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.:	**274-8277**
SRP Section:	**07.01 – Instrumentation and Controls – Introduction**
Application Section:	**07.01, 07.03, and 10.2**
Date of RAI Issue:	**10/27/2015**

Question No. 07.01-35

Provide additional clarification to the response for RAI 43-7887, Question 07.01-19 (ML15224B643), to demonstrate how the turbine generator (TG) I&C system interfaces with the safety I&C system to meet the independence requirements of IEEE Std. 603-1991, Clause 5.6.3. IEEE Std. 603-1991, Clause 5.6.3, "[Independence] Between Safety Systems and Other Systems," requires the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. IEEE Std. 603-1991, Clause 5.6.3.1, states, in part, “Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.” In RAI 43-7887, Question 07.01-19, the staff requested the applicant to provide information on the design of the TG I&C system interfaces with the safety-related I&C systems to meet the requirements of IEEE Std. 603, Clause 5.6.3. In response to this RAI, the applicant stated the turbine control system (TCS) interfaces with the plant protection system (PPS) in the safety I&C systems for the turbine trip function on reactor trip. APR1400 DCD, Tier 2, Subsection 7.2.1.4, "Reactor Trip Initiation Signals," Item I, "Turbine trip," and Figure 7.2-14, "[PPS] Interface Logic Diagram for Division D," provide information about the turbine trip function and functional logic. The PPS transmits the turbine trip signal via hardwired connection to the TCS when the reactor trip initiation signal is generated as indicated on the right side of Figure 7.2-14. APR1400 non-safety, standalone I&C systems include the TCS, seismic monitoring system (SMS), vibration monitoring system (VMS), NSSS integrity monitoring system (NIMS), and fixed in-core detector amplification system (FIDAS). This response includes a table (Table 07.01-19-1, "Interface Summary") that summarizes the interfaces between the non-safety standalone I&C systems with safety I&C systems. In addition, this response states that that the PPS and ex-core neutron flux monitoring system (ENFMS) do not receive any signals from non-safety systems but only send signals to non-safety systems. Electrical isolation is provided in the PPS and ENFMS through isolation devices.

Based on the response to RAI 43-7887, Question 07.01-19, the staff requests the following additional information to determine whether the requirements of IEEE Std. 603-1991, Clause 5.6.3, have been met for the interfaces between safety and standalone non-safety systems:

1. Include in the APR1400 FSAR the description from the RAI response regarding the interface between safety-related I&C systems and non-safety standalone system. This includes the statement that the PPS and ENFMS do not receive any signals from non-safety systems but only send signals to non-safety systems. The applicant stated that electrical isolation is provided in the PPS and ENFMS through isolation devices. The applicant should include in the APR1400 FSAR a clarification on whether these isolation devices are Class 1E qualified. In addition, include the information from Table 07.01-19-1 of this RAI response into the APR1400 FSAR.

2. APR1400 FSAR Tier 2, Figure 7.2-14, only shows the PPS system interface logic diagram for Division D. It is unclear to the staff whether the interfaces depicted in this figure also apply to the other three PPS divisions. Clarify in the APR1400 FSAR whether this figure applies to the other PPS divisions. If there are differences between these interfaces for different divisions, provide a description of the differences in the APR1400 FSAR.

3. APR1400 FSAR Tier 2, Section 10.2.2.3.3, states that each trip input is applied to a triple redundant protection module, where 2-out-of-3 majority voting is conducted within the protection system where possible to prevent spurious turbine trips and enhance protection system operation on an actual turbine trip. The turbine includes instrumentation for a trip on excess vibration and a remote trip input signal from the plant control system on a reactor trip. Since there are four divisions of PPS, and the turbine protection system only has triple redundancy, how does each PPS division interface with the turbine protection system to produce a turbine trip? Provide this information in the APR1400 FSAR.

Response

1. Section A.5.6 of the Safety I&C System technical report will be revised to clarify that the isolation devices in the plant protection system (PPS) and the ex-core neutron flux monitoring system (ENFMS) are Class 1E qualified.

   Also, the information provided in Table 07.01-19-1 of the response to RAI 43-7887, Question 07.01-19 will be provided in Sections 7.2.1.4, 7.2.2.3, and 7.7.1.5 of DCD Tier 2 and Section 4.2.1.1 of the Safety I&C System technical report.

2. Notes 2 and 4 on the bottom right of Figure 7.2-14 are already provided. The notes indicate the figure applies to all PPS divisions except for the CWP implementation.

3. The "2-out-of-3 majority voting" logic stated in APR1400 FSAR, Tier 2, Section 10.2.2.3.3 is dedicated logic within the turbine control system (TCS) to generate the turbine trip signal during the system abnormal condition (e.g., generator stator wind coolant low flow, generator stator inlet water low pressure). This 2-out-of 3 voting logic does not use the signal from the 2-out-of-4 voting logic implemented in the plant protection system (PPS).

   For turbine trip, each PPS division interfaces with the TCS as follows:

   Two (2) sets of contact signals are provided per division in the reactor trip switchgear system (RTSS). A total of eight (8) output signals are generated. The contact signal, as a momentary signal type, is provided through hardwired connections. Isolation is achieved by using Class 1E isolation relays within the RTSS.

   The two sets of contact signals from each division in the RTSS are inputted to two P-CCS cabinets through hardwired connections. The P-CCS cabinets have 2-out-of-4 voting logic to prevent spurious turbine trip due to single P-CCS cabinet failure. The results of the 2-out-of-4 voting logic in the P-CCS cabinets are provided to the TCS to initiate turbine trip.

   Section 7.2.1.4 and Figure 7.2-14 of DCD Tier 2 will be revised to include the above information.

Impact on DCD

Sections 7.2.1.4, 7.2.2.3, 7.7.1.5, and Figure 7.2-14 of DCD Tier 2 will be revised, 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

Sections 4.2.1.1 and A.5.6 of the Safety I&C System technical report will be revised, as indicated in the attachment associated with this response.

In addition, the PPS generates the turbine trip signal to the turbine control system (TCS) when any variable trip initiation occurs.

, which is unidirectional from the PPS to the TCS via a hardwired connection,

a. Variable overpower

The variable overpower trip is provided to trip the reactor when the neutron flux positive power rate or neutron flux power exceeds the preset value. The neutron flux value is the average of the three linear subchannel flux values from each ENFMS safety channel. A pre-trip alarm is initiated below the trip setpoint to provide an audible and visible indication of approach to a trip condition.

1) Input

Neutron flux power from the ENFMS

2) Purpose

To provide a reactor trip in the event of uncontrolled CEA withdrawal; the functional logic for variable overpower is shown in Figure 7.2-17

b. High logarithmic power level

The high logarithmic power level trip is provided to trip the reactor when indicated neutron flux power reaches a preset value. The flux signal used is the logarithmic power signal originating in each ENFMS safety channel. The trip can be manually bypassed by the operator if power is equal to or greater than a preset value. The operating bypass is removed automatically when the power decreases below the preset value. The operating bypass setpoint is provided in Table 7.2-1.

A pre-trip alarm is initiated below the trip setpoint to provide audible and visible indications of an approach to a trip condition. The pre-trip alarm is bypassed when the trip is bypassed.

1) Input

Neutron flux power from the ENFMS

2) Purpose

To provide a reactor trip in the event of an-RCP sheared shaft

The functional logic for low reactor coolant flow is shown in Figure 7.2-27.

l. Turbine trip

The turbine trip signal is generated whenever any RPS initiation signal is generated.

The time delay is implemented in the RPS so the turbine trip signal occurs 3 seconds following a reactor trip to prevent core damage from a single CEA withdrawal.

Add the descriptions on the next page.

1) Input

All RPS initiations including manual reactor trip

2) Purpose

To provide a turbine trip in the event of a single CEA withdrawal

The functional logic for a turbine trip on a reactor trip is shown in Figure 7.2-14.

7.2.1.5 Manual Reactor Trip and Actuated Devices

Manual trip switches (two pairs in the MCR and one pair in the RSR) are provided to open the RTSS, as shown in Figures 7.2-16 and 7.2-28. Actuation of any pair of switches opens the TCBs, resulting in interruption of the ac power to the CEDMs. Both manual trip switches in a pair must be actuated to initiate a reactor trip. The manual trip signals completely bypass the automatic trip logic in accordance with NRC RG 1.62 (Reference 2).

A minimum of two divisions of RPS trips are required for a reactor trip. The RPS initiation relays in each division interface with the undervoltage devices to trip the circuit breakers of the RTSS while the DPS interfaces with the shunt trip devices to trip the RTSGs. The final actuation logic for the RPS is connected to the RTSS, which connects or interrupts the power to the digital rod control system (DRCS).

Power for CEAs comes from two full capacity motor generator (MG) sets so that the loss of either set does not cause a release of the CEAs.

For turbine trip, each PPS division interfaces with the TCS as follows:

Two (2) sets of contact signals are provided per division in the reactor trip switchgear system (RTSS). A total of eight (8) output signals are generated. The contact signal, as a momentary signal type, is provided through hardwired connections. Isolation is achieved by using Class 1E isolation relays within the RTSS.

The two sets of contact signals from each division in the RTSS are inputted to two P-CCS cabinets through hardwired connections. The P-CCS cabinets have 2-out-of-4 voting logic to prevent spurious turbine trip due to single P-CCS cabinet failure. The results of the 2-out-of-4 voting logic in the P-CCS cabinets are provided to the TCS to initiate turbine trip.

7.2.2.3 Independence

a. 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.

b. Independence between safety systems and effects of design basis events

Independence between the components of the RPS and the effects of design basis event is provided by qualifying the equipment in accordance with the requirements in Subsections 7.2.2.2 and 7.2.2.8.

Class 1E

c. Independence between safety systems and non-safety systems

The PPS and non-safety systems are isolated using qualified isolation devices or fiber-optic cables so that any failure in a non-safety system does not cause loss of the safety system function. The PPS signals transmitted to the IPS/QIAS-N are isolated using fiber-optic cable.

Data flow is unidirectional from Class 1E systems to non-Class 1E systems.

7.2.2.4 Diversity and Defense-in-Depth

The diversity and defense-in-depth analysis is described in Reference 3. The diversity features of the PPS are described in Subsection 7.2.1.9.

7.2.2.5 System Testing and Inoperable Surveillance

The system integrity is confirmed through self-diagnostics and surveillance testing. Testing features are provided for RPS testing during power operation or shutdown.

The RPS testing covers the trip path from the sensor input to the RTSG, as shown in Figure 7.2-11. The system test does not affect the protective functions. The testing system meets

Both high and low resolution rates of historical data can be transferred to the secondary storage by operator's demand. Operators can specify the time spans of the available historical data to be backed up in the secondary storage.

The historical data stored in a disk or other media are utilized for trending in the information FPDs and the LDP.

7.7.1.5 NSSS Integrity Monitoring System

The NSSS integrity monitoring system (NIMS) detects selected conditions that indicate deterioration or that could lead to deterioration of the RCS pressure boundary.

The NIMS is a non-safety monitoring system that consists of the internals vibration monitoring system (IVMS), acoustic leak monitoring system (ALMS), loose parts monitoring system (LPMS), and RCP vibration monitoring system (RCPVMS).

unidirectional

The IVMS monitors the motion of the reactor internals by using the ex-core neutron flux signals from the ENFMS detectors and provides diagnostic information that can be used to evaluate the reasons for changes in the motion of the reactor internals.

through the Class 1E qualified isolation devices

The ALMS detects a leak at specific locations or within specific components in the primary pressure boundary and provides information that is used to determine changes in the leak rate from specified components or at specified locations.

The LPMS detects the presence of loose part impacts within the major NSSS components, including the reactor vessel, steam generators, and RCP, and provides diagnostic information that allows plant system engineers to evaluate the impact location, energy, and mass of loose parts. The system is designed in compliance with NRC RG 1.133 (Reference 6).

The RCPVMS monitors the vibration levels of RCP motor and pump bearing assemblies. The RCPVMS also monitors the rotation speed and displacements of the RCP shafts.

The alarms generated by each system are provided to the operators in the MCR.

The failure of the NIMS has no effect on the function of the safety system.

- Low SG water level (fixed setpoint)
- Low SG pressure (manual reset setpoint)
- Low reactor coolant flow (high decreasing rate, minimum value) (rate limited setpoint)
- High containment pressure (fixed setpoint)

, which is unidirectional from the PPS to the TCS via a hardwired connection

Pre-trip alarms are also transmitted to the QIAS-N and IPS to provide audible and visual indication of an approach to a trip condition.

The PPS also automatically initiates a turbine trip signal to the TCS. The turbine trip signal is generated from the PPS when the PPS generates a reactor trip signal.

4.2.1.2 ESFAS Function

The ESFAS actuates system-level ESF functions that transmit signals to ESF components necessary to mitigate the consequences of the design basis accidents. This includes minimizing fuel damage and subsequent release of fission products to the environment.

There is an actuation signal for each ESFAS function. Each actuation function is similar except that specific inputs (and bypasses where provided) and the actuated devices are different.

There are ESFAS initiation signals associated with each of the following six NSSS ESF functions:

- Safety injection actuation signal
- Main steam isolation actuation signal
- Containment spray actuation signal
- Containment isolation actuation signal
- Auxiliary feedwater for SG1 actuation signal
- Auxiliary feedwater for SG2 actuation signal

4.2.1.3 Control Function

A CEA withdrawal prohibit (CWP) signal is generated when a CPC-CWP signal is input from the CPCS or high pressurizer pressure pre-trip condition is present.

The CWP signal is sent to the DRCS where it blocks CEA withdrawal.

4.2.1.4 Alarm Function

The PPS provides status alarm signals to the QIAS-N and IPS for the following types of conditions:

- Bistable trips
- Bistable pre-trips
- Operating bypasses

Clause 5.6.2: Between Safety Systems and Effects of Design Basis Event

“Safety system equipment required to mitigate the consequences of a specific DBE shall be independent of, and physically separated from, the effects of the DBE to the degree necessary to retain the capability to meet the requirements of this standard. Equipment qualification in accordance with 5.4 is one method that can be used to meet this requirement.”

Analysis:

Independence of the components in the safety I&C system to the effects of a design-basis event is provided by qualifying the equipment in accordance with the requirements in Section 6 of this report.

Clause 5.6.3: Between Safety Systems and Other Systems

“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.

5.6.3.1 Interconnected Equipment

(1) Classification: Equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems, Isolation devices used in a safety system boundary shall be classified as part of the safety system.

(2) Isolation: No credible failure on the non-safety side of an isolation device shall prevent any portion of a safety system from meeting its minimum performance requirements during and following any DBE requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.”

, including the signal interface from the PPS to the TCS and from the ENFMS to the NIMS,

Analysis:

The safety I&C system consists of four independent divisions except the QIAS-P and the BOP ESFAS which consist of two divisions. The protection division is physically separated and electrically isolated from the other three protection divisions. All connections to non-safety equipment are through isolation devices and are one way during plant operation. As an exception, the IFPD communicated to the ESCM to send identification data, which does not adversely affect safety functions and systems, through communication isolation to meet the guidance DI&C-ISG-04. The details for communication independence are described in Appendix C.5. As a result, failures of non-safety systems cannot prevent any safety I&C system from performing its safety function. All equipment/components used for safety-related functions are qualified as safety.

that are Class 1E qualified

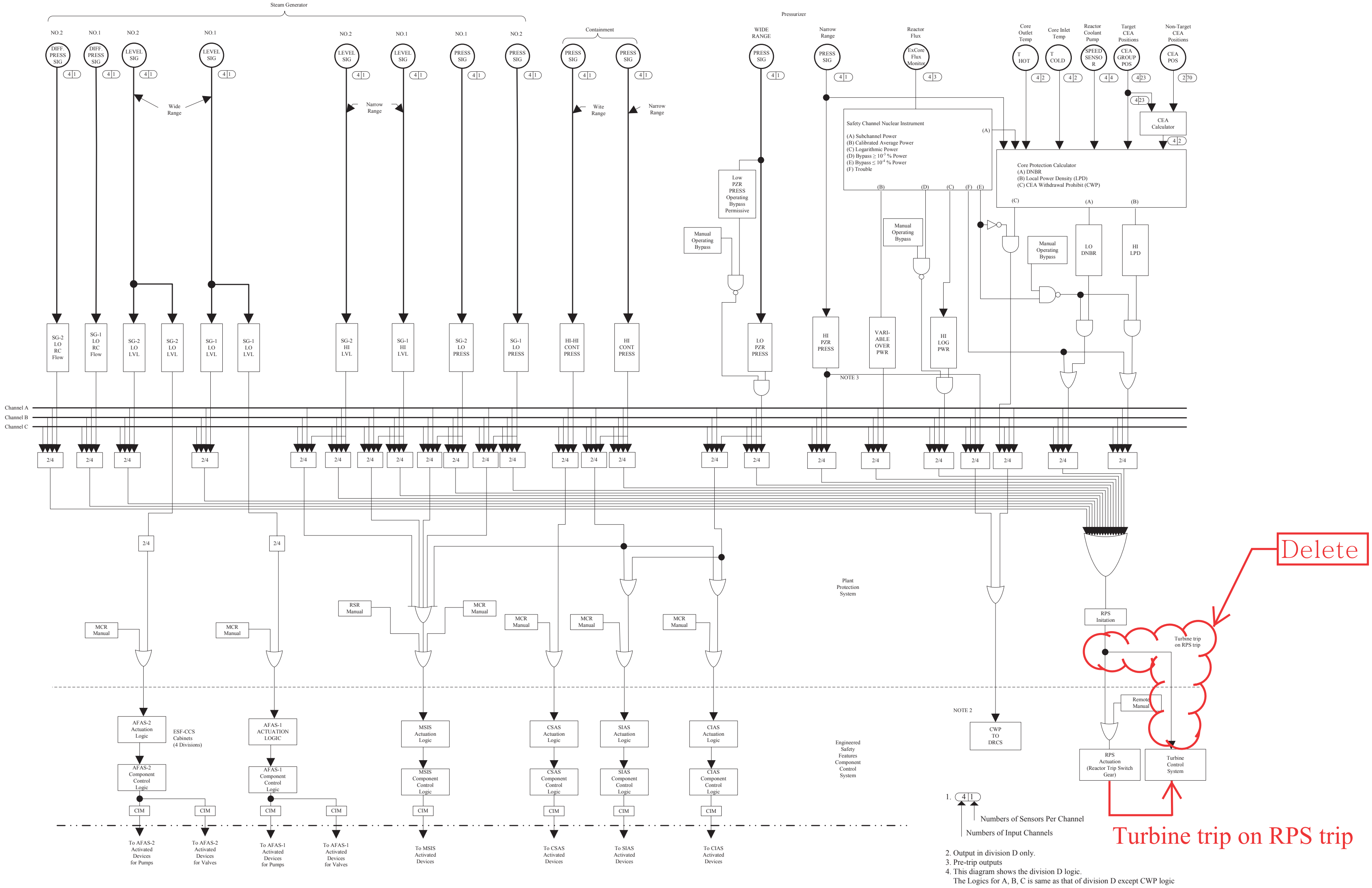
Outputs from the safety system to non-safety-related areas are isolated utilizing fiber optic cable so that a failure in the non-safety-related area does not cause loss of the safety system function. Also, these communications are unidirectional.

A non-Class 1E instrumentation circuits and cables that are in proximity of Class 1E circuits without adequate physical separation or electrical isolation are classified as an associated circuit regardless of whether or not analyses or tests can demonstrate that credible failures therein cannot adversely affect Class 1E circuits.

“5.6.3.2 Equipment in Proximity

(1) Separation: Equipment in other systems that is in physical proximity to safety system equipment, but that is neither an associated circuit nor another Class 1E circuit, shall be physically separated from the

APR1400 DCD TIER 2



2. Output in division D only.
3. Pre-trip outputs
4. This diagram shows the division D logic.
The Logics for A, B, C is same as that of division D except CWP logic

Figure 7.2-14 Plant Protection System Interface Logic Diagram for Division D

Non-Proprietary

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.:	**274-8277**
SRP Section:	**7.1 - Instrumentation and Controls**
Application Section:	**7.1, 7.3, and 10.2**
Date of RAI Issue:	**10/27/2015**

Question No. 07.01-37

Clarify how the Core Protection Calculator System (CPCS) responds to failures in order to meet the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 23.

GDC 23 requires the protection system to be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. Section C.5.1.3.7,“DI&C-ISG-04 Staff Positions,” of Technical Report APR1400-Z-J-NR-14001, Revision 0, “Safety I&C System”, last paragraph at the bottom of page C24 discusses reed switch position transmitter (RSPT)1 and RSPT2 failure, penalty factors (PF) and plant trips.

Based on the staff’s review of the CPCS, the staff requests the applicant to clarify the following:

1) During normal plant operation, explain how the predetermined control element assembly (CEA) PF value provides assurance that it will be a PF value that is an accurate representation of the actual core CEA PF.

2) Discuss why, after sensing that both RPST1 and RSPT2 signals have failed, the safety system would not automatically place the affected channel(s) in trip. By not placing the affected channel in trip how are the requirements of GDC 23 met?

3) Discuss why, after sensing that both CEAC1 and CEAC2 are inoperable, the safety system would not automatically place the affected channel(s) in trip. By not placing the affected channel in trip how are the requirements of GDC 23 met?

The staff requests the applicant to include this clarification in the APR1400 FSAR or its referenced documents.

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

The Safety I&C System Technical Report "APR1400-Z-J-NR-14001" will be revised, as indicated in the attachment associated with this response.

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

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.

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

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

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.:	**274-8277**
SRP Section:	**7.1 - Instrumentation and Controls**
Application Section:	**7.1, 7.3, and 10.2**
Date of RAI Issue:	**10/27/2015**

Question No. 07.01-38

Define terminology used when discussing the CPCS and ensure the consistency of these terms among the APR1400 FSAR sections and the referenced documents.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.1 of IEEE Std. 603-1991 states, in part, "The safety systems shall perform all safety functions required for a DBE in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the DBE requiring the safety functions.

APR1400 FSAR Tier 2, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," No. 2-12 a), states "Affected CPC uses the last valid PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger." However, Technical Report (TeR) APR1400-F-C-NR-14003, Rev. 0, "Functional Design Requirements for CPCS," Section 4.2.4 uses the term "last good" DNBR and LPD PFs. It is not clear to the staff whether these terms refer to the same PF. It is also not clear to the staff what is meant by "last good" or "last valid" PF. In addition, the Functional Design Requirements for CPCS TeR refers to DNBR and LPD PFs from the CEAC which is not used in the APR1400 FSAR or other referenced document. For example, the TeR APR1400-Z-J-NR-14001, "Safety I&C System" states that the CEAC processor module calculates the magnitude of CEA deviation PFs and does not refer to the DNBR and LPD PFs. Further APR1400 FSAR Tier 2, Table 7.2-7, No. 2-12 a), states, "If the other CEAC is failed/declared inoperable/or in test, a large pre-assigned PF is assumed in that CPC." While the Functional Design Requirements for CPCS TeR, Section 4.2.4 states, "Both CEACs are considered inoperable. Use the pre-determined DNBR and LPD penalty factors..." It is not clear to the staff whether the terms "pre-assigned" and "pre-determined" have the same meaning. Definitions were also not provided for these terms. As such, the staff requests the applicant to review the design descriptions of the CPCS in the APR1400 FSAR and its referenced documents to ensure consistency of the terminology used and to provide definitions for terms used.

Response

The TeRs and the DCD use terminology which is not consistent. To provide consistency, DCD Table 7.2-7 will be revised as follows:

- The term of "last valid" PF will be replaced with "last good" PF.
- The term of "pre-assigned" PF will be replaced with "pre-determined" PF.

The following definitions will be provided in Table 7.2-7.

- Last good PF/Position : Last PF/Position value which is received from the sending processor when the quality is good.
- Pre-determined PF : Penalty Factor which is determined based on the reactivity worth for each CEA.

Impact on DCD

Table 7.2-7 of DCD Tier 2 will be revised, 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.

Table 7.2-7 (17 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-4	Non-target CEA position	a) Low level signal caused by failure (out of range)	• Shorted resistor • Failed reed switches • Power supply malfunction	Erroneous input to one of 2 CEACs in all four CPC channels. CEAC sensor fail indication for out of range or rate of change failures. If more than three CEAs are affected, likely CEAC fail condition. If failure occurs slowly, and multiple CEAs are affected, may get large PF to all operable CPC channels, causing a reactor trip.	• CEAC sensor failure indication/annunciation. CEA Position display depiction • CPC DNBR/LPD channel trips unlikely, but possible on slowly developing failure	Normally, no PF or trip on sensor failure. If failure is slow to develop, and is not recognized by CEAC as a sensor failure until after out of range, PF could occur. On excessive number of failures (as in the loss of RSPT power), a CEAC Fail condition occurs.	• If sensor failure is recognized, and few sensors are affected (less than 4), then there is no effect on RPS. • CEAC uses ~~last valid~~ last good [1] position of the sensor in calculations. RPS remains in 2-out-of-3 coincidence logic. If sensor failure is not recognized by CEAC prior to sensor going out of range, reactor trip may occur on CEAC PF, Multiple CEA failures can cause CEAC Fail. CPC then selects ~~last valid~~ last good PF from failed CEAC, or current PF from operable CPC, whichever is larger. • RPS logic is converted to a 2-out-of-2 coincidence logic on a channel trip.	

(1) Last good PF/Position : Last PF/Position value which is received from the sending processor when the quality is good.

Table 7.2-7 (19 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-4	Non-target CEA position (Continued)	d) High-level signal caused by failure (out of range)	Shorted resistor, failed reed switches, power supply malfunction	• Erroneous input to one of two CEACs in all four channels. CEAC sensor fail and channel trouble indication for out of range or deviation from normal change rate. • If more than four CEAs are affected, likely CEAC fail condition. In case that the failure proceeds slowly and many CEAs are affected, the operating CPC receives a large PF and generates reactor trip.	• CEAC sensor failure indication/annunciation on OM and MTP. CEA position display depiction • CPCS channel trip unlikely, but possible on slowly developing failure from erroneous PF calculation	Sensor failure does not cause PF or trip. Until the range is deviated during the failure is developing slowly, the PF can be generated if not acknowledged as sensor failure by CEAC. On excessive number of failures (as in the loss of RSPT power), a CEAC fail condition occurs.	• If sensor failure is recognized, and few sensors are affected (less than 4), then there is no effect on RPS. • CEAC uses ~~last valid~~ last good position of the sensor in its calculations. • RPS remains in 2-out-of-3 coincidence logic. • If sensor failure is not recognized by CEAC prior to sensor going out of range, reactor trip may occur on CEAC PF. • Multiple CEA failures can cause CEAC failure. CPC then selects ~~last valid~~ PF from failed CEAC, or current PF from operable CPC, whichever is larger. • RPS logic is converted to a 2-out-of-2 coincidence logic on a channel trip.	.

Table 7.2-7 (26 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-12	CEAC 1 processor module (PM) processor section	a) OFF; processor off	Loss of module power; software execution stops	• CEAC 1 watchdog timer timeout, CEAC 1 fail indication on OM/MTP. • Channel trouble indication / annunciation. • CEAC 1 fail flag to CPC in the same channel.	• CEAC 1 fail indication on OM/MTP • Channel trouble indication / annunciation CEAC 1 processor fault lamp on, green run lamp out	Two redundant CEACs in each channel.	• Affected CPC uses the ~~last valid~~ last good PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger. • If the other CEAC is failed/declared inoperable/or in test, a large ~~pre-assigned~~ pre−determined (2) PF is assumed in that CPC.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; processor running, CEAC fails to detect proper CEA position, or otherwise fails to produce desired results.	Erroneous inputs, unrecognized hardware or software malfunction;	• Possible inconsistency in CEA position with respect to other CEAC/pulse count. • Failure to properly indicate CEA motion.	• Cross channel comparison of CEA position	Two redundant CEACs in each channel.	• Affected CPC uses the higher of the PFs from the two CEACs in the affected channel. • CEAC 1 is the preferred source of Target CEA position to the CPC. • If target CEA position is improper, could get improper channel response to a valid subgroup deviation or groups out of sequence. • If so, only one CPC channel is affected. • RPS logic is converted to a 2-out-of-2 coincidence logic.	To restore the PPS logic to 2-out-of-3 coincidence, the bypassed channel is returned to operation and the failed channels are bypassed. Note that on line diagnostics identify problems in CEAC module and generate CEAC failure.

(2) Pre−determined PF : Penalty Factor which is determined based on the reactivity worth for each CEA.

Table 7.2-7 (27 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-13	CEAC 2 processor module (PM) processor section	a) OFF; processor off	Loss of module power; software execution stops	• CEAC 2 watchdog timer timeout, CEAC 2 fail indication on OM/MTP. • Channel trouble annunciation. • CEAC 2 Fail flag to CPC in the same channel.	• CEAC 2 Fail indication on OM/MTP • Channel Trouble annunciation CEAC 2 processor fault lamp on, green run lamp out	Two redundant CEACs in each channel.	• Affected CPC uses the ~~last valid~~ last good PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger. • If other CEAC is failed/declared inoperable/or in test, a large ~~pre-assigned~~ pre-determined PF is assumed in that CPC.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; processor running, CEAC fails to detect proper CEA position, or otherwise fails to produce desired results.	Unrecognized hardware or software malfunction	Possible inconsistency in CEA position with respect to other CEAC/pulse count. Failure to properly indicate CEA motion.	Cross channel comparison of CEA position	Two redundant CEACs in each channel.	• Affected CPC uses the higher of the PFs from the two CEACs in the affected channel. • CEAC 2 is the alternate source of Target CEA position to the CPC. • Therefore, Target CEA position errors are not passed on to CPC unless CEAC 1 is also inoperable.	• Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3. • After on-line diagnostic function is performed and the problem within CEAC module is identified, CEAC fail condition is generated.

Table 7.2-7 (31 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-16	One CEAC to CPC high speed link in a CPC channel	Loss of one SDL	Mechanical failure, loss of fiber-optic modem power, damage to link	• SDL diagnostics indicate SDL failure, channel trouble indication on OM/MTP, trouble annunciation • CPC uses ~~last valid~~ last good PF from inoperable CEAC versus current PF from operable CEAC. • Target CEA position sent to CPC over remaining link	• Channel trouble indicated on OM/MTP in affected channel(s) • Diagnostics identify nature of failure.	• Redundant CEAC to CPC SDL provides PFs and Target CEA position input. • One channel has one inoperable CEAC. • All others channels fully operable.	• One channel has one inoperable CEAC. • Other channels fully operable. • RPS remains in 2-out-of-3 coincidence logic.	Operation with one failed CEAC in one or more channels addressed by LCO 3.3.3.
2-17	Both CEAC to CPC high speed links in a CPC channel	Loss of both SDL	Mechanical failure, loss of fiber-optic modem power, damage to link	• SDL diagnostics indicate SDL failure, channel trouble indication on OM/MTP, trouble annunciation • Both CEACs fail. CPC uses ~~pre-assigned~~ pre−determined PF on loss of both CEACs. • Likely channel trip if at high power levels • If SDL failure also causes loss of target CEA position transmission, CPC Fail and DNBR/LPD channel trip occurs.	• CPC Fail indicated on OM/MTP in affected channel(s) • Diagnostics identify nature of failure • Channel trip (DNBR/LPD trip/pre-trip/CWP) likely	• On loss of both CEACs, CPC channel uses ~~pre-assigned~~ pre−determined penalty. • Trip likely at high power levels. • Loss of Target CEA position input causes aux trip (DNBR/LPD) • Three channel redundancy in PPS	• One channel has two inoperable CEACs. Likely channel trip. • RPS is converted to 1-out-of-2 coincidence logic.	To restore the PPS logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channels are bypassed.

Table 7.2-7 (32 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-18	Loss of all SDL within a single CPC channel	Off, no transmission	Loss of fiber-optic modem power	• Channel trouble indication on OM/MTP in receiving channels • DNBR/LPD trip in failed channel due to loss of target CEA position • CPC fail indicated at OM/MTP • Failure of one CEAC in other operable CPC channels	• SDL include diagnostics to detect failures by receiving processor. • Channel trouble indicated on OM/MTP in receiving channel(s) • One CEAC failed in other channels. • Both CEACs failed in inoperable channel DNBR/LPD trips in failed channel. • CPC fail indication on OM/MTP • Diagnostics in receiving processors identify nature of failure	• Two CEACs per operable CPC channel. • Other CEAC remains operable. • CPC uses ~~last valid~~ last good PF from failed CEAC or current PF from operable CEAC, whichever is larger. • One CPC channel in trip, three channel redundancy	• One CEAC Failed in all operable CPC channels, and one CPC channel in trip (RPS in a 1-out-of-2 coincidence logic). • Other CPC channels remain operable with one CEAC in each channel.	Operation with a single CEAC failure in one or more channels addressed in LCO .3.3.3. To restore the PPS logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channels are bypassed.

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.:	**274-8277**
SRP Section:	**7.1 - Instrumentation and Controls**
Application Section:	**7.1, 7.3, and 10.2**
Date of RAI Issue:	**10/27/2015**

Question No. 07.01-39

Describe what happens to the output of safety-related I&C system processors when the processor is declared inoperable.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.1, "Single-Failure Criterion," of IEEE Std. 603-1991 states, in part, "The safety systems shall perform all safety functions required for a [DBE] in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the [DBE] requiring the safety functions."

APR1400 FSAR Tier 2, Table 7.2-7 provides the system level failure modes and effects analysis (FMEA) for the PPS. For several of the entries in this table, the applicant states that the effect on the PPS will be the respective safety-related I&C system processor (e.g. CEAC) is declared inoperable. The staff could not find a description of what happens to the output of this processor (e.g. forced to a predefined value of 0 or 1) when it is declared inoperable per technical specification. As such, the staff requests the applicant to modify the APR1400 FSAR to describe what happens to the output of safety-related I&C system processors when the processor is declared inoperable.

Response

Section 1.1 of DCD Tier 2 Chapter 16 Technical Specifications provides the following definition for the terms “operable” and “operability”:

“A system, subsystem, division, train, component or device shall be OPERABLE or have OPERABILITY when it is capable of performing its specified safety function(s)...

The term ‘inoperable’ indicates that the system, subsystem, division, train, component or device is not capable of performing its specified safety function(s)...”

Accordingly, the output of the safety-related I&C system processors stays at a non-trip state when the processor is declared inoperable.

Therefore, the following description will be added to Table 7.2-7 of DCD Tier 2 where the term “inoperable” is used for the first time:

The output of the safety-related I&C system processors stay in a non-trip state when the processor is declared inoperable.

Impact on DCD

Table 7.2-7 of DCD Tier 2 will be revised, 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.

Table 7.2-7 (26 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-12	CEAC 1 processor module (PM) processor section	a) OFF; processor off	Loss of module power; software execution stops	• CEAC 1 watchdog timer timeout, CEAC 1 fail indication on OM/MTP. • Channel trouble indication / annunciation. • CEAC 1 fail flag to CPC in the same channel.	• CEAC 1 fail indication on OM/MTP • Channel trouble indication / annunciation CEAC 1 processor fault lamp on, green run lamp out inoperable[3]	Two redundant CEACs in each channel.	• Affected CPC uses the last valid PF from the failed CEAC or the current PF from the operable CEAC, whichever is larger. • If the other CEAC is failed/declared inoperable/or in test, a large pre-assigned PF is assumed in that CPC.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; processor running, CEAC fails to detect proper CEA position, or otherwise fails to produce desired results.	Erroneous inputs, unrecognized hardware or software malfunction;	• Possible inconsistency in CEA position with respect to other CEAC/pulse count. • Failure to properly indicate CEA motion.	• Cross channel comparison of CEA position	Two redundant CEACs in each channel.	• Affected CPC uses the higher of the PFs from the two CEACs in the affected channel. • CEAC 1 is the preferred source of Target CEA position to the CPC. • If target CEA position is improper, could get improper channel response to a valid subgroup deviation or groups out of sequence. • If so, only one CPC channel is affected. • RPS logic is converted to a 2-out-of-2 coincidence logic.	To restore the PPS logic to 2-out-of-3 coincidence, the bypassed channel is returned to operation and the failed channels are bypassed. Note that on line diagnostics identify problems in CEAC module and generate CEAC failure.

[3] The output of the safety−related I&C system processors stay in a non−trip state when the processor is declared inoperable.

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.:	**274-8277**
SRP Section:	**7.1 - Instrumentation and Controls**
Application Section:	**7.1, 7.3, and 10.2**
Date of RAI Issue:	**10/27/2015**

Question No. 07.01-40

Clarify the terms used in APR1400 FSAR Tier 2, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” Item 2-14, and clarify why an improper CEA position renders a CPC inoperable and changes the voting logic.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995. Clause 5.1 of IEEE Std. 603-1991, states, in part, “The safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

For the APR1400 FSAR Tier 2, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” Item 2-14, Failure Mode Item b), identifies the following failure terms:

a. Unrecognized software malfunctions
b. Erroneous control element assembly (CEA) position transmission and indication
c. Improper CEA position

It is unclear to the staff what these terms mean with respect to the failure analysis. In addition, it is unclear to the staff how an improper CEA position renders a core protection calculator (CPC) channel inoperable and changes the logic to 2-out-of-2 coincidence. Describe and define the failure terms used: software malfunction, erroneous CEA position, erroneous CEA indication, and improper CEA position. In addition, clarify why an improper CEA position renders a CPC inoperable, and changes the logic to 2-outof- 2 coincidence (e.g. does the voting logic change to 2-out-of-2). Provide diagrams regarding the operation of the CPCS in the APR1400 FSAR to support these clarifications.

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

The Safety I&C System Technical Report "APR1400-Z-J-NR-14001" will be revised, as indicated in the attachment associated with this response.

LIST OF TABLES

Figure 4−9a. CEA Position and PF movement

LIST OF FIGURES

TS

TS

- Qualified indication and alarm system - non-safety
- Vital bus power supply system
- Field sensors

The figure will be added.

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.

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

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