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 System**
Application Section:	**07.09**
Date of RAI Issue:	**06/23/2015**

Question No. 07.09-2

List all safety system to safety system interfaces and their connection types and all safety system to non-safety system interfaces and their connection types.

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 regulations. Section 4.2.4 of the technical report, "System Interfaces," discusses Plant Protection System (PPS) cabinet interfaces. The applicant provided description for some of the system interfaces and their type (e.g. Auxiliary Process Cabinet - Safety connects to PPS cabinets via hardwire cables, Core Protection Calculator System connects to PPS cabinets via hardwire cables, and PPS sends initiation signals to Engineered Safety Features-Component Control System Group Controllers through fiber optic Serial Data Link). It is not clear how other safety systems and non-safety systems are connected. List all safety to safety system interfaces and their interface type, and to list all safety to non-safety system interfaces and their interface type, and provide information on how these interfaces meet the requirements of IEEE Std. 603-1991, Clause 5.6, or provide a reference to sections of the

FSAR or technical reports where this information resides. Update the FSAR with the requested information.

Response

Conformance to IEEE Std. 603 and RG1.75 independence requirements is described and provided in Section 7.1.2.42 of DCD Tier 2 and Appendix A of Safety I&C System Technical Report.

The system interfaces for the PPS, and the connection types, are described in Section 4.2.4 of the Safety I&C System Technical Report. The connection types that are not clearly described in Section 4.2.4 of the Safety I&C System Technical Report will be revised to clarify what type of connection is used.

The system interfaces for the core protection calculator system (CPCS), and the connection types, are described in Section 4.3.4 of the Safety I&C System Technical Report. The connection types that are not clearly described in Section 4.3.4 of the Safety I&C System Technical Report will be revised to clarify what type of connection is used.

The system interfaces for the ESF-CCS and the connection types are described in Section 4.4.4 of the Safety I&C System Technical Report.

The system interfaces for the qualified indication and alarm system-P(QIAS-P) and the connections types are described in Section 4.5.3 of the Safety I&C System Technical Report. The connections types that are not clearly described will be added to Section 4.5.3 of the Safety I&C System Technical Report.

The interfaces for the reactor trip switchgear system (RTSS), and the connection types, are described in Section 4.8.2 of the Safety I&C System Technical Report. The connection types that are not clearly described in Section 4.8 of the Safety I&C System Technical Report will be revised to clarify what type of connection is used.

In summary, Sections 4.2.4, 4.3.4, 4.5.3, and 4.8.2 of the Safety I&C System Technical Report will be revised to include the corresponding interface types as indicated on the attached mark-up.

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

Sections 4.2.4, 4.3.4, 4.5.3 and 4.8.2 of the Safety I&C System Technical Report(APR1400-Z-J-NR-14001-NP) will be revised as indicated on the attached mark-up.

4.2.4 System Interfaces

The PPS cabinet interfaces with the following equipment:

- Auxiliary process cabinet - safety
- Core protection calculator system
- Ex-core neutron flux monitoring system
- Reactor trip switchgear system
- Engineered safety features - component control system
- Information processing system
- Qualified indication and alarm system – P
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Control panel multiplexer
- DRCS remote I/O cabinet
- Operator module

The APC-S provides four channels, physically and electrically separate signals for each safety-related plant parameter to the PPS cabinet via hardwired cables. There are no programmable digital devices in the APC-S.

The CPCS provides four channels, physically and electrically separate DNBR and LPD states to the PPS cabinet via hardwired cables.

via hardwired cables

The PPS receives the log power, calibrated linear power, logarithmic power operating bypass permissive, and ex-core trouble annunciation for the power trip test interlock from the ENFMS safety channel via hardwired cables. These signals are not generated by a programmable digital device.

The RTSS receives a reactor trip signal from the initiation circuit in the PPS. The RTSS interrupts power to the DRCS to allow gravity insertion of the CEAs upon receipt of a trip signal which is generated by either the RPS section of the PPS or one of the two sets of manual reactor trip switch on the MCR SC.

The PPS sends the ESFAS initiation signals to the ESF-CCS GCs in all ESF-CCS divisions through the fiber optic SDL.

The PPS sends the monitored plant parameters to the QIAS-P via the SDN.

The PPS provides status alarms to the IPS and QIAS-N via the MTP and ITP respectively.

Each PPS division is powered from a vital bus power supply system (VBPSS) inverter. Each VBPSS division provides a non-interruptible battery backed 120 Vac, single phase, ungrounded power source for

The description of the interfaces from the MTP to the IPS and from the ITP to the QIAS-N is provided in Section 4.6.

essential instrumentation and plant control. The RSR provides the capability to control selected equipment and monitor selected plant variables necessary to achieve an orderly plant safe shutdown when the MCR is uninhabitable.

The conventional switch signals for operating bypass and setpoint reset in the MCR and RSR are sent to the BP from the CPMs that acquire these signals and send them via the SDL.

The DRCS remote I/O cabinet receives a CWP signal from ~~the PPS~~ division D ~~only~~. A CWP logic signal is transmitted to the DRCS when a 2-out-of-4 coincidence condition occurs on either a CPC initiated CWP or PPS high pressurizer pressure pre-trip signal. This signal is treated as an associated circuit and isolated at the DRCS remote I/O cabinet.

The OM in each safety division is shared by the PPS, CPCS and ESF-CCS. The OMs are located on the MCR SC and provide the PPS status (trip/pre-trip/bypass), initiation circuit status, TCB phase current status and operating bypass information to the operator. Each division has its own dedicated OM, and it is physically separated and electrical isolated from other OMs in redundant divisions.

The PPS cabinets are located in divisionalized I&C equipment rooms. Equipment and circuits of the PPS require four division physical separation and electrical isolation meeting the requirements of IEEE Std. 384 as endorsed by RG 1.75.

Communication cablings between redundant PPS divisions are routed via fiber optic cables. The fiber optic cables satisfy the isolation and independence requirements.

The ESFAS initiation outputs from each PPS division to the four divisions of ESF-CCS cabinets are routed and isolated using fiber optic cables.

TS

4.3.4 System Interfaces

The CPCS interface with other systems is shown in Figure 4-10. The CPCS cabinet housing the CPC rack and CEACs rack interfaces with the following equipment:

- Auxiliary protective cabinet - safety
- Ex-core neutron flux monitoring system
- Reactor coolant pump shaft speed sensing system
- Reed switch position transmitter
- Plant protection system
- Information processing system
- Qualified indication and alarm system - P
- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Field sensors

The pressurizer pressure signals are used in the DNBR and the LPD calculations.

4.3.4.1 Auxiliary Process Cabinet-Safety

The CPC processor receives the pressurizer pressure signals from the APC-S ~~used for DNBR and LPD calculation.~~

via hardwired cable

4.3.4.2 Ex-core Neutron Flux Monitoring System

The CPC processor receives the linear sub-channel power signals from the ENFMS. These are used for the reactor power calculation and power distribution calculation.

4.3.4.3 Reactor Coolant Pump Shaft Speed Sensing System

via hardwired cable

The CPC processor receives RCP speed signal from reactor coolant pump shaft speed sensing system (RCPSSSS) ~~for the flow rate calculation.~~

The RCP speed signal is used in the flow rate calculation.

4.3.4.4 Reed Switch Position Transmitter

The CEA position is provided by two RSPT inputs on each CEA. All RSPT inputs are converted to a digital value in the CPP PM and are input to all four CPC/CEAC channels over fiber optic isolated SDL data links. The CPPs in channel A(D) receive 23 CEA positions from RSPT1(2), and the CPPs in channel B(C) receive 70 CEA positions from RSPT1(2).

The RSPTs are hardwired to the CPPs.

4.3.4.5 Plant Protection System

The CPCS system provides the following hardwired signals to the PPS.

- Low DNBR trip/pre-trip
- High LPD trip/pre-trip
- CEA withdrawal prohibit

The description of the interface from the MTP to the IPS is provided in Section 4.6.

4.3.4.6 Information Processing System

The CPC and auxiliary CPC processor transmit CPC data to the IPS via the MTP. The CEAC also transmits CEAC data to the IPS via the MTP.

4.3.4.7 Qualified Indication and Alarm System-P

The CPCS transmits CEA position data to the QIAS-P via the SDN.

4.3.4.8 Qualified Indication and Alarm System-Non safety

The CPCS transmits pre-selected data to the QIAS-N via the ITP.

4.3.4.9 Field Sensors

The CPCS receives the following hardwired field sensor signals.

- Hot leg temperature loop 1
- Hot leg temperature loop 2
- Cold leg temperature loop 1
- Cold leg temperature loop 2

The description of the interface from the ITP to the QIAS-N is provided in Section 4.6.

- ITP (then to QIAS-N),
- QIAS-P display

~~The HJTC heater power is hardwired directly to the HJTCs.~~

Table 4-2 provides a summary of the I/O signals for the QIAS-P.

The signal interfaces between the QIAS-P cabinet and process instrumentation, ICIS, HJTC, and the APC-S are done by hardwired cables.

The signal interface between the QIAS-P cabinet and the DIS, which is a non-safety system, is done by hardwired cables and isolators.

The communications between the QIAS-P cabinet and the safety systems such as the PPS, CPCS, MTP, ITP, the QIAS-P display, and the ESF-CCS are done via SDN.

The communications between the QIAS-P cabinet and the IPS and QIAS-N, which are non-safety systems, are done through the MTP and the ITP, respectively.

4.8 Reactor Trip Switchgear System

4.8.1 Functions

TS

4.8.2 Design Features

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.:	**45-7883**
SRP Section:	**07.09 – Data Communication System**
Application Section:	**07.09**
Date of RAI Issue:	**06/23/2015**

Question No. 07.09-6

Provide summary of how communication independence requirements are met between redundant portions of the safety system.

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.

APR1400 FSAR, Tier 2, Section 7.2.2.3, "Independence" states, “Independence between redundant portions of the safety system. The routing of Class 1E and associated cabling and sensing lines from sensors meets the guidance of NRC RG 1.75 (Reference 7) and NRC RG 1.151 (Reference 8). The cablings for the four safety divisions are routed separately. The PPS divisions receive ac power from the vital bus power supply system. The PPS does not share the power between divisions.” This section of the FSAR does not discuss how data communication independence between redundant portions of the Plant Protection System (PPS) is achieved to meet the requirements of IEEE Std. 603-1991, Clause 5.6.1. Provide either a summary of how communications independence requirements are met or reference the particular section of the Safety I&C System Technical Report where data communication independence between redundant portions of the safety system is being analyzed.

Response

Section 4.6 of the Safety I&C System Technical Report describes the data communication system, and subsection 4.6.2.1 describes the interdivisional serial data links used for data communication between safety portions of the plant protection system (PPS) in particular. This subsection states that both the bistable processor (BP) and local coincidence logic (LCL) processor include a communication processor as shown in Figure 4-19 of the Safety I&C System Technical Report. The data flow between redundant PPS divisions is buffered at the outgoing side of the communication processor of the BP and at the incoming side of the communication processor of the LCL processor to ensure independence of the redundant safety divisions. One way communication over fiber optic cable is used to ensure communication independence and electrical isolation between redundant portions of the safety system.

Further discussion regarding compliance of interdivisional communication between redundant portions of the safety system is provided in C.5.1 of the Safety I&C System Technical Report.

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 Reports.

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 Issue: **06/23/2015**

Question No. 07.09-7

Clarify what is meant by "any errors", and describe potential data communication faults and mitigating measures.

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.

DI&C ISG-04, Section 1, Position 12, states, in part, "Communication faults should not adversely affect the performance of required safety functions in any way...", and lists examples of credible communication faults. APR1400 FSAR, Tier 2, Section 7.1, Page 7.1-3, states, in part, “Data communications within or between I&C systems are designed to provide reasonable assurance that any error in data communication will not cause inadvertent actuations or prevent the safety functions from being performed.” Clarify whether the applicant really meant "any" errors as this goal is typically difficult to achieve except on simple communication schemes. Also, per DI&C ISG-04, Section 1, Position 12, describe the potential data communication faults between IFPD and ESCM and the mitigating measures for each fault.

Response

The use of “any error” in APR1400 DCD, Tier 2, Section 7.1 means the malfunctions that lead to detectable and undetectable failures of data communications. APR1400 FSAR, Tier 2, Section 7.1, Page 7.1-3, sub-part, “Data Communication” will be updated as follows: “Data communications within or between I&C systems is provided with the communication independence to ensure that there will be no adverse impact on the safety systems. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, a qualified serial data link, and Ethernet network. Communication independence is provided among safety divisions and between safety and non-safety data communication systems. The safety and non-safety data communication systems are diverse.”

TS

.

Impact on DCD

APR1400 DCD Tier 2, Section 7.1, Page 7.1-3 will be revised as indicated in Attachment 1.

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-Z-J-NR-14001-P/NP, Rev. 0, “Safety I&C System”, Subsection C.5.1.5 will be revised as indicated in Attachment 2.

Some I&C functions are not installed on a common PLC and DCS platform. These functions are implemented in independent systems to fulfill system design requirements. Non-standard systems include the diverse protection system (DPS), diverse indication system (DIS), NSSS integrity monitoring system (NIMS), radiation monitoring system (RMS), and seismic monitoring system (SMS).

Data Communications

~~Data communications within or between I&C systems are designed to provide reasonable assurance that any error in data communication will not cause inadvertent actuations or prevent the safety functions from being performed. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, and a network between qualified PLC and non-qualified DCS. The qualified PLC data communications network is independent and diverse from the non-qualified DCS data network.~~

Replace with "A" on the next page.

Human-System Interface

The APR1400 HSI is designed based on a compact workstation using the soft control and digital DCS. The compact workstation, which is based on HSI, provides a convenient operating environment to facilitate the display of plant status information to the operator so that operability is enhanced by using advanced display, alarm, and procedure systems. The HSI has sufficient diversity to demonstrate defense-in-depth protection against common-cause failure of the safety system.

7.1.1 Identification of Safety Systems and Non-Safety Systems

Safety and non-safety I&C systems, including supporting systems, are identified in the following subsections.

7.1.1.1 Plant Protection System

The PPS is a safety system that includes electrical, electronic, network, mechanical devices, and circuits and performs the following protective functions:

a. Reactor protection system (RPS)

"A"

Data communications within or between I&C systems is provided with the communication independence to ensure that there will be no adverse impact on the safety systems. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, a qualified serial data link, and Ethernet network. Communication independence is provided among safety divisions and between safety and non-safety data communication systems. The safety and non-safety data communication systems are diverse.

TS

TS

TS

TS

TS

Figure C.5-1 ESCM Interface Diagram

TS

TS

TS

TS

TS

Intentionally blank

Intentionally blank

Intentionally blank

Intentionally blank

TS

TS

TS