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.:	**555-9163**
SRP Section:	07.02 – Reactor Trip System
Application Section:	7.2 [NSAL-17-2]
Date of RAI Issue:	**09/20/2017**

Question No. 07.02-19

Title 10 of the Code of Federal Regulations (10 CFR), Section 52.47(a)(2), "Contents of applications; technical information," requires in part, that the description of the structures, systems, and components (SSCs) of the facility shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. 10 CFR Part 50 Appendix A, General Design Criterion (GDC) 23 states, in part, that the protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other predefined basis. Due to new Common Q Platform design information presented in the Westinghouse Nuclear Safety Advisory Letter (NSAL)-17-2, dated July 5, 2017 (Agency Documents Access and Management System (ADAMS) Accession No. ML17213A208), the staff requests Korea Hydro & Nuclear Power Co., Ltd. (KHNP) to review the applicable safety-related Common Q platform based systems design descriptions of the APR1400 design certification application (DCA) and demonstrate that the APR1400 DCA is not affected by the design information contained within the NSAL. Specifically, the staff requests KHNP to:

1) Review information presented in NSAL-17-2 against information presented in the APR1400 Final Safety Analysis Report (FSAR) and referenced technical reports design descriptions to determine if the information present in NSAL-17-2 affects the APR1400 DCA;

2) Review and clarify whether the specified watchdog timers (WDTs) referenced in the APR1400 FSAR, Tier 2 and the APR1400-Z-J-NR-14001-P, "Safety Instrumentation and Controls (I&C) System," Technical Report, Revision 1 are the window WDTs referenced in WCAP-16097, "Common Qualified Platform Topical Report," Revision 3, and make appropriate modifications in the APR1400 FSAR Tier 2 and its referenced technical reports to reflect this clarification;

3) Verify that the window WDTs are hardware-based (i.e., does not contain software and do not rely upon software for activation), as specified in the APR1400 DCA and WCAP-16097, and include the definition for the term “hardware” provided in the response to RAI 356-7881, Question 07-14 into the APR1400 FSAR, Tier 2 or the Safety I&C System Technical Report; and

4) Expand the design descriptions in APR1400 FSAR Tier 1, Sections 2.5.1.1, Item 13 and 2.5.4.1, Item 10 and corresponding Inspections, Tests, Analyses and Acceptance Criteria in Tier 1, Tables 2.5.1-5, Item 13 and 2.5.4-5, Item 10, respectively, to verify that the WDTs used to generate trip and fail-safe conditions for reactor trip and engineered safety features actuation system functions, respectively, are hardware-based.

Response – (Rev.2)

1) The watchdog timer (WDT) related design information in DCD Tier 2 and the Safety I&C System technical report refers to "window WDT" and the safety functions of the APR1400 safety systems do not utilize the stall timer addressed in NSAL-17-2.

   Furthermore, the applicable safety-related Common Q platform based systems design descriptions of the APR1400 design certification application are not affected or conflicted by the design information contained within NSAL-17-2: there is no impact to the safety-related function or operability.

   Should the licensing basis be revised, the COL applicant will address the change accordingly.

2) The WDTs provided in DCD Tier 2 and the Safety I&C System technical report are all window WDTs and they will be clearly stated as indicated in the attachment with supplemental description of the window WDT.

3) The WDTs addressed in Rev.1 Response to RAI 356-7881, Question 07-14(ML16271A351), are all window WDTs. The window WDTs are external to the microprocessors which are part of the Common Q^{TM} platform. Each window WDT is strictly a hardware device (e.g., does not employ a programmable hardware device like an FPGA or contain software). Each window WDT does not rely upon software for activation.

   Additionally, the common output relay is a hardwired component located on the processor module.

   The above information will be added to the Safety I&C System technical report as indicated in the attachment.

4) The design description in DCD Tier 1, Sections 2.5.1.1, Item 13 and its corresponding Inspections, Tests, Analyses and Acceptance Criteria in Tables 2.5.1-5, Item 13 are expanded to verify that the WDTs from NRC-approved safety I&C platform used to generate trip and fail-safe conditions for reactor trip are hardware-based as indicated in the attachment. Likewise, the design description in DCD Tier 1, Section 2.5.4.1, Item 10

and its corresponding Inspections, Tests, Analyses and Acceptance Criteria in Tables 2.5.4-5, Item 10 are expanded to verify that the WDTs from NRC-approved safety I&C platform used for generating alarms are hardware-based as indicated in the attachment.

Impact on DCD

Sections 2.5.1.1 and 2.5.4.1, and Tables 2.5.1-5 and 2.5.4-5 of DCD Tier 1 will be revised as indicated in the attachment.

Table 7.2-7 of DCD Tier 2 will be revised as indicated in the attachment.

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 4.2.2.1, 4.3.3.3, 4.4.3.1, 4.4.3.2, A.5.7, Figure 4-7, Figure 4-13, and Figure 4-18 will be revised, as indicated in the attachment.

- A single 120 volts alternating current (Vac) power is provided to redundant direct current (DC) power supplies in each PPS division. A loss of the 120 Vac power feeds to a PPS division causes the safety outputs for the division to fail to the predefined safe state.

- The heartbeat signal of the BP is supervised by the LCL to ensure appropriate trip signals are generated for the reactor trip function.

- Each PPS LCL RT processor is supervised by the built-in watchdog timer (WDT). The contacts outputs of WDT are hardwired in series to the RPS initiation circuit to ensure appropriate trip signals are generated for the reactor trip function as shown in Figure 4-7. If the WDT contained in the LCL RT processor module fails to be reset in the predefined time, the WDT will block the power going through the interposing relay. This will result in opening the interposing relay of the undervoltage trip device in the reactor trip initiation circuit. The detailed information on hardware watchdog timer configuration and relations to fail-safe operation are provided in Reference 12.

The hardware and software for the PPS meet the SFC outlined in IEEE Std. 603-1991 and IEEE Std. 379 as endorsed by RG 1.53 and RG 1.153.

The PPS is designed to detect any error condition of the PPS through the self-diagnostic and supervisory functions such as I/O module diagnostic, processor module diagnostic, application program CRC, communication error CRC, and etc. The detailed information is provided in Reference 12.

The PPS software execution is deterministic to ensure predictable system performance and response under worst-case plant loading condition. The task scheduler schedules the execution of the application programs and periodic system software tasks based on predefined priorities. The detailed information of the deterministic performance and the deterministic performance is provided in Reference 12.

Each PPS division contains a BP and LCL racks. Each BP sends its bistable trip status to each redundant LCL processors in the same division via non-fiber optic SDL and to other redundant divisions' LCL racks via fiber optic SDL. The redundant LCL racks within each division receive the bistable trip signals and perform the 2-out-of-4 local coincidence logic for each RT and ESFAS function. Each LCL rack has digital output (DO) module(s) whose outputs are combined to form the selective 2-out-of-4 coincidence initiation circuit. The configuration is shown in Figure 4-5.

The system, including the processor modules, is subject to continuous hardware monitoring and annunciation of failures to maximize system availability. ~~A watchdog timer~~ within the processor modules monitors the operability of the processor modules (PMs). Refer to Section 5.2.1.3 in Reference 12.

The PPS has redundancy and diversity features. Redundant PPS analog input parameters considering DBEs are assigned to each analog input module for minimizing the effects of a single failure of an analog input (AI) module as shown in Figure 4-5. Each BP processes the bistable logic in the reverse order to that of the other BP to increase the degree of software diversity. The design includes redundant BP racks in each division. The independent configuration of the I/O and communication devices in redundant cabinets is provided.

The selective 2-out-of-4 initiation logic combination of RPS initiation signals is designed to permit testing of the LCL processor without causing RT initiation in a division and still permit valid trip signals to propagate to the RTSS. This design provides hot swap capability for a single PLC module, without causing an output initiation signal. A design goal is to enhance the system's fault tolerance by accommodating a single processor module or SDL data communication link failure in the division without

window
window
window
Section 5.2.1.3 "Watchdog Timer" of
The window WDTs

● There are two window WDTs in a processor module: one located in the processing section and the other one in the communication section of the processor module. Those two window WDTs share a common output relay (a hardwired component located on the processor module) that is tripped by a fault either in the processing section or in the communication section of the processor module.
● The window WDTs are external to the microprocessors which are part of the Common Q^{TM} platform. Each window WDT is strictly a hardware device (e.g., does not employ a programmable hardware device like an FPGA). See Section 5.2.1.3 of Reference 12 for more details.

TS

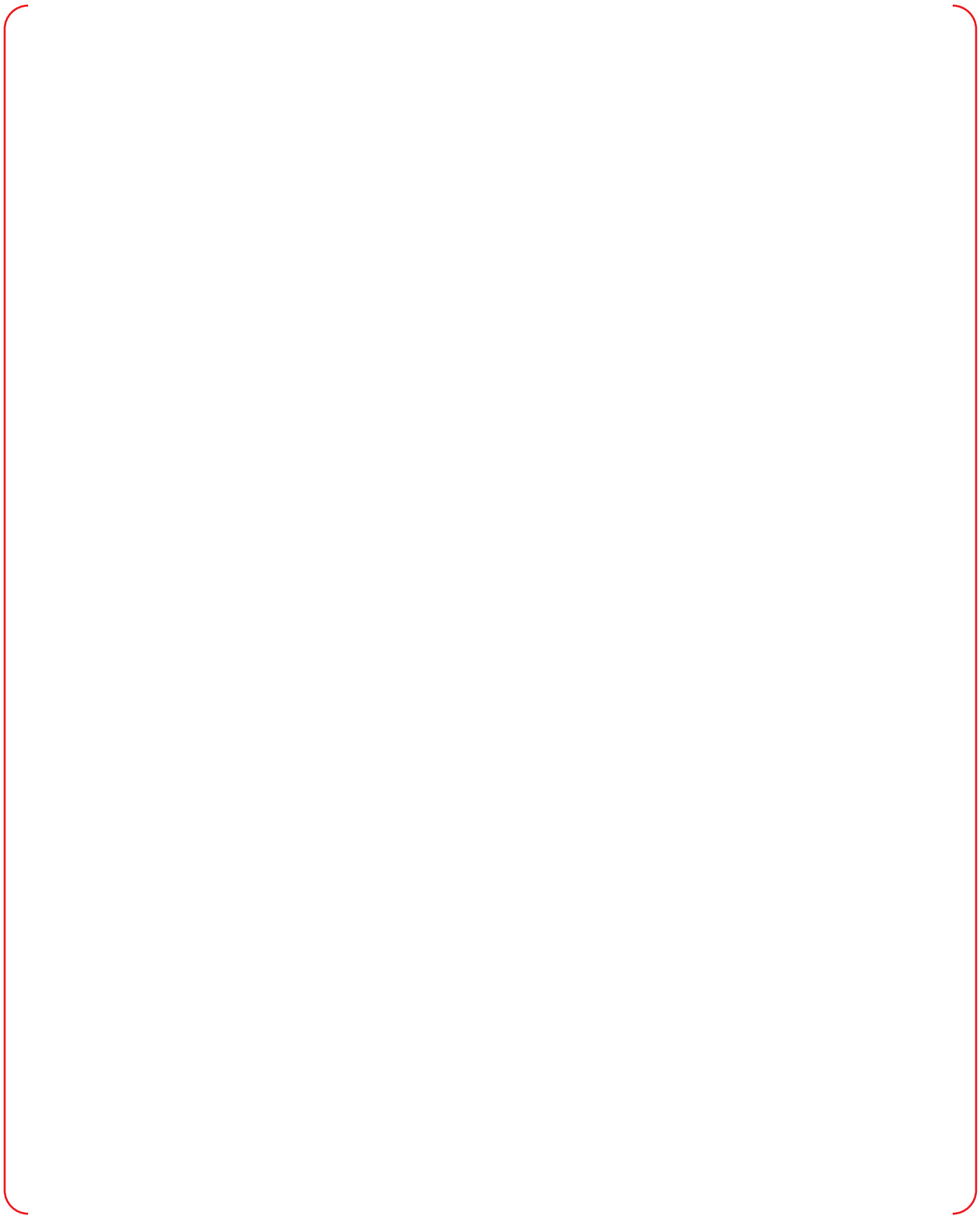

Figure 4-7 Watchdog Timer for PPS

TS

.

TS

.

4.3.4 System Interfaces

The CPCS interface with other systems is shown in Figure 4-12. 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 via hardwired cable from the APC-S . The pressurizer pressure signals are used in the DNBR and the LPD calculations

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.

TS

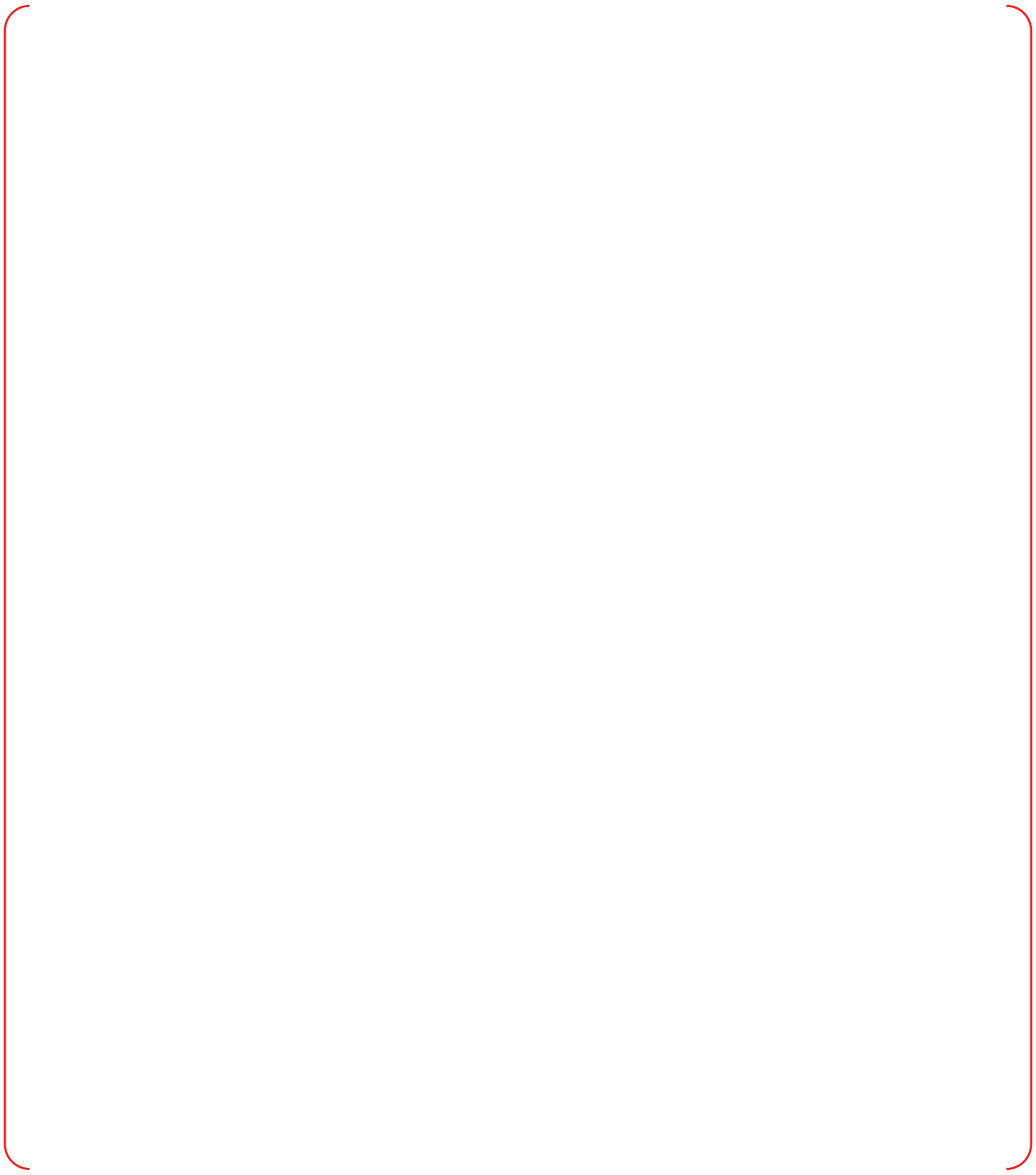

Figure 4-13 Watchdog Timer for CPCS

TS

TS

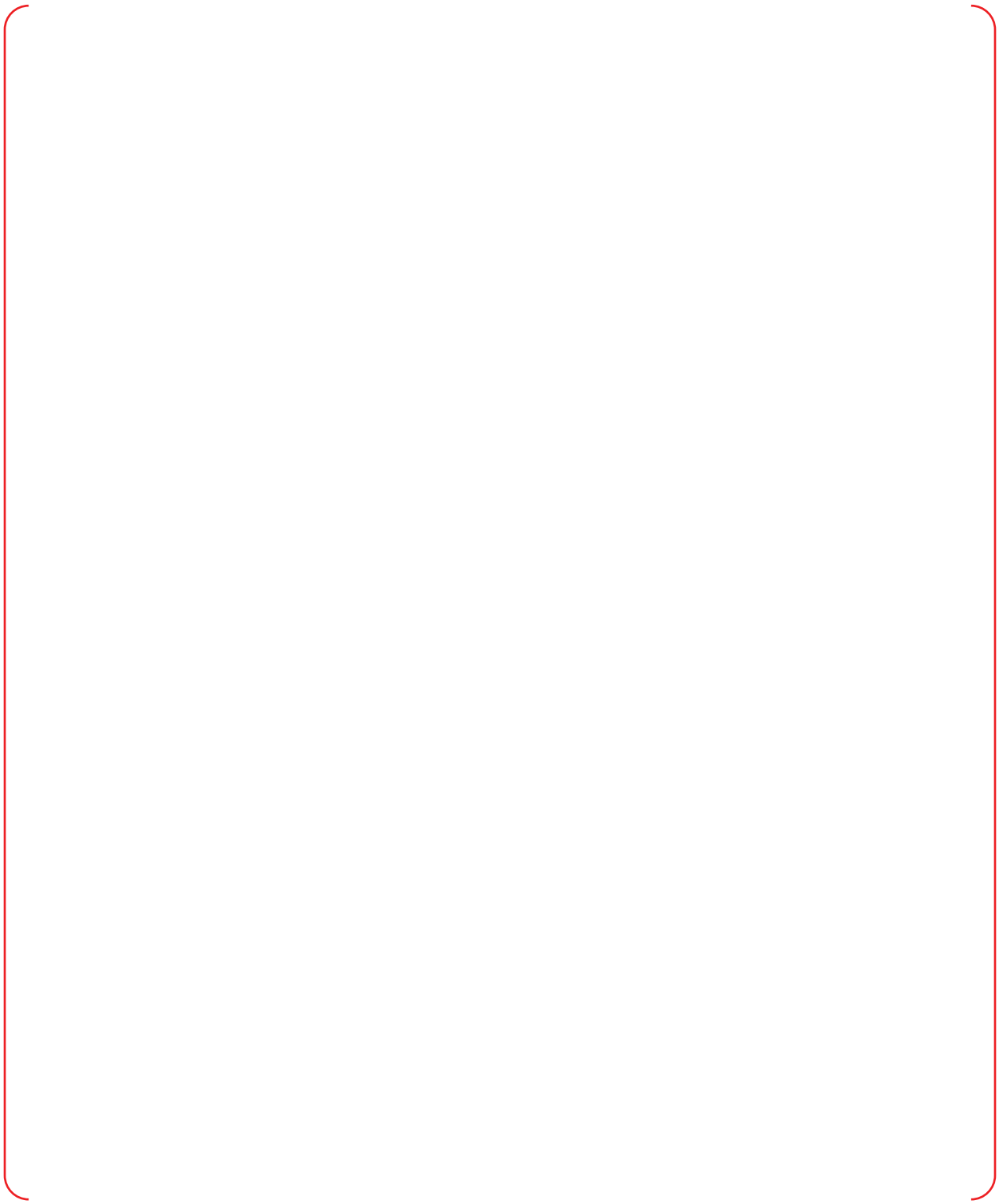

Figure 4-18 Watchdog Timer for ESF-CCS

A.5.7 Capability for Test and Calibration

Clause 5.7: Capability for Test and Calibration

"Capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. Testing of Class 1E systems shall be in accordance with the requirements of IEEE Std. 338-1987. Exceptions to testing and calibration during power operation are allowed where this capability cannot be provided without adversely affecting the safety or operability of the generating station. In this case:

(1) appropriate justification shall be provided (for example, demonstration that no practical design exists),

(2) acceptable reliability of equipment operation shall be otherwise demonstrated, and

(3) the capability shall be provided while the generating station is shut down."

Analysis:

The safety I&C system design complies with IEEE Std. 338-1987 and RG 1.22.

The safety I&C system incorporates enhanced continuous system self-checking features. System self-checking features include on-line diagnostics for the PLC software, hardware, and communications systems. Administrative procedures provide appropriate guidance in the event a portion of the safety system is in bypass or is manually tripped. These procedures are augmented by automatic indication at the system-level that a portion of the system is in bypass or that a portion of the protection system and/or the systems actuated or controlled by the protection system is tripped.

The PPS, CPCS, and ESF-CCS make extensive use of watchdog timers in performing built-in self tests. The output of the watchdog timer causes the fail-safe state for RPS and ESFAS functions.

Provisions for periodic manual surveillance testing provide the overlapped testing functions that confirm operability of the system and specifically determine operability of portion of the system that is not tested by the system's self-diagnostics.

The requirement for periodic testing is addressed by channel calibrations, channel checks and functional testing. The channel calibrations are performed during refueling outages when the PPS is not required to be operable. Calibration and testing will be performed according to plant specific approved procedures that establish specific surveillance techniques and surveillance intervals intended to maintain high reliability.

Manual surveillance testing verifies that the system components and connections have not failed or degraded, and that trip signal paths for safety functions are correct. Software itself does not "degrade" over time unless there is an associated hardware failure. Also, V&V confirms that the software is correct. Therefore, the purpose of surveillance testing is to validate system operability. The PLC internal diagnostic functions check the hardware integrity and supervise software integrity by CRC checks.

The test feedback of one division is displayed only by the MTP of that division. The ITP puts the data on the SDN for the MTP displays.

The PPS bypasses are initiated via channel bypass switches on the MTP switch panel.

lifecycle phase in the software development process conform to the requirements of that phase.

12. The cabinets listed in Table 2.5.1-1 have key locks and door open alarms, and are located in a vital area of the facility.

13. The RT logic of the PPS is designed to fail to a safe state such that a processor lock-up or loss of electrical power to a division of PPS results in a trip condition for that ~~division but the~~ ESFAS logic of the PPS is designed to fail to a safe state such that loss of electrical power to a division of PPS does not result in ESF initiation for that division.

division. The

14. Redundant safety equipment listed in Table 2.5.1-1 is provided with means of identification. by the hardware-based window watchdog timer (from the NRC-approved safety I&C platform) located in the processor module

15. The input signals of PPS through APC-S or ENFMS are derived from RT and ESF initiation measurement instrumentation that measures monitored variables identified in Tables 2.5.1-2 and 2.5.1-3.

16. The PPS provides RT and ESF initiation signals to meet the required response time for trip and initiation conditions identified in Tables 2.5.1-2 and 2.5.1-3.

17. The Class 1E equipment listed in Table 2.5.1-1 is protected from accident related hazards such as missiles, pipe breaks, and flooding.

18. The RTS and ESF system instrumentation (referenced in Tables 2.5.1-2 and 2.5.1-3) monitors the normal operating, anticipated operational occurrence (AOO), and postulated accident (PA) events.

19. The Class 1E instrument identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.

20. The PPS providing RT and ESF initiation signals has the testing function that can be initiated from the PPS MTP. This testing function verifies the functionality of the bistable processing logic and coincidence processing logic within the PPS.

Table 2.5.1-5 (8 of 12)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
11. (cont.)	11.e An inspection and analysis of the outputs including documentation of the test phase will be performed.	11.e The test phase outputs including documentation exist and conclude that the test phase activities are performed and these activities conform to the requirements of the test phase.
	11.f An inspection and analysis of the outputs including documentation of the installation and checkout phase will be performed.	11.f The installation and checkout phase outputs including documentation exist and conclude that the installation and checkout phase activities and performed and these activities conform to the requirements of the installation and checkout phase.
12. The cabinets listed in Table 2.5.1-1 have key locks and door open alarms, and are located in a vital area of the facility.	12.a A test of the as-built cabinets listed in Table 2.5.1-1 for key lock capability, and a test of door open alarms, will be performed.	12.a Each as-built cabinet listed in Table 2.5.1-1 has key locking capability, and alarms are received in the as-built MCR when cabinet doors are opened.
	12.b Inspection of the cabinets listed in Table 2.5.1-1 will be performed.	12.b The cabinets listed in Table 2.5.1-1 are located in a vital area of the facility.
e PPS is a safe state such that a processor lock-up or loss of electrical power to a division of PPS results in a trip condition for that ~~division but the~~ ESFAS logic of the PPS is designed to fail to a safe state such that loss of electrical power to a division of PPS does not result in ESF initiation for that division.	13. ~~A test will be performed by making a processor lock-up or disconnecting the electrical power to each division of the as-built PPS.~~	13. Each division of the as-built RT logic of the as-built PPS fails to a safe state upon a processor lock-up or loss of electrical power to the ~~division and does not result in ESF initiation.~~
14. Redundant safety equipment listed in Table 2.5.1-1 is provided with means of identification.	14. An inspection of the as-built equipment for conformance with the identification requirements will be performed.	14. The as-built equipment listed in Table 2.5.1-1 and related field equipment complies with the labeling and color coding requirements.

by the hardware-based window watchdog timer (from the NRC-approved safety I&C platform) located in the processor module

division. The

by operation of the hardware-based window watchdog timer (from the NRC-approved safety I&C platform) located in the processor module

Two separate tests will be performed. The first test simulates the processor lock up. The second test disconnects the electrical power to each division of the as built PPS.

division. Each division of the as-built ESFAS logic of the as-built PPS fails to a safe state upon loss of electrical power to the division such that the ESF does not initiate for that division.

9.a Once a NSSS ESF actuation has been actuated (automatically or manually), the ESF actuation logic is latched in the actuated state and is not reset automatically when the NSSS ESF initiating condition has been cleared. After the initiating condition has been cleared, the NSSS ESF actuation is manually reset.

9.b Once a BOP ESF actuation has been actuated (automatically or manually), the ESF actuation logic is latched in the actuated state and is not reset automatically when the ESF actuation signal has been cleared. Once the initiating condition is cleared, the ESF actuation is manually reset.

(1)

10. Loss of power or a processor lock-up in an ESF-CCS division results in the respective ESF-CCS division output assuming fail-safe output condition.

11. Manual ESF actuation switches are provided in the MCR and RSR for the ~~and the actuation of the hardware-based window watchdog timer from NRC-approved safety I&C platform in the ESF-CCS generates the alarm to prompt the operator action~~

12. The operator modules (OMs) in the MCR display ESF actuation status, manual ESF actuation status, and ESF-CCS status information including the test status for ESF actuations identified in Tables 2.5.4-2 and 2.5.4-3.

13. The component interface module (CIM) provides state-based priority logic to prioritize the ESF-CCS and diverse protection system (DPS) signals.

14. The CIM provides system-based priority logic for the front panel control switch signals on the CIM, the signals generated by the diverse manual ESF actuation (DMA) switches, the signals from the ESF-CCS, and the signals from the DPS. The front panel control switches have the highest priority, and the signals from the DMA switches have priority over signals from the ESF-CCS and DPS.

15. The application software for the ESF-CCS is implemented according to each lifecycle phase in the software development process : concept phase, requirement phase, design phase, implementation phase, test phase, and installation and checkout phase. The outputs including documentation, of each lifecycle phase in the software development process conform to the requirements of that phase.

16. The ESF-CCS equipment and components identified in Table 2.5.4-1 withstand the electrical surge, electromagnetic interference (EMI), radio-frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist

and (2) the relay output of the hardware-based window watchdog timer (from the NRC-approved safety I&C platform) being energized and generating the alarm to prompt operator action.

Table 2.5.4-5 (5 of 11)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
9.b Once a BOP ESF actuation has been actuated (automatically or manually), the actuation logic is latched in the actuated state and is not reset automatically when the BOP ESF actuation signal has been cleared. Once the initiating condition is cleared, the BOP ESF actuation is manually reset.	9.b.i A test will be performed by returning simulated signals to a level within the predetermined limits of plant process signals at the as-built RMS input for BOP ESFAS functions as identified in Tables 2.5.4-2 and 2.5.4-3 after simulating the BOP ESF actuation.	9.b.i Each BOP ESF actuation signal of the as-built ESFCCS remains upon return of simulated signals to a level within the predetermined limits of plant process signals for BOP ESFAS functions as identified in Tables 2.5.4-2 and 2.5.4-3 after simulating the ESF actuation.
	9.b.ii A Test of the as-built BOP ESFAS reset function is performed manually to reset the actuated BOP ESFAS function.	9.b.ii The BOP ESF actuation is manually reset once the initiating condition is cleared.
10. Loss of power or a processor lock-up in an ESF-CCS division results in the respective ESF-CCS division output assuming fail-safe output condition.	10. ~~A test will be performed simulating loss of power or a processor lock-up in each as-built ESF-CCS division.~~	10. Loss of power or a processor lock-up in each ESF-CCS division results in the assumed fail-safe output condition.
11. Manual ESF actuation switches are provided in the MCR and RSR for the manual ESF actuations identified in Table 2.5.4-3.	11. A test will be performed to verify the actuation of the as-built ESF-CCS manual ESF actuation using the manual ESF actuation switches in the MCR and RSR.	11. Each as-built ESF-CCS manual ESF actuation identified in Table 2.5.4-3 actuates upon receipt of a signal from its respective manual ESF actuation switches in the MCR and RSR.
12. The operator modules (OMs) in the MCR display ESF actuation status, manual ESF actuation status, and ESF-CCS status information including the test status for ESF actuations identified in Tables 2.5.4-2 and 2.5.4-3.	12. A test of the as-built OM in the MCR will be performed to demonstrate the display capability.	12. Each as-built OM in the MCR displays ESF actuation status, remote manual ESF actuation status, and ESF-CCS status information including the test status for actuations identified in Tables 2.5.4-2 and 2.5.4-3.

(1)

(1)

(2)

relay output

the

and the ~~actuation~~ of the hardware-based window watchdog timer from NRC-approved safety I&C platform ~~in the ESF-CCS generates~~ the alarm to prompt the operator action

~~energizing the hardware-based window watchdog timer from NRC-approved safety I&C platform due to the~~

being energized and generating

being energized and generating the alarm to prompt operator action.

and relay output of the hardware-based window watchdog timer from NRC-approved safety I&C platform ~~is energized for generating alarms~~

the

(2)

Two separate tests will be performed. The first test simulates the processor lock up. The second test disconnects the electrical power to each division of the as-built ESF-CCS.

Table 7.2-7 (1 of 25)

Failure Modes and Effects Analysis for the Plant Protection System

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
1-1	Ex-core neutron flux detector	a) Low output	Loss of high power supply source	• Data loss • Incorrect data • Detection failure of high neutron flux level	• Alarm: comparison of three channels • Periodic test	Three-channel redundancy	The resulting reactor trip coincidence logic on variable overpower, high logarithmic power, DNBR/LPD becomes 2-out-of-2 coincidence logic.	Loss of high power supply makes all three sub-channel detectors not work properly. Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) High output	• Short circuit of detector • Continuous ionization	Channel trip can occur due to variable overpower, low DNBR, high logarithmic power level or high LPD.	Occurrence of pre-trip and trip alarm for variable overpower, low DNBR, high logarithmic power level, or high LPD.	Three-channel redundancy	The resulting reactor trip coincidence logic on variable overpower, high logarithmic power, DNBR/LPD becomes 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
1-2	Pressurizer pressure (wide range)	a) One signal turns on due to failure (high level signal)	• Sensor failure • Component failure	• High-level pressure signal is input to bistable logic. • Low pressurizer pressure bistable logic does not generate trip under trip condition.	• Alarm: comparison of three channels • Periodic test	Three-channel redundancy	The resulting coincidence logic for reactor trip, CIAS, and SIAS becomes 2-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) One signal turns off due to failure (low level signal)	• Sensor failure • DC power supply failure • Open circuit	• Low-level pressure signal input to bistable logic. • Low pressurizer pressure bistable logic initiates channel trip.	Occurrence of pre-trip and trip alarm for low pressurizer pressure channel	Three-channel redundancy	The resulting coincidence logic for reactor trip, CIAS and SIAS becomes 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
1-3	Pressurizer pressure (narrow range)	a) Signal turns on (high level signal)	• Sensor failure • Component failure	• High-level pressure signal is input to bistable logic. • High pressurizer pressure bistable logic initiates channel trip.	Occurrence of pre-trip and trip alarm for high pressurizer pressure channel	Three-channel redundancy	• The resulting reactor trip coincidence logic on low DNBR becomes 2-out-of-2 coincidence logic. • The resulting reactor trip coincidence on high pressurizer pressure becomes 1-out-of-2 coincidence logic. • The resulting CWP coincidence logic on high pressurizer pressure becomes 1-out-of-2 coincidence logic.	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.
		b) Signal turns off (low-level signal)	• Sensor failure • DC power supply failure • Open circuit	• Low-level pressure lowers margin of DNBR and initiates low DNBR channel trip. • High pressurizer pressure bistable logic does not generate trip under trip condition.	Occurrence of pre-trip and trip alarm for low DNBR channel	Three-channel redundancy	• The resulting reactor trip coincidence logic on low DNBR becomes 1-out-of-2 coincidence logic. • The resulting reactor trip coincidence logic on high pressurizer pressure becomes 2-out-of-2 coincidence logic. • The resulting CWP coincidence logic on high pressurizer pressure becomes 2-out-of-2 coincidence logic	Operator has to bypass the channel in failure after restoring the bypassed channel to operating state in order to restore the system logic to 2-out-of-3 coincidence logic.

~~The "watchdog timer" or "WDT" described in Table 7.2-7 refers to the "window watchdog timer".~~
~~See Section 5.2.1.3 of Common Qualified Platform Topical Report listed as Reference 77 in Section 7.1.5.~~

VOID

Table 7.2-7 (25 of 25)

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
39	MTP / ITP cabinet power supply auctioneering circuit applicable to all cabinet power supplies: 24 VDC	a) Open diode	Overload, component failure	• One supply is not available to power the downstream components in the affected cabinet. • No loss of DC circuit functionality	Annunciation – one of the auctioneered power supplies is offline.	The companion power supply/diode combination supplies power to the components receiving power from the supply.	No loss of safety function	N/A
		b) Shorted diode	Overload, component failure	• The voltage applied to the components in the cabinet are the same as the voltage at the supply terminals. • No loss of DC circuit functionality	Periodic test	Each power supply in the auctioneered pair is capable of providing power to all of the components.	No loss of safety function	N/A
40	MTP / ITP cabinet power supply auctioneering circuit applicable to 24 VDC cabinet power supply	Overvoltage	Component failure	• Overvoltage device detects and removes voltage to the connected load. • Lose ITP station • No SDL or SDN activity	Receiving stations for SDLs and SDN networks detect loss of update and alarm.	ITP in other three safety divisions operable	• No loss of safety function. • Some PPS screens on MTP and OM not updated.	N/A
41	MTP / ITP cabinet power supply auctioneering circuit applicable to 24 VDC I/O power supplies	Overvoltage	Component failure	Dominant voltage is present on the loads.	Periodic test	Components operate to qualified conditions.	No effect on PPS safety function	N/A
42	MTP / ITP cabinet primary ac feed breaker for MTP	Breaker opens on overload.	Component failure	MTP ac transfer relay de-energizes and provides alternate vital ac to MTP via relay contacts.	Indicator on relay module not illuminated.	Two vital ac sources provided for powering MTP / ITP cabinet.	No loss of safety function	N/A
43	MTP / ITP cabinet alternate ac feed breaker for MTP	Breaker opens while powering the MTP.	Component failure	• Alternate vital ac lost to MTP • MTP is not available as it normally operates from primary vital ac.	Stations on SDN detect loss of updates from MTP and generate an alarm.	MTPs operating in three other safety divisions.	Loss of MTP function with PPS in the safety division	N/A
44	MTP ac transfer relay	a) Relay coil opens.	Component failure	MTP ac transfer relay de-energizes and provides alternate vital ac to MTP via relay contacts.	Indicator on relay module not illuminated.	Two vital ac sources provided for powering MTP.	No loss of safety function	N/A
		b) One relay contact position not in agreement with coil state.	Mechanical failure	The neutrals of the vital ac feeds are independent, so a failure in the relay contact, which switches the lines or neutrals, results in the loss of vital ac to the MTP.	Stations on SDN detect loss of updates from MTP and generate an alarm.	Three other safety divisions operating.	Lose MTP function with PPS in the safety division	N/A
45	Trip circuit breaker (TCB) of RTSG	1) Open	• Loss of 125Vdc control power • Unwanted energizing of UV coil • Mechanical failure of TCB	The RTSG opens.	• Alarm • Indication on the MTP and OM in the MCR	The RTSGs in other divisions are not affected.	The resulting logic of RTSGs becomes 1-out-of-3.	
		2) Closed	• Mechanical failure of TCB • Failure of UV coil • Short contact of TCB	The RTSG cannot be opened.	Periodic test	The RTSGs in other divisions are not affected	The resulting logic of RTSGs becomes 2-out-of-3.	

(1) FMEA assumes that all trip parameters in one channel are already bypassed. The inherent compensating provisions and effects are described based on this assumption.

(2) Pre-selected PF : Penalty factor which is selected to initiate plant trip for two CEACs fail condition

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

(4) The "watchdog timer" or "WDT" described in Table 7.2-7 refers to the "window watchdog timer". See Section 5.2.1.3 of Common Qualified Platform Topical Report listed as Reference 77 in Section 7.1.5.