
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.: 348-8279

SRP Section: 07.09 - Data Communication Systems

Application Section:

Date of RAI Issue: 12/24/2015

Question No. 07.09-11

Describe the measures used to prevent data going from non-safety systems to safety-related systems.

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." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

Section 4.1.1.4 of Technical Report APR1400-Z-J-NR-14001-P states "The QIAS-P also transmits the sensor signals and their calculated variables to the IPS and QIAS-N through the MTP and ITP, respectively. In the case of the IPS, this data communication is a uni-directional protocol from the MTP. In the case of the ITP, the SDL data communication is used to transmit data to the QIAS-N." The first paragraph of section 4.2.3.4 of the same report also discusses the MTP, its capabilities, displays, interfaces, and data transmission details.

Section 4.3.1.5 of the same report states "This MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCN-I gateway." In addition, Figure 4-22 of the technical report shows that the MTP to IPS link is a one way fiber optic cable. Section C.4.2 of the report contains the following, "... (no receiving connection) ..."

Describe the uni-directional interface between MTP and IPS and clarify what is meant by "no receiving connection," since a typical Ethernet connector has 4 pairs of wires. It is not clear to staff if a standard Ethernet cable is used or a modified cable/connectors with TX pairs/pins on the non-safety end removed and RX pairs/pins on the safety end removed.

Response

The uni-directional media converter is used for one-way data transmission across a single fiber optic cable from the maintenance and test panel (MTP) to the distributed control system (DCS) gateway server in the information processing system (IPS). Standard duplex fiber connectors are utilized with their full-duplex function disabled. This uni-directional media converter provides the Fast Ethernet RJ-45 ports, which are switch-selectable to allow a choice of forced full duplex or auto-negotiated twist-pair connections with other network devices. Even if full-duplex links are established at the unshielded twist pair (UTP) interface, they never actually transport full-duplex traffic. The transmit (Tx) port of the transceiver converter is connected to the receive (Rx) port of the receiver converter using a single fiber strand; the RJ-45 port of each converter is then connected and configured with its associated host for secure, one-way data transmission.

The MTP processor has a full-duplex link to the RJ-45 port in the transceiver converter. The transceiver converter receives data from the MTP processor and forwards one-way data, and provides a fiber optic path with transported and forwarded one-way data to the receiver converter. This receiver converter forwards one-way data to the DCS gateway server.

The reference plant, Shin-Kori 3&4, uses CFT-206XD and CFT-206XDR of Canary Communication for the receiver converter and transceiver converter to implement uni-directional communication from the MTP to the DCS gateway server.

The following changes will be made to APR1400-Z-J-NR-14001-P, Rev.0 Safety I&C System, Section 4.3.1.5, "Maintenance and Test Panel" to describe the uni-directional interface between the MTP and the IPS:

The MTP provides the isolated interface to the non-safety DCN-I network via the gateway. This MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCS gateway server. The uni-directional media converter is used for one-way data transmission across a single fiber optic cable from the MTP to the DCS gateway server in the IPS. Standard duplex fiber connectors are utilized with their full-duplex function disabled. This uni-directional media converter provides the Fast Ethernet RJ-45 ports which are switch-selectable to allow a choice of forced full duplex or auto-negotiated twist-pair connections with other network devices. The MTP processor has a full-duplex link to the RJ-45 port in the transceiver converter. The transceiver converter receives data from the MTP processor and forwards one-way data, and provides a fiber optic path with transported and forwarded one-way data to the receiver converter. This receiver converter forwards one-way data to the DCS gateway server.

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

APR1400-Z-J-NR-14001-NP, Rev.0, "Safety I&C System", Section 4.3.1.5 will be revised as indicated in the attachment associated with this response.

- LPD margin
- CPCS calculated values
- CPCS trouble
- Processor failure
- CPCS in test

4.3.1.4 Operator Module Function

The OM, which is shared with the PPS and ESF-CCS, is provided to monitor certain inputs and calculated results and status for operator. The OM has a dedicated area of display for alarm conditions. In the OM, the specific activities such as monitoring of values or changing addressable constants are performed.

4.3.1.5 Maintenance and Test Panel

The MTP provides the capability to modify the CPCS addressable constants, and displays information such as system parameters, various system status, and test results. The MTP also provides an interface to initiate and support testing. It is located in the MTC and is shared with other safety systems within the division. ~~The MTP provides the isolated interface to the non-safety DCN-I via a gateway. This MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCN-I gateway.~~

Manual switches and/or touch panels are used to enable the CPCS control functions such as addressable constant changes, test initiation, etc.

4.3.1.6 Interface and Test Processor

The ITP is located in the same cabinet as the MTP, separate from the CPC and CEA calculator (CEAC) cabinet. Data are shared with other safety systems in the same division using the SDN (e.g. the ITP communicates with the CPCS via the SDN). The ITP also provides the interfaces between the CPCS and QIAS-N by transmitting safety-related data to the QIAS-N via the SDL.

The MTP provides the isolated interface to the non-safety DCN-I network via the gateway. This MTP interface is a unidirectional point-to-point Ethernet datalink from the MTP to the DCS gateway server. The uni-directional media converter is used for one-way data transmission across a single fiber optic cable from the MTP to the DCS gateway server in the IPS. Standard duplex fiber connectors are utilized with their full-duplex function disabled. This uni-directional media converter provides the Fast Ethernet RJ-45 ports which are switch-selectable to allow a choice of forced full duplex or auto-negotiated twist-pair connections with other network devices. The MTP processor has a full-duplex link to the RJ-45 port in the transceiver converter. The transceiver converter receives data from the MTP processor and forwards one-way data, and provides a fiber optic path with transported and forwarded one-way data to the receiver converter. This receiver converter forwards one-way data to the DCS gateway server.

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.: 348-8279

SRP Section: 07.09 – Data Communication Systems

Application Section:

Date of RAI Issue: 12/24/2015

Question No. 07.09-12

Demonstrate how the effects of data storms are addressed for this connectivity in order to provide reliable data transmissions to support safety system functions.

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." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6. 10 CFR 50, Appendix A, Criterion 13, states instrumentation shall be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems.

To comply with DI&C-ISG-04, Section 1, Position 4, in section C.5.1.5(4) of technical report APR1400-Z-J-NR-14001-P, the applicant stated "The EP [Ethernet Processor] checks the integrity of the received data by ..." This section goes on to discuss actions taken "...over a certain number of cycles,..." [Question 1] Since the ESCM is connected to 4 IFPDs, the applicant is requested to identify the "certain number of cycles" and the how much erroneous data the Ethernet Communication Module can handle.

To comply with DI&C-ISG-04, Section 1, Position 19 (section C.5.1.5(19), the applicant stated "...even if incorrect data are broadcasted or a broadcast data storm occurs on a network causing an excess of data traffic..." [Question 2] The staff also request the applicant to demonstrate how the effects of data storms are addressed for this connectivity in order to

provide reliable data transmissions to support important to safety functions as required by GDC 13.

Response

TS

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

APR1400-Z-J-NR-14001-NP, Rev.0, "Safety I&C System", Section C.5.1.5 will be revised, as indicated in the attachment associated with this response.

Page intentionally blank

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.: 348-8279

SRP Section: 07.09 – Data Communication Systems

Application Section:

Date of RAI Issue: 12/24/2015

Question No. 07.09-13

Discuss how the Information Flat Panel Display (IFPD) communications to ESF-CCS Soft Control Module (ESCM) support or enhance the performance of the safety functions.

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.” 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, Section C.5.1.5(3), states conformance to DI&C ISG-04, Section 1, Position 3, and defines the purpose of the IFPD to ESCM interdivisional communication. DI&C ISG-04, Section 1, Position 3 states, in part, “A safety channel should not receive any communication from outside its own safety division unless that communication supports or enhances the performance of the safety function.” It is not clear to the staff how the IFPD interdivisional communication as described in the technical report meets DI&C ISG-04, Section 1, Position 3. Specifically, how do the described IFPD interdivisional communications support or enhance the performance of the safety functions? The staff requests the applicant to address this portion of DI&C ISG-04 and update the FSAR accordingly.

Response

TS



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

APR1400-Z-J-NR-14001-NP, Rev.0, "Safety I&C System", Section C.5.1.5 will be revised, as indicated in the attachment associated with this response.

9 REFERENCES

1. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," November 2014
2. APR1400-Z-A-NR-14019-P, "CCF Coping Analysis", November 2014
3. APR1400-E-J-NR-14001-P, "Component Interface Module," November 2014
4. DI&C-ISG-04, Rev.1, "Highly Integrated Control Rooms – Communications Issues," 2009
5. APR1400-K-Q-TR-11005-N, "KHNP Quality Assurance Program Description (QAPD) for the APR1400 Design Certification"
6. APR1400 DC Quality Assurance Manual (QAM)
7. APR1400-Z-J-NR-14004-P, "Uncertainty Methodology and Application for Instrumentation," November 2014
8. APR1400-Z-J-NR-14005-P, "Setpoint Methodology for Plant Protection System," November 2014
9. APR1400-F-C-NR-14001-P, "CPC Setpoint Analysis Methodology for APR1400," July 2014.
10. APR1400-Z-J-NR-14003-P, Rev. 0, "Software Program Manual", November 2014
11. Design Control Document for the APR1400
12. WCAP-16097-P-A, "Common Qualified Platform Topical Report", Rev. 3, February 2013
13. APR1400-Z-J-NR-14013-P, "Response Time Analysis of Safety I&C System," November 2014
14. APR1400-Z-J-NR-14012-P, "Control System CCF Analysis," November 2014
15. APR1400-F-C-NR-14003-P, "Functional Design Requirements for a Core Protection Calculator System for APR1400," August 2014
16. APR1400-E-I-NR-14012-P, "Style Guide," December 2014
17. APR1400-A-J-NR-14004-P (WCAP-17922-P, "Common Q Platform Supplemental Information in Support of the APR1400 Design Certification," Rev. 0, August 2014
18. APR1400-A-J-NR-14003-P (WCAP-17926-P), "APR1400 Disposition of Common Q Topical Report NRC Generic Open Item and Plant Specific Action Items," Rev.0, October 2014
19. APR1400-E-I-NR-14011-P, "Basic Human-System Interface," December 2014.

Page intentionally blank

Page intentionally blank

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.: 348-8279

SRP Section: 07.09 – Data Communication Systems

Application Section:

Date of RAI Issue: 12/24/2015

Question No. 07.09-14

Discuss how response times will be verified for IFPD to ESCM interdivisional communication.

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." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

To comply with DI&C-ISG-04, Section 1, Position 20, for IFPD to ESCM interdivisional communication, in APR1400-Z-J-NR-14001-P, section C.5.1.5(20), the applicant describes how the maximum delay time is calculated, including the time components involved in the calculation. Discuss the testing and analysis that will be performed to demonstrate how these response times will be verified for IFPD to ESCM interdivisional communication; particularly for those manual actions that are credited to implement a safety function.

Response

TS

TS

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

APR1400-Z-J-NR-14001-NP, Rev.0, "Safety I&C System", Section C.5.1.5 will be revised, as indicated in the attachment 1 associated with this response.

APR1400-E-J-NR-14011-NP, Rev.0 "Basic Human System Interface," Sections 4.10.3 and 5 will be revised, as indicated in the attachment 2 associated with this response.

9 REFERENCES

1. APR1400-Z-J-NR-14002-P, "Diversity and Defense-in-Depth," November 2014
2. APR1400-Z-A-NR-14019-P, "CCF Coping Analysis", November 2014
3. APR1400-E-J-NR-14001-P, "Component Interface Module," November 2014
4. DI&C-ISG-04, Rev.1, "Highly Integrated Control Rooms – Communications Issues," 2009
5. APR1400-K-Q-TR-11005-N, "KHNP Quality Assurance Program Description (QAPD) for the APR1400 Design Certification"
6. APR1400 DC Quality Assurance Manual (QAM)
7. APR1400-Z-J-NR-14004-P, "Uncertainty Methodology and Application for Instrumentation," November 2014
8. APR1400-Z-J-NR-14005-P, "Setpoint Methodology for Plant Protection System," November 2014
9. APR1400-F-C-NR-14001-P, "CPC Setpoint Analysis Methodology for APR1400," July 2014.
10. APR1400-Z-J-NR-14003-P, Rev. 0, "Software Program Manual", November 2014
11. Design Control Document for the APR1400
12. WCAP-16097-P-A, "Common Qualified Platform Topical Report", Rev. 3, February 2013
13. APR1400-Z-J-NR-14013-P, "Response Time Analysis of Safety I&C System," November 2014
14. APR1400-Z-J-NR-14012-P, "Control System CCF Analysis," November 2014
15. APR1400-F-C-NR-14003-P, "Functional Design Requirements for a Core Protection Calculator System for APR1400," August 2014
16. APR1400-E-I-NR-14012-P, "Style Guide," December 2014
17. APR1400-A-J-NR-14004-P (WCAP-17922-P, "Common Q Platform Supplemental Information in Support of the APR1400 Design Certification," Rev. 0, August 2014
18. APR1400-A-J-NR-14003-P (WCAP-17926-P), "APR1400 Disposition of Common Q Topical Report NRC Generic Open Item and Plant Specific Action Items," Rev.0, October 2014

19. APR1400-E-I-NR-14011-P, "Basic Human-System Interface," December 2014.

20. APR1400-E-I-NR-14007-P, "Human-System Interface Design Implementation Plan," December 2014.

21. APR1400-E-I-NR-14004-P, "Task Analysis Implementation Plan," December 2014.

Page intentionally blank

TS

4.11 Controls

TS

4.11.1 Soft Controls

TS

5. DEVELOPMENT PROCESS

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.: 348-8279

SRP Section: 07.09 – Data Communication Systems

Application Section:

Date of RAI Issue: 12/24/2015

Question No. 07.09-15

Address DI&C-ISG-04, "Highly Integrated Control Room - Communication," Rev. 1, Positions 12, 13, 14, 15 and 17 for the IFPD to ESCM interface.

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." Digital I&C Interim Staff Guidance (DI&C-ISG)-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

For DI&C-ISG-04, Section 1, Positions 12, 13, 14, 15, and 17, in technical report APR1400-Z-JNR- 14001-P, section C.5.1.5, the applicant stated that DI&C-ISG-04 position is not applicable to the communication between IFPD and the ESCM. The staff disagrees. DI&C-ISG-04 states "vital communication as used are communications that are needed to support a safety function," and based on the discussions in Technical Report APR1400-Z-J-NR-14001-P, the IFPD and ESCM connectivity supports a safety function (e.g., steam generator tube rupture manual actions). Address DI&C-ISG-04 Positions 12, 13, 14, 15, and 17 for the IFPD to ESCM interface.

Response

KHNP had previously addressed the DI&C-ISG-04, Positions 12 for the IFPD to ESCM interface in the response to RAI 45-7883, Question No.07.09-7.

TS



TS

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

APR1400-Z-J-NR-14001-NP, Rev.0, "Safety I&C System", Section C.5.1.5 will be revised, as indicated in the attachment associated with this response.

Page intentionally blank

Page intentionally blank