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.:	**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 – (Rev. 2)

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.

The detailed interface information between redundant portions of the safety system and between the safety and non-safety systems is provided as Tables 1 and 2. These tables (to be incorporated into the Safety I&C System technical report as Tables 4.1-1 and 4.1-2, respectively) also provide clarification of the as-built interface type such as hardwired connection, data link connection (SDL), data network connection (SDN), and Ethernet data link connection. The attached Table 3 (to be incorporated into the Safety I&C System technical report in response to RAI 45-8279 Question 07.09-9 Rev. 1 and is included for information) is provided as the list of interdivisional hardwired links in the ESF-CCS.

Table 1. Interface between redundant portions of the safety system

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
1	PPS BP	PPS LCL	Partial trip	SDL	4.2.2.1
2	PPS	ESF-CCS GC	ESFAS initiation	SDL	4.1.1.2, 4.2.3.2, 4.2.3.3, 4.2.4
3-1	ITP Division A	ITP Division B	CIV signals (74 signals)	SDL	4.5.2
3-2	ITP Division C	ITP Division B	CIV signals (10 signals)	SDL	4.5.2
3-3	ITP Division D	ITP Division B	CIV signals (9 signals)	SDL	4.5.2
3-4	ITP Division B	ITP Division A	CIV signals (69 signals)	SDL	4.5.2
3-5	ITP Division C	ITP Division A	CIV signals (10 signals)	SDL	4.5.2
3-6	ITP Division D	ITP Division A	CIV signals (9 signals)	SDL	4.5.2
4	CPP in CPCS	CPC/CEAC in CPCS	Digitized RSPT values	SDL	4.3.2.1

Note 1: The ESF-CCS in each division sends the CIV signals to the ITP of the same division via fiber optical data network connection (SDN).

Table 2. Interface between safety and non-safety system

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
1	PPS	DRCS Remote I/O Cabinet	CWP contact	Hardwired	4.2.4
2	DIS	QIAS-P	Transfer command, HJTC heater power control	Hardwired	Figure 4-17, Table 4-2
3	QIAS-P	DIS	CETs, HJTCs, control status	Hardwired	Figure 4-17, Table 4-2
4	P-CCS	ESF-CCS	Non-safety control signals for CVCS, steam generator blowdown system, condenser vacuum system, fuel handling area HVAC system, fire protection system, process sampling system, and class 1E 4.16kV system	Hardwired	4.4.4.12
5	DMA Switches	CIM	Actuation signals for ESF components	Hardwired	4.1.1.7
6	DPS	CIM	Component control signals	Hardwired	4.1.1.7
7	ITP	QIAS-N	PPS status alarm, CPC data, Type A,B,C variables, ICC-related variables,	SDL	3.3.2, 4.1.1.4, 4.2.2.1, 4.2.3.5, 4.3.1.6,

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
			operating ESF-CCS status for EOP, plant safe shutdown, cabinet trouble alarm, system in test		
8	MTP	DCS Gateway Server of IPS	PPS status alarm, CPC data, Type A,B,C variables, ICC-related calculation variables, control cabinet alarms, system in test	Ethernet Data Link	3.3.2, 4.3.1.5
9	IFPD (on each operator console)	ESCM (on each operator console)	Safety component selection information	Ethernet Data Link	4.1.2.7
10	PPS	TCS (turbine control system)	Turbine trip signal	Hardwired	4.2.1.1
11	ENFMS (ex-core neutron flux monitoring system)	NIMS (NSSS integrity monitoring system)	Sub-channel neutron flux signal	SDL	A.5.6

Some of the descriptions in Section 4.4.4.12, “Process-Component Control System” of the Safety I&C System technical report will be modified as indicated in the attachment. The detailed information on these signals is provided in Sections 4.9.1, 4.9.2, and 4.9.3 of the Control System CCF Analysis technical report and the related mark-up that was provided in the response to RAI 68-7892 Question 07.07-8 Rev.1 (refer to KHNP submittal MKD/NW-16-0986L dated September 20, 2016; ML16264A400).

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, 4.4.4.12, 4.5.3, and 4.8.2 of the Safety I&C System Technical Report will be revised as indicated on the attached mark-up.

communication via the serial data link (SDL, i.e., HSL) from safety systems to non-safety systems (i.e., QIAS-N) and buffering circuit using dual-ported memory are commonly used to prevent endangering the safety function. The other means from safety to non-safety data communication is via the plant computer datalink using the unidirectional protocol from the MTP.

- The DPS is diverse from the safety I&C system in aspects of trip mechanism, hardware and software.
- In addition to the DPS, the hardwired DMA switches and the DIS are provided on the MCR SC to cope with CCF of the safety I&C system.

The safety I&C system has the interface with redundant portions of the safety system and with non-safety system. Tables 4.1-1 and 4.1-2 provide the specific interface information.

4.1.1 Safety I&C Systems

4.1.1.1 Plant Protection System

Insert the tables on the next page.

The PPS consists of four redundant divisions that perform the necessary bistable, coincidence, initiation logic, maintenance and test function.

The PPS initiates reactor trip and system-level ESF actuation functions when a safety limit is exceeded by the plant conditions. To detect such conditions, the system utilizes measurements of the reactor core, reactor coolant system, main steam supply system, and containment building parameters.

Each PPS redundant division receives the process and discrete signals directly from field sensors or via the APC-S, ENFMS, and CPCS. The PPS provides the reactor trip signals to the RTSS using hardwired cables and ESFAS initiation signals to the ESF-CCS via fiber optic SDLs.

4.1.1.2 Engineered Safety Features - Component Control System

The ESF-CCS consists of four independent divisions that perform additional 2-out-of-4 voting logic, component control logic, and priority logic function.

The group controller (GC) of each ESF-CCS division receives four division ESFAS initiation signals derived from the ESFAS portion of the PPS and performs additional selective 2-out-of-4 coincidence logic to generate the ESF actuation signal. The GC also receives two division ESFAS initiation signals derived from the radiation monitoring system (RMS) and performs 1-out-of-2 logic to generate the ESF actuation signal. The ESF actuation signals are transmitted to the loop controller (LC) of the ESF-CCS. The LC executes the component control logic and outputs the component control signal to the CIM. The component control logic includes the priority logic for the operator's manual control signal and ESF actuation signal. The ESF-CCS soft control module (ESCM) on the operator console generates a component control signal of safety components by manual operator actions.

4.1.1.3 Core Protection Calculator System

The CPCS has four redundant channels that compute the DNBR and LPD values using process values, reactor coolant pump (RCP) speed, CEA position and ex-core neutron flux.

The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed a safety limit, a trip signal is transmitted to the PPS using hardwired cables.

4.1.1.4 Qualified Indication and Alarm System - P

The QIAS-P, which has two independent divisions A and B, is implemented on the common PLC platform for the safety system. The QIAS-P processes the plant parameters that are input from the safety I&C

Table 4.1-1. Interface between redundant portions of the safety system

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
1	PPS BP	PPS LCL	Partial trip	SDL	4.2.2.1
2	PPS	ESF-CCS GC	ESFAS initiation	SDL	4.1.1.2, 4.2.3.2, 4.2.3.3, 4.2.4
3-1	ITP Division A	ITP Division B	CIV signals (74 signals)	SDL	4.5.2
3-2	ITP Division C	ITP Division B	CIV signals (10 signals)	SDL	4.5.2
3-3	ITP Division D	ITP Division B	CIV signals (9 signals)	SDL	4.5.2
3-4	ITP Division B	ITP Division A	CIV signals (69 signals)	SDL	4.5.2
3-5	ITP Division C	ITP Division A	CIV signals (10 signals)	SDL	4.5.2
3-6	ITP Division D	ITP Division A	CIV signals (9 signals)	SDL	4.5.2
4	CPP in CPCS	CPC/CEAC in CPCS	Digitized RSPT values	SDL	4.3.2.1

Note: The ESF-CCS in each division sends the CIV signals to the ITP of the same division via fiber optical data network connection (SDN).

Table 4.1-2. Interface between safety and non-safety system

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
1	PPS	DRCS Remote I/O Cabinet	CWP contact	Hardwired	4.2.4
2	DIS	QIAS-P	Transfer command, HJTC heater power control	Hardwired	Figure 4-17, Table 4-2
3	QIAS-P	DIS	CETs, HJTCs, control status	Hardwired	Figure 4-17, Table 4-2
4	P-CCS	ESF-CCS	Non-safety control signals for CVCS, steam generator blowdown system, condenser vacuum system, fuel handling area HVAC system, fire protection system, process sampling system, and class 1E 4.16kV system	Hardwired	4.4.4.12
5	DMA Switches	CIM	Actuation signals for ESF components	Hardwired	4.1.1.7
6	DPS	CIM	Component control signals	Hardwired	4.1.1.7
7	ITP	QIAS-N	PPS status alarm, CPC data, Type A,B,C	SDL	3.3.2, 4.1.1.4, 4.2.2.1, 4.2.3.5,

No.	FROM	TO	SIGNAL DESCRIPTION	INTERFACE TYPE	Safety I&C TeR Section
			variables, ICC-related variables, operating ESF-CCS status for EOP, plant safe shutdown, cabinet trouble alarm, system in test		4.3.1.6,
8	MTP	DCS Gateway Server of IPS	PPS status alarm, CPC data, Type A,B,C variables, ICC-related calculation variables, control cabinet alarms, system in test	Ethernet Data Link	3.3.2, 4.3.1.5
9	IFPD (on each operator console)	ESCM (on each operator console)	Safety component selection information	Ethernet Data Link	4.1.2.7
10	PPS	TCS (turbine control system)	Turbine trip signal	Hardwired	4.2.1.1
11	ENFMS (ex-core neutron flux monitoring system)	NIMS (NSSS integrity monitoring system)	Sub-channel neutron flux signal	SDL	A.5.6

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.

via hardwired cable

of the PPS

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.

via SDN

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 via hardwired cable. These are used for the reactor power calculation and power distribution calculation.

4.3.4.3 Reactor Coolant Pump Shaft Speed Sensing System

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.

TS

- 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

FOR INFORMATION
RAI 348-8279, 07.09-9_Rev. 1

TS

TS

TS

TS

TS

TS

TS

TS

TS

TS