC circuits are isolated from the electronics. Therefore, the MCR operator consoles, LDP, safety console, and RSC circuits are inherently isolated from each other.

2) All MCR operator consoles, safety console, and RSC circuits are designed passively. Momentary contacts are used for all switches, and the memory of MCR operator consoles and safety console commands is retained only in electronics located in the I&C equipment rooms. This passive design is used for discrete state component controls, setpoint change commands, and position change commands from process controllers for analog components. This passive design provides reasonable assurance that transfer of control from the MCR to the RSR (or vice versa) is bumpless (i.e., no setpoints or component states are affected). This design also provides reasonable assurance that all open circuit failures have no impact on control setpoints, modes, or component states

3) The MCR, RSR, and I&C equipment rooms are located in separate fire zones. Therefore, the plant can be safely shut down with a catastrophic fire in the MCR, the RSR, or any one of the I&C equipment rooms.

Insert "A" on the next page

MCR/RSR master transfer switches are provided in the RSR and I&C equipment rooms for transfer of control from the MCR to the RSR. If a fire is detected within the MCR consoles, as indicated by an early warning smoke detector, the operator actuates the switches. Actuation of the switches initiates the transfer to deactivate the MCR consoles as a control interface and to activate the RSC control interface. The MTP provides interlocks for performing the transfer of control from the MCR to the RSR.

b. TSC and ERF Interfaces

The guidance for the TSC and the ERF is defined in NUREG-0696 (Reference 13). The guidance provides basic design and qualification criteria for the onsite TSC, operation support center (OSC), the near-site emergency operations facility (EOF), and the emergency response data system (ERDS).

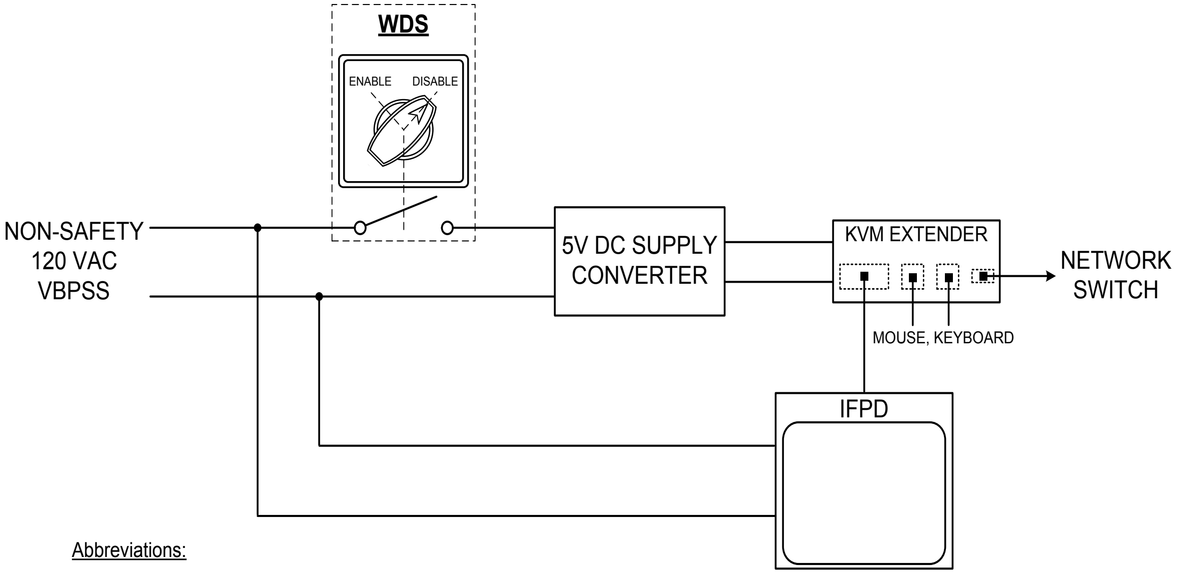
RAI 356-7881 - Question 07-18_Rev.2

"A"

The workstation disable switch (WDS) is to disconnect the signal interface of the IFPD and peripheral devices (e.g., mouse, keyboard) from the node of the DCN-I network should these non-safety devices generate spurious signals.

The WDS is located on each operator console and is a hardwired two-position (enable/disable) type of cam switch. Therefore, there are five WDSs for the RO, TO, EO, SS, and STA console. The keyboard, monitor, and mouse of the operator console are connected to the keyboard/video/mouse (KVM) extender. The KVM extender sends signals over an internal communication cable between the KVM extender and the network switch. When the WDS is switched to the disable mode, the switch disconnects 120 Vac power that comes from the power branch of the non-safety vital bus power supply system (VBPSS) to the KVM extender on the corresponding operator console. The configuration of the WDS will be shown in Figure 7.7-15.

The WDS does not have any software and, therefore, is not subject to a software CCF. The failure of a WDS does not impact any safety devices, including ESCMs at the operator console, because the WDS does not have any interfaces with safety devices. If a single failure of a WDS occurs, the operator can use the IFPD and peripheral devices at another operator console. A multiple failure of all five WDSs occurring concurrently is highly unlikely because the WDSs are hardwired devices and each WDS is separated, which enables an operator to perform the required operator actions on the safety console.



Abbreviations:

IFPD	: Information Flat Panel Display
KVM	: Keyboard/Video/Mouse
VBPSS	: Vital Bus Power Supply System
WDS	: Workstation Disable Switch

Figure 7.7-15 Configuration of Workstation Disable Switch

New figure 7.7-15 is added into DCD Tier 2, Rev.1, Section 7.7