SUPPLEMENTAL 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 l, "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.

Supplemental Response

Descriptions of the non-safety standalone I&C systems, including turbine/generator control system, seismic monitoring system, vibration monitoring system, NSSS integrity monitoring system, and fixed in-core detector amplification system and their interface with safety systems will be added as Section 7.9.1.4 Item d, “Non-safety standalone I&C systems” in DCD Tier 2.

Impact on DCD

Sections 7.2.1.4, 7.2.2.3, 7.7.1.5, 7.9.1.4, 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.

c. Independence between safety systems and non-safety systems

Class 1E

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).

The IVMS monitors the motion of the reactor internals by using the unidirectional ex-core neutron flux signals from the ENFMS detectors through the Class 1E qualified isolation devices and provides diagnostic information that can be used to evaluate the reasons for changes in the motion of the reactor internals.

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.

The ITP sends the status and alarm information to the QIAS-N through the SDL unidirectionally. Therefore the failure of the QIAS-N does not prevent the ITP from performing the intended functions.

c. DCS gateway server

The DCS gateway server receives data from safety systems with fiber-optic isolation.

Insert the descriptions on the next page.

Data Communication from Non-Safety System to Safety System

Ethernet communication is used to communicate from the IFPD to the ESCM. The connection does not transfer any safety or control information to perform any safety or control functions. The signal from the IFPD provides component identification information to the ESCM. This signal is used for bringing up the control template on the ESCM display and is not used for performing any control functions. Therefore, the ESF-CCS division does not rely on information from the IFPD to accomplish its function.

Compliance with DI&C-ISG-04 regarding communication from the IFPD to the ESCM is described in Appendix C of the Safety I&C System Technical Report (Reference 3).

Data Communication between the QIAS-N and Other Systems

The QIAS-N network is implemented by the SDN.

a. QIAS-N network

The QIAS-N network is used for signal connections as follows:

1) QIAS-N processor

2) QIAS-N display

3) QIAS-N MTP

The QIAS-N network and the DCN-I network are independent of each other. The QIAS-N network uses different data communication hardware and protocols from the DCN-I network.

d. Non-safety standalone I&C systems

Non-safety standalone I&C systems of APR1400 consist of T/GCS, seismic monitoring system (SMS), vibration monitoring system (VMS), NIMS, and FIDAS. SMS, VMS, and FIDAS have no interface with safety I&C systems. However, T/GCS has interface with PPS and NIMS has interface with the ex-core neutron flux monitoring system (ENFMS). The interface between T/GCS and PPS and between NIMS and ENFMS is all unidirectional signal interfaces from the safety system to the non-safety system through Class 1E qualified isolation devices.

- 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

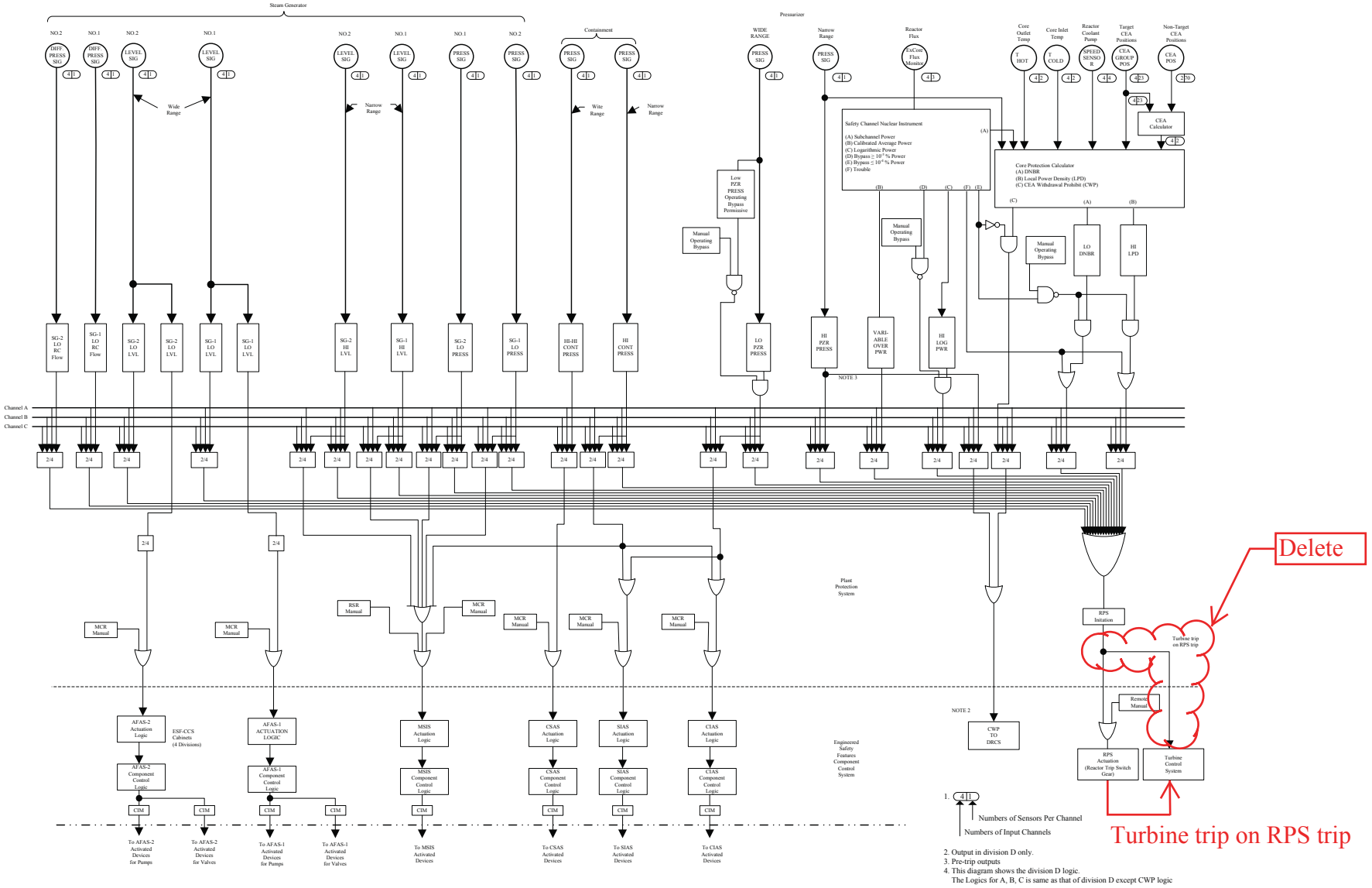

Figure 7.2-14 Plant Protection System Interface Logic Diagram for Division D