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.: **45-7883**

SRP Section: **07.09 - Data Communication Systems**

Application Section:

Date of RAI Issued: **06/23/2015**

Question No. 07.09-3

Address multidivisional control and display stations staff guidance for the data communication interface between the Information Flat Panel Display (IFPD) and Engineered Safety Features-Component Control System Soft Control Module (ESCM).

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, “Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function,” and Clause 5.6.3, states, in part, “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Technical Report, APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System,” describes the design features of the APR1400 digital I&C system and how the design complies with NRC regulation. Technical Report, Appendix C, Section C.3, "Data Communication Systems" states, in part, “DI&C-ISG-04 Section 3 is not applicable as described in Section C.5.3." Section C.5.1.5 discusses communication between IFPD and ESCM, and that data sent from IFPD to ESCM are used to support operator's manual action.

Although the ESCM may not be used to perform a credited safety function, it appears to the staff that the component data from IFPD (non-safety control) to ESCM (safety-related) may be used to control safety-related equipment. Section 3.1.1 of DI&C-ISG-04 provides guidance on the control of safety-related equipment from a non-safety workstation. Based on the staff’s understanding of the interface between ESCM and the IFPD, the staff finds that the non-safety

IFPD is used to indirectly control safety-related equipment. Thus, the guidance of DI&C-ISG-04 applies. The staff requests the applicant to address the staff positions in ISG-04, Section 3, for this interface. Also, it is not clear if it is possible to bypass or lockout any safety functions from the non-safety IFPD via the ESCM. Identify and describe the various types of commands that ESCM could send to the Engineered Safety Features - Component Control System (ESF-CCS) Loop Controller (LC). The staff requests applicant to clarify, and update the FSAR with this information.

Response

Section C.5.3 of technical report, APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System,” will be wholly revised to address compliance of the interface between the engineered safety features-component control system (ESF-CCS) soft control module (ESCM) and the information flat panel display (IFPD) to the guidance in DI&C ISG-04, Section 3, as shown in the attachment associated with this response.

The ESCM does not provide any manual bypass function or lockout function for safety components or safety systems.

The signal types sent from the ESCM to the ESF-CCS loop controller (LC) are as follows:

- Discrete control signal(e.g., on/off, start/stop)
- Modulation control signal(e.g., level control, flow control)

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

Section C.5.3 of technical report APR1400-Z-J-NR-14001-NP, Rev. 0, "Safety I&C System" will be updated as indicated in the attachment associated with this response.

TS

Replace with "A" on pages 8~21

TS

TS

TS

TS

TS

"A"

(1) Compliance to DI&C-ISG-04, Section 3.1, Position 1

DI&C-ISG-04, Section 3.1, Position 1 states:

"Nonsafety stations receiving information from one or more safety divisions:

All communications with safety-related equipment should conform to the guidelines for interdivisional communications."

ESCM and IFPD Compliance: TS

(2) Compliance to DI&C-ISG-04, Section 3.1, Position 2

DI&C-ISG-04, Section 3.1, Position 2 states:

"Safety-related stations receiving information from other divisions (safety or nonsafety):

All communications with equipment outside the station's own safety division, whether that equipment is safety-related or not, should conform to the guidelines for interdivisional communications. Note that the guidelines for interdivisional communications refer to provisions relating to the nature and limitations concerning such communications, as well as guidelines relating to the communications process itself."

ESCM and IFPD Compliance: TS

"A"

(3) Compliance to DI&C-ISG-04, Section 3.1, Position 3

DI&C-ISG-04, Section 3.1, Position 3 states:

"Nonsafety stations controlling the operation of safety-related equipment:

Nonsafety stations may control (see note above) the operation of safety-related equipment, provided the following restrictions are enforced:

- The nonsafety station should access safety-related plant equipment only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules.

- A nonsafety station should not affect the operation of safety-related equipment when the safety-related equipment is performing its safety function. This provision should be implemented within the safety-related system, and must be unaffected by any operation, malfunction, design error, software error, or communication error in the nonsafety equipment. In addition:

  - The nonsafety station should be able to bypass a safety function only when the affected division has itself determined that such action would be acceptable.

  - The nonsafety station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)

  - The nonsafety station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable."

ESCM and IFPD Compliance: **TS**

"A"

TS

Figure C.5-2 Control Procedure on ESCM

"A"

TS

(4) Compliance to DI&C-ISG-04, Section 3.1, Position 4

DI&C-ISG-04, Section 3.1, Position 4 states:

"Safety-related stations controlling the operation of equipment in other safety-related divisions: Safety-related stations controlling (see note above) the operation of equipment in other divisions are subject to constraints similar to those described above for nonsafety stations that control the operation of safety-related equipment.

- A control station should access safety-related plant equipment outside its own division only by way of a priority module associated with that equipment. Priority modules should be designed and applied as described in the guidance on priority modules."

- A station must not influence the operation of safety-related equipment outside its own division when that equipment is performing its safety function. This provision should be implemented within the affected (target) safety-related system, and should be unaffected by any operation, malfunction, design error, software error, or communication error outside the division of which those controls are a member. In addition:

  - The extra-divisional (that is, "outside the division") control station should be able to bypass a safety function only when the affected division itself determined that such action would be acceptable.

  - The extra-divisional station should not be able to suppress any safety function. (If the safety system itself determines that termination of a safety command is warranted as a result of the safety function having been achieved, and if the applicant demonstrates that the safety system has all information and logic needed to make such a determination, then the safety command may be reset from a source outside the safety division. If operator judgment is needed to establish the acceptability of resetting the safety command, then reset from outside the safety division is not acceptable because there would be no protection from inappropriate or accidental reset.)

  - The extra-divisional station should not be able to bring a safety function out of bypass condition unless the affected division has itself determined that such action would be acceptable."

ESCM and IFPD Compliance:

TS

"A"

(5) Compliance to DI&C-ISG-04, Section 3.1, Position 5

DI&C-ISG-04, Section 3.1, Position 5 states:

"Malfunctions and Spurious Actuations:

The result of malfunctions of control system resources (e.g., workstations, application servers, protection/control processors) shared between systems must be consistent with the assumptions made in the safety analysis of the plant. Design and review criteria for complying with these requirements, as set forth in 10 C.F.R. § 50.34 and 50.59, include but are not limited to the following:

- Control processors that are assumed to malfunction independently in the safety analysis should not be affected by failure of a multidivisional control and display station."

ESCM and IFPD Compliance:

TS

DI&C-ISG-04, Section 3.1, Position 5 states:

- "Control functions that are assumed to malfunction independently in the safety analysis should not be affected by failure of a single control processor."

ESCM and IFPD Compliance:

TS

"A"

DI&C-ISG-04, Section 3.1, Position 5 states:

- "Safety and control processors should be configured and functionally distributed so that a single processor malfunction or software error will not result in spurious actuations that are not enveloped in the plant design bases, accident analyses, ATWS provisions, or other provisions for abnormal conditions. This includes spurious actuation of more than one plant device or system as a result of processor malfunction or software error. The possibility and consequences of malfunction of multiple processors as a result of common software error must be addressed."

ESCM and IFPD Compliance:

TS

DI&C-ISG-04, Section 3.1, Position 5 states:

- "No single control action (for example, mouse click or screen touch) should generate commands to plant equipment. Two positive operator actions should be required to generate a command. For example: When the operator requests any safety function or other important function, the system should respond "do you want to proceed?" The operator should then be required to respond "Yes" or "No" to cause the system to execute the function. Other question-and-confirm strategies may be used in place of the one described in the example. The second operation as described here is to provide protection from spurious actuations, not protection from operator error. Protection from operator error may involve similar but more restrictive provisions, as addressed in guidance related to Human Factors."

ESCM and IFPD Compliance:

TS

"A"

TS

Figure C.5-3 Operating Procedure for the Soft Control using the IFPD and ESCM

"A"

DI&C-ISG-04, Section 3.1, Position 5 states:

- "Each control processor or its associated communication processor should detect and block commands that do not pass the communication error checks."

ESCM and IFPD Compliance: **TS**

DI&C-ISG-04, Section 3.1, Position 5 states:

- "Multidivisional control and display stations should be qualified to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and all other design basis conditions applicable to safety-related equipment at the same plant location. This qualification need not demonstrate complete functionality during or after the application of the design basis condition unless the station is safety-related. Stations which are not safety- related should be shown to produce no spurious actuations and to have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during the condition and afterwards. If spurious or abnormal actuations or stoppages are possible as a result of a design basis condition, then the plant safety analyses must envelope those spurious and abnormal actuations and stoppages. Qualification should be supported by testing rather than by analysis alone. D3 considerations may warrant the inclusion of additional qualification criteria or measures in addition to those described herein."

TS

ESCM and IFPD Compliance:

"A"

TS

DI&C-ISG-04, Section 3.1, Position 5 states:

- "Loss of power, power surges, power interruption, and any other credible event to any operator workstation or controller should not result in spurious actuation or stoppage of any plant device or system unless that spurious actuation or stoppage is enveloped in the plant safety analyses."

ESCM and IFPD Compliance:

TS

DI&C-ISG-04, Section 3.1, Position 5 states:

- "The design should have provision for an "operator workstation disable" switch to be activated upon abandonment of the main control room, to preclude spurious actuations that might otherwise occur as a result of the condition causing the abandonment (such as control room fire or flooding). The means of disabling control room operator stations should be immune to short-circuits, environmental conditions in the control room, etc. that might restore functionality to the control room operator stations and result in spurious actuations."

ESCM and IFPD Compliance:

TS

"A"

TS

DI&C-ISG-04, Section 3.1, Position 5 states:

- "Failure or malfunction of any operator workstation must not result in a plant condition (including simultaneous conditions) that is not enveloped in the plant design bases, accident analyses, and anticipated transients without scram (ATWS) provisions, or in other unanticipated abnormal plant conditions."

ESCM and IFPD Compliance:

TS

"A"

TS

6) Compliance to DI&C-ISG-04, Section 3.2: Human Factors Considerations

DI&C-ISG-04, Section 3.2 states:

"Safety-related plant equipment should have safety-related controls and displays:

- as required by IEEE 603
- as recommended in Regulatory Guide 1.97
- as referenced in:
  - plant safety or transient analyses
  - emergency or normal operation procedures
  - D3 or ATWS analyses
  - other design basis analyses
- as suggested in the plant control and display "minimum inventory" interim staff guidelines

For any safety-related equipment not having safety-related controls and displays, an applicant should

"A"

demonstrate that safety-related controls and displays are not needed in consideration of the above criteria or of any other considerations or requirements.

Safety-related controls and displays may be provided via operator workstations, or they may be provided via hardwired devices such as switches, relays, indicators, and analog signal processing circuits. In either case, the safety-related controls and indications must consist of safety-related devices with safety-related software and must be dedicated to specific safety divisions.

Under some circumstances as described below, it may be acceptable for the plant operator to use nonsafety controls and displays in lieu of safety-related controls and displays in the performance of safety functions. However, it must be possible for the operator to perform all safety functions using safety-related controls and displays and without the need for any nonsafety equipment.

IEEE 603-1991, Section 5.6.3.1, specifies that equipment "… that is used for both safety and nonsafety functions shall be classified as part of the safety systems…" Therefore equipment that is not classified as part of a safety system must not be credited for performing safety functions. Nevertheless, non-safety multidivisional control and display stations may be used to perform safety functions. The control and monitoring of functions credited with the protection of the plant in the plant safety analyses must be capable of being performed using only safety-related resources. Non-safety multidivisional control and display stations may supplement the safety-related control and display equipment that is credited in the plant safety analyses.

When using nonsafety-related multidivisional control and display stations to perform safety-related actions, plant operators are expected to confirm that appropriate responses have been achieved for the actions taken. In accordance with the guidance in section 3.1, Item 5 of this ISG, nonsafety multidivisional control and display stations should be designed to withstand the effects of adverse environments, seismic conditions, EMI/RFI, power surges, and other plant design-basis conditions, for the purpose of surviving in the environment in which the multidivisional control and display station is being used to execute safety functions. In such an environment, a nonsafety control and display station should not produce malfunctions and spurious actuations. However, these nonsafety-related multidivisional control and display stations are not fully qualified safety-related equipment. Accordingly, whenever plant operators cannot confirm the appropriate response to the safety-related action taken by use of a nonsafety multidivisional control and display station, then it would be necessary to confirm the desired response from the safety-related controls and displays. If the operator observes that operation of the nonsafety multidivisional control and display station has been compromised, or the plant is not responding as expected, then safety-related control actions must be taken from safety-related control and display stations.

Also, an applicant would need to demonstrate that Human Factors considerations, including consideration of operator response time and situation awareness, are consistent with the system design bases, operating procedures, and accident analyses and are both reasonable and adequate given the possibility of erroneous or inaccurate indications from the nonsafety equipment. In the context of the failure of nonsafety control stations, situational awareness involves the operator's ability to identify erroneous operation of equipment or indications, and take the appropriate actions.

This aspect of the application should be reviewed and found acceptable by appropriate Human Factors, Operations, and plant system experts within the NRC. There are many other Human Factors considerations applicable to the design of operator workstations, whether multidivisional or not. Such

"A"

considerations are not addressed here."

ESCM and IFPD Compliance:

TS

"A"

TS

(7) Compliance to DI&C-ISG-04, Section 3.3

DI&C-ISG-04, Section 3.3 states:

"D3 considerations may influence the number and disposition of operator workstations and possibly of backup controls and indications that may or may not be safety-related. The guidance provided herein is not dependent upon such details.

D3 considerations may also impose qualification or other measures or guidelines upon equipment addressed in this ISG. The guidance presented herein does not include such considerations.
Consideration of other aspects of D3 is outside the scope of this guidance. Additional guidance concerning D3 considerations is provided separately."

TS

ESCM and IFPD Compliance: