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.:	**356-7881**
Review Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	**7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-3

Describe the diagnostic programs used to test digital computer channels in the APR1400 design.

As required by 10 CFR 50.55a(h)(3), IEEE Std. 603-1991, Clause 5.7, states, in part, that 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. APR1400 FSAR Tier 2, Chapter 16, Section 1.1, "Definitions" states with regard to the Channel Functional Test, in part,

> *"Digital Computer channels - the use of diagnostic programs to test digital computer hardware and the injection of simulated process data into the channel to verify OPERABILITY, including alarms and trip functions."*

1. Describe the diagnostic programs used for testing. Specifically, what are these programs? How do they help to ensure operability of safety system components?

2. Describe the testing process or describe where in the application the testing process is explained in detail.

3. How does the design ensure that there is adequate independence such that injected signals are only received by the channel being tested and not to other channels on the safety system data network?

4. How does the design ensure that online testing does not result in an unplanned component or spurious actuation of a component(s) while testing is being performed?

Response

1. The diagnostic programs used to monitor the integrity of the hardware are addressed in the response to RAI 356-7881 Question No. 07-1. This consists of the automatic self-test functions provided by the AC160 module self-diagnostics and the application automatic self-checking features which are discussed in the response to both RAI 356-7881 Questions 07-1 and 07-2.

   Surveillance testing provisions for the reactor protection system (RPS) are provided by the set of overlap tests depicted in Figure 7.2-11, “PPS Testing Overlap” of DCD Tier 2 and Figure 4-6, “Overlap in Functional Testing for the PPS” of the Safety I&C System technical report, APR1400-Z-J-NR-14001, Rev. 0.

   The starting point of a test, as depicted in the figures identifies the entry point in the signal path where a test signal specified by the maintenance and test panel (MTP) is injected into the signal path. The endpoint of a test depicts the point in the signal path where monitoring signals representing the results of system processing are provided, which can be observed on the MTP flat panel display (FPD).

   Surveillance testing provisions for the engineered safety features (ESF) are provided by a combination of the overlap tests identified in Figure 7.2-11 of DCD Tier 2 and the test logic depicted in Figure 7.3-22, “ESF-CCS Simplified Test Logic Diagram” (to cover the signal path through the engineered safety features – component control system (ESF-CCS) group controllers) of DCD Tier 2.

   Operation of the overlap tests identified in Figure 7.2-11 of DCD Tier 2 is accomplished by observation/comparison of the redundant process inputs to the PPS from each channel, replacement of the actual inputs or intermediate calculations with test signals which follow the same signal path as the input or calculated signals, and observation of the results of the system processing associated with the injected test signals.

   Operation of the test logic depicted in Figure 7.3-22 of DCD Tier 2 is accomplished by injection of test signals into the normal signal path of the ESF-CCS group controllers and observation of monitoring points provided to the MTP FPD.

   Therefore, the proper operation of the safety system components is assured by a combination of:

   - No diagnostic error messages (hardware operating properly),
   - No CRC changes on the AC160 processor modules (software has not changed)
   - The injected test signals utilize the same path as actual signals (tests actual logic)
   - The monitored response is the expected response (logic is correct)

   This approach is described and approved in the Common Qualified Platform Topical Report.

2. Section 4.2.2.2, “Manual Testing Features” of the Safety I&C System technical report provides the specific tests that can be initiated and performed during plant power

operation as well as during plant shut down. These tests are initiated from the MTP FPD over division paths that range from sensor inputs to the reactor trip switchgear system (RTSS) or the input of the ESF-CCS as shown in Figure 4-6, “Overlap in Functional Testing for the PPS” of the Safety I&C System technical report. Also, Section 7.2.2.5 of DCD Tier 2 provides descriptions of the specific types of tests used to verify the integrity of the PPS and the CPCS and the trip path from the sensor input to the reactor trip switchgear. As shown in Figure 7.2-11, “PPS Testing Overlap” of DCD Tier 2, the PPS test is performed over the overlap test area to verify the functionality of the entire PPS.

Operation of these tests is accomplished by observation of redundant process sensor inputs from each channel on the MTP FPD, injection of MTP specified test signals into the PPS signal path, and observation of monitoring points provided on the MTP FPD.

3. The MTP and interface and test processor (ITP) are used to support the periodic testing of the safety I&C system. Tests are initiated from the MTP FPD. The test injection signals are provided by the MTP or ITP, and the tests provide monitoring points (i.e. test feedback) that can be displayed on the MTP FPD. Sections 7.2.2.5 and 7.3.2.5 of DCD Tier 2 state that the test equipment consists of divisionalized MTP, ITP, and the associated interface circuits.

   The safety system data network (SDN) is used to communicate test injection signals and monitoring points (i.e. test feedback). Section 4.6.2.2 of the Safety I&C System technical report states that the SDN is contained within a division and does not cross safety division boundaries. The architectural design of the SDN does not provide for cross-division communication. Therefore, test injection signals transmitted by the MTP or ITP cannot be received by a process station in a different channel than the transmitting MTP or ITP.

4. Testing during plant power operation is performed through the periodic functional test, which is administratively controlled in accordance with the Technical Specifications.

   As described in Section 7.2.2.5 of DCD Tier 2, the system test does not affect the protective functions and meets the guidance of IEEE Std. 338, which is endorsed by NRC RG 1.118. The testing also complies with RG 1.22. In addition, Section 3.2, item j. of the Safety I&C System technical report provides analysis regarding GDC 21, “Protection System Reliability and Testability.”

   The channel bypass is required to be applied to the trip parameter(s) to be tested in a channel which is undergoing testing. This procedure prevents any safety related components or devices from operating in an unintended way due to the test signals.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

There is no impact on any Technical, Topical or Environmental Report.

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.:	**356-7881**
SRP Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	**7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-5

Describe the I&C and its supporting features (e.g. location of equipment, power sources, etc.) for the remote control center (RCC) in the APR1400 design.

General Design Criteria (GDC) 19 requires, in part, that equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

Regarding the RCC, the applicant states in APR1400 FSAR Tier 2, Section 7.7.1.1, "Conrol Systems," subsection o.3)c), the RCC has minimum equipment necessary to maintain the plant for 24 hours to accomplish hot standby. The applicant also states that the RCC is located separately from the main control room (MCR) so that aircraft impact to the MCR does not adversely affect the RCC. The applicant goes on to state that the RCC panels have divisionalized control of safety and non-safety controls to achieve plant hot shutdown. In Section 7.7.1.2, "Main Control Room Facility," the applicant states the MCR and remote shutdown room (RSR) both meet the requirements of GDC 19, but makes no mention of the RCC. In Section 7.7.1, "Description," of FSAR Tier 2, the applicant states that the RSR is subject to the human factors engineering process described in Chapter 18 of the APR1400 FSAR Tier 2 but does not mention a similar design commitment for the RCC.

The applicant mentions that the RCC has safety and non-safety related controls available but does not state that RCC complies with any other applicable requirements for this configuration such as independence. The RCC is not depicted on Figure 7.1-1, “APR1400 I&C System Overview Architecture,” therefore, there is no physical depiction of how the functionality of the RCC is taken into account within the overall I&C architecture or how its implemented. The acronym for the remote control center is also not defined in the acronym and abbreviation list in Section 7.0 of FSAR Tier 2. It cannot be determined what the difference is between the RCC and RSR.

1. Describe the RCC including all instrumentation, controls, and displays available at the RCC, all communications and architectural details used to implement the RCC, how the RCC addresses all the applicable requirements to the RCC (i.e. Independence), the specific design functions the RCC is intended to meet, the locations of RCC equipment (i.e. I&C cabinets, if applicable).

2. What is the difference between the RCC and the RSR?

3. Have the controls and displays available at the RCC been designed using the human factors engineering process as described in Chapter 18?

Response

1. The remote control center (RCC) is designed with the following design features:

   1) The RCC provides manual control and monitoring means to bring the plant to hot standby under accident conditions.

   2) The RCC is manipulated by one reactor operator who monitors and controls the plant.

   3) For control and monitoring, the RCC provides four divisionalized engineered safety features (ESF) component control system (CCS) soft control modules (ESCMs) for safety component control and process monitoring. Conventional hardwired switches, related indicators, and non-safety component control are also provided.

   4) The ESCMs and conventional switches in the RCC are physically separated from the MCR and RSR. These ESCMs are connected to the ESF-CCS loop controller (LC) in the remote multiplexer (MUX) room through a dedicated route which is separated from the routes of the main control room (MCR) and the remote shutdown room (RSR). The conventional switches are connected to the P-CCS cabinets in the remote MUX room through a dedicated route. This route also is separated from the routes of the MCR and the RSR.

   5) No single credible event that would require the concurrent evacuation of the MCR and the RSR (or fire damage in the MCR and RSR) would make the RCC inoperable.

   6) The ESF-CCS LCs and P-CCS LCs that are related with plant hot shutdown are interfaced with the RCC panel.

   7) MCR/RCC transfer switches are located in the MCR. MCR/RCC transfer switches are provided for safety division A, B, C, D, and the non-safety division. One transfer switch is provided for each division of ESF-CCS LC and each division of P-CCS LC, respectively. These transfer switches disconnect signal paths between the ESCMs in the MCR and the RSR and ESF-CCS LC in the remote MUX room.

   8) The RCC panel room is located on the opposite side of the plant from the MCR and the RSR so that an aircraft impact cannot affect the MCR, RSR, and the RCC panel.

2. The RSR is designed to achieve safe shutdown outside of the MCR in the unlikely event that the MCR becomes uninhabitable, in conformance with GDC 19. Displays and controls

on the remote shutdown console in the RSR are the same type as those on the consoles of the MCR.

The RCC panel is designed as a supplemental facility to accommodate the aircraft impact event. This panel is to provide manual control and monitoring means to bring the plant to hot shutdown in the unlikely event of an aircraft impact. The RCC panel is designed as non-safety class.

3. The controls and displays available at the RCC have been designed according to the guidelines in NUREG-0700, “Human-System Interface Design Review Guidelines.” The RCC has not been specifically described in Chapter 18; however, design of the RCC will follow the NUREG-0711, human factors engineering process as a local control station facility.

DCD Tier 2, Section 7.0 and Section 7.7.1.1 will be revised, and the depiction of the I&C architecture of the RCC will be added as Figure 7.7-14, as indicated in the attachment associated with this response.

Impact on DCD

DCD Tier 2, Sections 7.0 and 7.7.1.1 will be revised, and Figure 7.7-14 will be added, 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.

NA	not applicable
NIMS	NSSS integrity monitoring system
NPCS	NSSS process control system
NRC	Nuclear Regulatory Commission
NSSS	nuclear steam supply system
OM	operator module
OSC	operational support center
P&ID	piping and instrumentation diagram
PA	postulated accident
PC	personal computer
P-CCS	process-component control system
PCS	power control system
PF	penalty factor
PLC	programmable logic controller
PLCS	pressurizer level control system
PM	processor module
POSRV	pilot operated safety relief valve
PPCS	pressurizer pressure control system
PPS	plant protection system
PRV	process representative value
PS	processing section
PSCEA	part-strength CEA
PZR	pressurizer
QA	quality assurance
QAPD	quality assurance program description
QIAS	qualified indication and alarm system
QIAS-N	qualified indication and alarm system – non-safety
QIAS-P	qualified indication and alarm system – P
RAM	random access memory
RCC	remote control ~~console~~ center

the sump provides an alarm in the MCR to alert the operator of the presence of water in that area.

b) Hydrogen mitigation system

The HMS allows adiabatic, controlled burning of hydrogen at low concentrations during degraded core accident conditions. Divisionalized HMS igniters are manually actuated from the MCR.

The HMS controls and instrumentation are described in Subsection 6.2.5. Electrical power distribution is described in Section 8.3.

c) Remote control center

The RCC is designed against aircraft impact to meet the requirements of 10 CFR 50.150 (Reference 11). The minimum equipment needed to maintain the reactor for 24 hours is provided to accomplish hot standby plant condition. The operator can shut down the reactor from the MCR 10 minutes before aircraft impact upon the MCR in the auxiliary building, and the control and monitoring is transferred to the RCC using a transfer switch located in the MCR. The RCC is located separately from the MCR so that aircraft impact to the MCR does not adversely affect the RCC operation integrity.

The RCC panel consists of divisionalized safety control and non-safety controls to achieve plant hot shutdown. The signals from the RCC are routed from the RCC to the I&C equipment room as well as to the motor control center (MCC) through multiplexers.

Insert "A" on following page

7.7.1.2 Main Control Room Facility

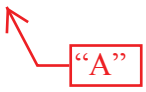
The MCR facilities are composed of the following major functional units:

a. The MCR includes the MCR operator consoles, a large display panel (LDP), safety console, and an adjacent meeting room.

b. The computer room contains the IPS that monitors plant performance, drives various display units, and logs plant data.

The remote control center (RCC) is designed with the following design features:
- The RCC provides manual control and monitoring means to bring the plant to hot standby under accident conditions.
- The RCC is manipulated by one reactor operator who monitors and controls the plant.
- For control and monitoring, the RCC provides four divisionalized engineered safety features (ESF) component control system (CCS) soft control modules (ESCMs) for safety component control and process monitoring. Conventional hardwired switches, related indicators, and non-safety component control are also provided.
- The ESCMs and conventional switches in the RCC are physically separated from the MCR and RSR. These ESCMs are connected to the ESF-CCS loop controller (LC) in the remote multiplexer (MUX) room through a dedicated route which is separated from the routes of the main control room (MCR) and the remote shutdown room (RSR). The conventional switches are connected to the P-CCS cabinets in the remote MUX room through a dedicated route. This route also is separated from the routes of the MCR and the RSR.
- No single credible event that would require the concurrent evacuation of the MCR and the RSR (or fire damage in the MCR and RSR) would make the RCC inoperable.
- The ESF-CCS LCs and P-CCS LCs that are related with plant hot shutdown are interfaced with the RCC panel.
- MCR/RCC transfer switches are located in the MCR. MCR/RCC transfer switches are provided for safety division A, B, C, D, and the non-safety division. One transfer switch is provided for each division of ESF-CCS LC and each division of P-CCS LC, respectively. These transfer switches disconnect signal paths between the ESCMs in the MCR and the RSR and ESF-CCS LC in the remote MUX room.
- The RCC panel room is located on the opposite side of the plant from the MCR and the RSR so that an aircraft impact cannot affect the MCR, RSR, and the RCC panel.

The I&C system architecture for the RCC panel is shown in Figure 7.7-14



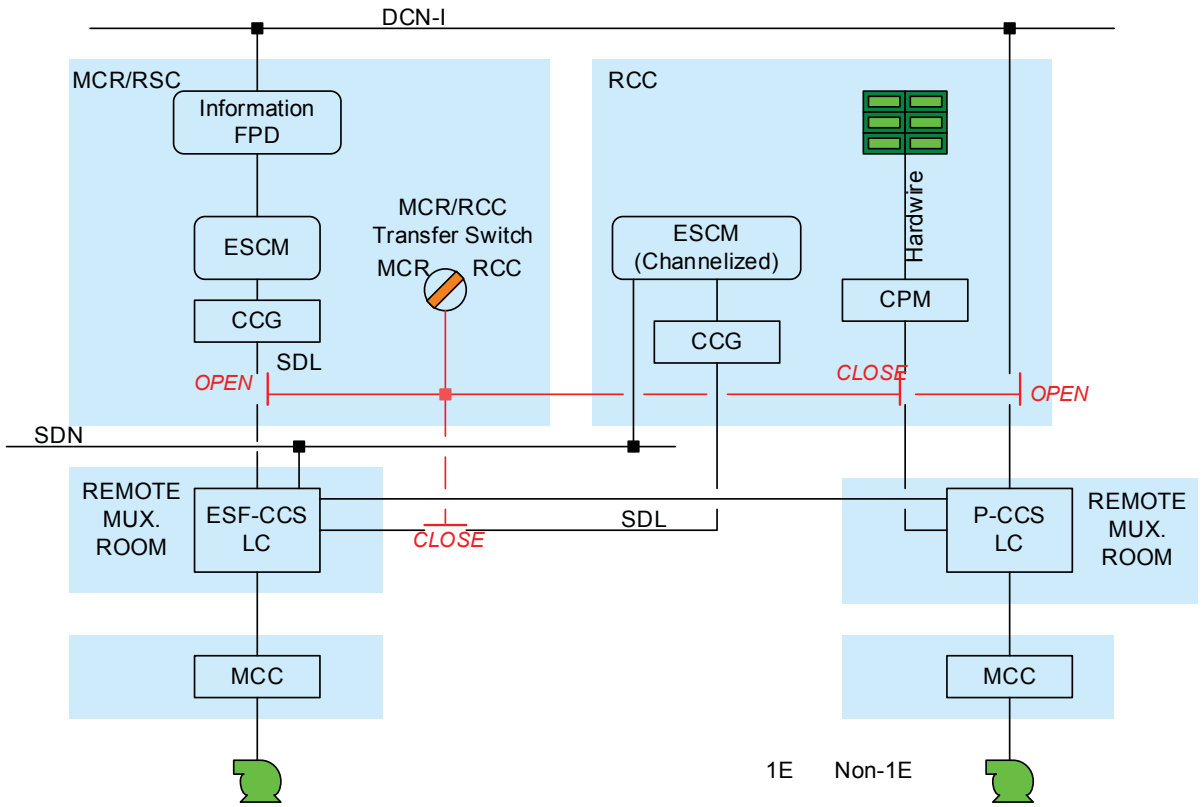


Figure 7.7-14 I&C System Architecture for the RCC Panel

Added

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.:	**356-7881**
SRP Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	**7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-8

Clarify the design statement regarding embedded digital devices in both safety and non-safety components.

10 CFR 50.55a(h)(3) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, the safety system design shall be such that credible failure in, and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. The applicant makes a statement with regard to embedded devices in field equipment in the second paragraph of Section 4.10, "CCF Analysis of Embedded Devices in Field Eqiupment," of APR1400-Z-J-NR-14012-P, "Control System CCF Analysis," Revision 0.

1. Does the applicant imply that embedded devices contained in non-safety components are diverse from the embedded devices contained within safety-related components?

2. Provide analysis or further description demonstrating that embedded devices within nonsafety components are different or diverse from embedded devices in safety-related components.

3. Provide a summary of all types of components that will have embedded digital technology. Identify the functionality provided by the embedded technology for these components.

4. For embedded digital devices contained within safety-related components, has the applicant evaluated the potential consequences of a software CCF for these components?

Response

TS

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

Section 4.10 of technical report APR1400-Z-J-NR-14012-NP, Rev. 0, “Control System CCF Analysis” will be revised as indicated in the attachment associated with this response.

4.10. CCF Analysis of Embedded Devices in Field Equipment

TS

4.10.1. Evaluation for the CCF of Non-safety Field Instruments

4.10.2. Evaluation for the CCF of Non-safety Field Actuators

4.10.3. Evaluation for the Effect on Field Instruments due to Controller Failures

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.:	**356-7881**
SRP Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	**7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-13

Describe the environmental protections (e.g. high temperature equipment alarms or cooling) for the Power Control System (PCS), Process – Component Control System (P-CCS) and DAS.

10 CFR 50.55a(h)(3) requires compliance to IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. Standard review plan Section 7.7 states, in part, that I&C systems should include protection from environmental extremes. APR1400 FSAR Tier 2, Section 7.7.1.4.c, states that, for Information Processing System (IPS) cabinets, temperature switches and alarms exists to protect against high temperature conditions and to alert operators to the potential high temperature condition. Section 7.7 does not address similar design functionality for cabinets containing equipment that comprises the PCS, P-CCS and DAS. FSAR Tier 2, Section 9.4, "Heating, Ventilation and Air Conditioning Systems," does not appear to provide specific information on the cabinets for these systems as well.

1. Describe the environmental protection design attributes for the cabinets (and rooms that contain these cabinets) for the PCS, P-CCS and DAS systems (i.e. high temperature protections and alarms).

2. Do the safety I&C systems have similar equipment cabinet environmental protective design features as the non-safety equipment cabinets?

Response

1. The non-Class 1E cabinets for power control system (PCS) and process-component control system (P-CCS) are designed and fabricated to operate without loss of function for the following environmental conditions of the room:

   - Temperature (°F) — 50-104 °F in auxiliary building area; 70-77 °F in non-safety I&C equipment rooms; 65-85 °F for DRCS power cabinets of PCS
   - Relative humidity (%) — 7-90 % in auxiliary building area; 40-60 % in non-safety I&C equipment rooms; 40-60 % for DRCS power cabinets of PCS
   - Radiation (Gy) — Negligible

   The non-Class 1E cabinets for diverse protection system (DPS) and diverse indication system (DIS) are located in the non-safety I&C equipment rooms and designed and fabricated to operate without loss of function for the following environmental conditions of the room:

   - Temperature (°F) — 70 – 77 °F
   - Relative humidity (%) — 40 – 60 %
   - Radiation (Gy) — Negligible

   For these cabinets, the cooling and ventilation are provided by a fan mounted in the cabinet. Each cabinet contains a temperature sensor in the cabinet that is monitored. The fans are designed for continuous operation when the cabinet is powered. Though an alarm for loss of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided.

2. The Class 1E cabinets located in the main control room and safety I&C equipment rooms are designed and fabricated to operate without loss of function when exposed to the environmental design requirements specified in Table 6-1 of APR1400-Z-J-NR-14001-P, Rev. 0, “Safety I&C System.”

   The Class 1E cabinets located in the auxiliary building area except main control room and safety I&C equipment rooms are designed and fabricated to operate without loss of function when exposed to the following environmental conditions:

   - Temperature (°F) — 50-104 °F
   - Relative humidity (%) — 7-90 %

- Radiation (Gy) ≤ 10 Gy (Gamma)

For these cabinets, the cooling and ventilation are provided by a fan mounted in the cabinet. Each cabinet contains a temperature sensor in the cabinet that is monitored. The fans are designed for continuous operation when the cabinet is powered. Though an alarm for loss of the fan is not provided, trouble alarms to indicate a high temperature in the cabinet are provided.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

There is no impact on any Technical, Topical, or Environmental Report.

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.:	**356-7881**
Review Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	**7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-14

Describe the specific design and implementation of the watchdog timers (WDTs) for the APR1400 design.

As required by 10 CFR 50.55a(h)(3), IEEE Std. 603-1991, Clause 5.5, states the safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. APR1400 FSAR Tier 2, Table 7.2-7, "Failure Modes and Effects Analysis for the Plant Protection System," refers to the WDT for core protection calculator (CPC) processor module (PM), the auxiliary CPC PM and the control element assembly calculator. WDT functionality is also mentioned for the local coincidence logic (LCL) processors responsible for performing reactor trips on Item 10 of Table 7.2-7. For this item, the stated effect of the WDT action is that the open WDT contact trips one-half of the safety division reactor trip initiation circuit. This is for LCL failures modes such as application program memory failure or failed program execution. Chapter 7 of the APR1400 FSAR Tier 2 does not provide specific details on the implementation of the WDT design, such as that the WDTs are non-programmable hardware.

Section 4.2.2, "Design Features," of Technical Report APR1400-Z-J-NR-14001-P, Rev.0, ″Safety I&C System” states that each LCL reactor trip processor has a built-in WDT. Section 4.2.2 also states that the outputs of the WDT are hardwired in series to the RPS initiation circuits to ensure appropriate trip signals are generated, as shown on Figure 4-7, "Watchdog Timer for PPS," of this report. The applicant also points to "Common Qualified Platform Topical Report" for detailed information on WDT configuration. The applicant makes similar assertions regarding the CPCS on Figure 4-11, "Watchdog Timer for CPCS." Figure 4-16, "Watchdog Timer for ESF-CCS," depicts the WDT configuration for the ESF-CCS. Figure 4-7 does not appear to show the actual wiring of the WDT and how it initiates a RT. Figure 4-16 does not appear to show how the WDT initiates a fail-safe condition for ESF-CCS components. Section 4.2.2 of technical report APR1400-Z-J-EC-13001-P, revision 0, “Safety I&C System”, states the following:

"Each PPS LCL RT processor is supervised by the PLC watchdog timer."

According to the acronym definition list in APR1400-Z-J-EC-14001-P, Rev. 0, "PLC" stands for programmable logic controller. This would imply that, for the LCLs, the WDTs are implemented with programmable technology and it is not clear that this is only applicable to LCLs, based upon the applicant's description. This implementation would run counter to the guidance of SRP 7.1-D, which describes an acceptable methodology for meeting the criterion set forth in IEEE Std. 7-4.3.2-2003, which the applicant states the APR1400 design complies with. SRP 7.1-D, Section 5.7, states, in part, that a non-software WDT is critical in the overall diagnostic scheme of a computer system. A software-based WDT may be subject to the similar failure modes as the operating system it is intended to monitor, such as CCF, as described in BTP 7-19, for which the applicant states the APR1400 design complies.

1. Is the trip path for the WDT design, for both reactor trip and ESF-CCS, include any portion of the PPS or supporting systems that is dependent on software or other programmable technology to initiate a fail-safe condition?

2. Provide a clear consolidated figure that depicts the specific internal design of the WDT and its external connections and demonstrates how it is physically integrated into the systems that are applicable to its function (e.g. LCLs for reactor trip function) to perform its safety function, from detection of a system fault to outputs to reactor trip breakers for fail-safe actuation for ESF-CCS components.

3. Regarding WDT physical design, does the applicant consider the WDTs within the APR1400 design to be hardware components or software components, considering the WDTs for the LCLs are implemented using programmable technology?

4. Identify whether WDTs used in the APR1400 design are implemented with programmable technology or not. What technologies are used to implement WDTs that are not implemented with PLCs?

5. If the WDTs are implemented with programmable technology, has the applicant accounted for potential failure modes of the WDTs in the D3 analysis or control system CCF analysis?

Response

1. The trip path of the watchdog timer (WDT) design in the plant protection system (PPS) does not include any software dependent portion of the PPS or other programmable technology to initiate a fail-safe condition. As shown in Figure 4-7, “Watchdog Timer for PPS” of the Safety I&C System technical report, the output of the WDT upon processor module (PM) failure is directly transmitted to the reactor trip initiation circuit via the local coincidence logic (LCL) digital output (DO) module.

2. Figure 4-7, “Watchdog Timer for PPS” and Figure 4-16, “Watchdog Timer for ESF-CCS” of the Safety I&C System technical report will be revised to show a clear consolidated design of the WDT and to represent how the WDT output is interfaced with the intended protective system function.

   Figure 4-7 is supplemented in the similar way that Figure 4-11, “Watchdog Timer for CPCS” is shown: the WDT is triggered by the CPU. In addition, Note 4 will be added in Figure 4-7 to direct the reader to the specific sections of the Common Q_{TM} Platform Topical Report where the detailed information regarding the WDT located in the Processor Module (PM) is described.

   The WDTs in the engineered safety features – component control system (ESF-CCS) are not used to initiate a fail-safe condition for ESF-CCS components, but is used for alarming and indication on the information flat panel display (IFPD) and qualified indication and alarm system – non-safety (QIAS-N) flat panel display (FPD). This information will be added to Section 4.4.3.1 and Figure 4-16 of the Safety I&C System technical report.

3. All the WDTs used by the APR1400 safety systems are identical and have the same operating mechanism. The WDTs are provided by a common Programmable Logic Controller (PLC) platform. This is the Common Q_{TM} platform which is referenced by Reference 12 of the Safety I&C System technical report.

   The WDTs are internal to the PM and are supported by the firmware of the PM, which is part of the Common Q_{TM} platform. The Common Q_{TM} platform has been accepted by the NRC for use in safety-related I&C applications in nuclear power plants. An interface to the watchdog function is provided by an output relay. The output relay is a hardwired component located on the PM.

   In summary, the WDTs mentioned in the following sections of the Safety I&C System technical report and DCD Tier 2 are a hardware component:
   - Safety I&C System technical report, Section 4.2, “Plant Protection System”
   - Safety I&C System technical report, Section 4.3, “Core Protection Calculator System”
   - Safety I&C System technical report, Section 4.4, “Engineered Safety Features – Component Control System”
   - DCD Tier 2, Table 7.2-7, “Failure Modes and Effects Analysis for the Plant Protection System”

- DCD Tier 2, Table 7.3-8, “Failure Modes and Effects Analysis for the Engineered Safety Features – Component Control System”

4. As provided in Response 3 of this RAI, the WDTs are provided by the Common Q_{TM} platform described in Reference 12 of the Safety I&C System technical report. The WDTs which are internal to the PM are supported by the firmware of the PM, which is part of the Common Q_{TM} PLC.

   On-line diagnostics in the PM verify proper operation of the WDT as identified in Subsection 4.1.1.2.1, and as described in the proprietary portion of Subsection 5.2.1.2.1 of Reference 12 of the Safety I&C System technical report.

   The interface to the watchdog function is provided by an output relay which is a hardware component located on the Common Q_{TM} PM. This output relay on the PM is used to annunciate failures or set outputs to a default fail-safe state.

5. As identified in the response to Question 4 of this RAI, the WDTs used in the APR1400 design are part of the Common Q_{TM} PLC platform. This platform has been accepted by the NRC for use in safety related I&C applications in nuclear power plants, as identified in the Safety Evaluation by The Office Of Nuclear Reactor Regulation attached to Reference 12 of the Safety I&C System technical report. The interface to the watchdog function is provided by an output relay which is a hardware component located on the Common Q^{TM} PM.

   The Diversity and Defense-in-Depth technical report provides the design description of the diverse actuation system (DAS) which consists of the diverse protection system (DPS), diverse indication system (DIS), and diverse manual ESF actuation (DMA) switches. Section 4.1 of the Diversity and Defense-in-Depth technical report states that the DPS and DIS are implemented on a FPGA-based logic controller (FLC), which is diverse from the common safety PLC platform. It also states that the DIS display is implemented on a non-safety flat panel display (FPD) which is diverse from the common safety PLC platform and that the DMA switches are implemented by conventional switches, which are diverse from the common safety PLC platform.

   In summary, the DAS is implemented on a platform that is diverse from the common safety PLC platform.

   Therefore, potential failures of the WDTs used in the APR1400 safety systems do not impact the DAS and do not need to be addressed in the D3 or control system CCF analysis.

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

Section 4.4.3.1, Figure 4-7, and Figure 4-16 of the Safety I&C System technical report, APR1400-Z-J-NR-14001, Rev. 0 will be revised, as indicated in the attachment associated with this response.

TS

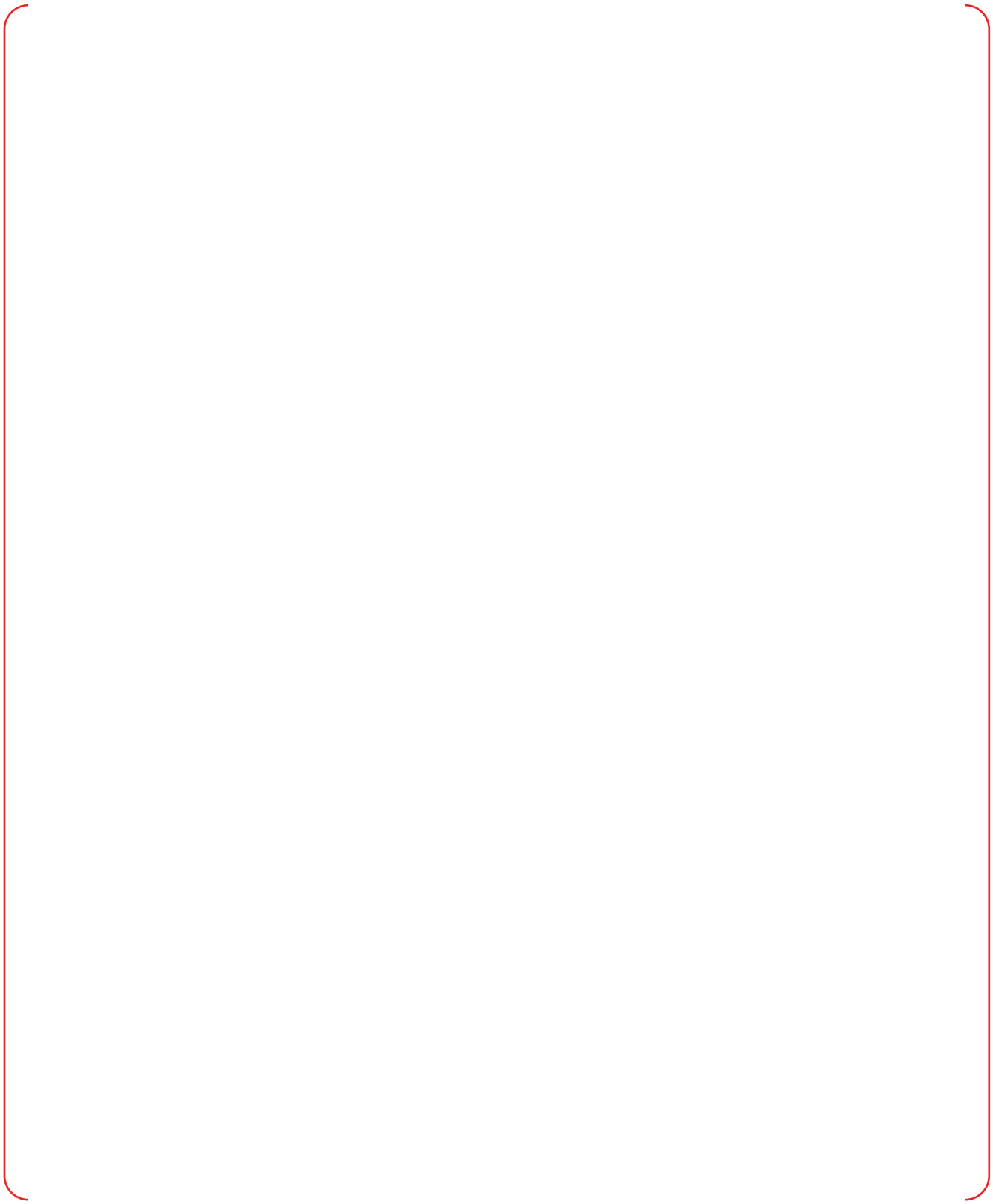
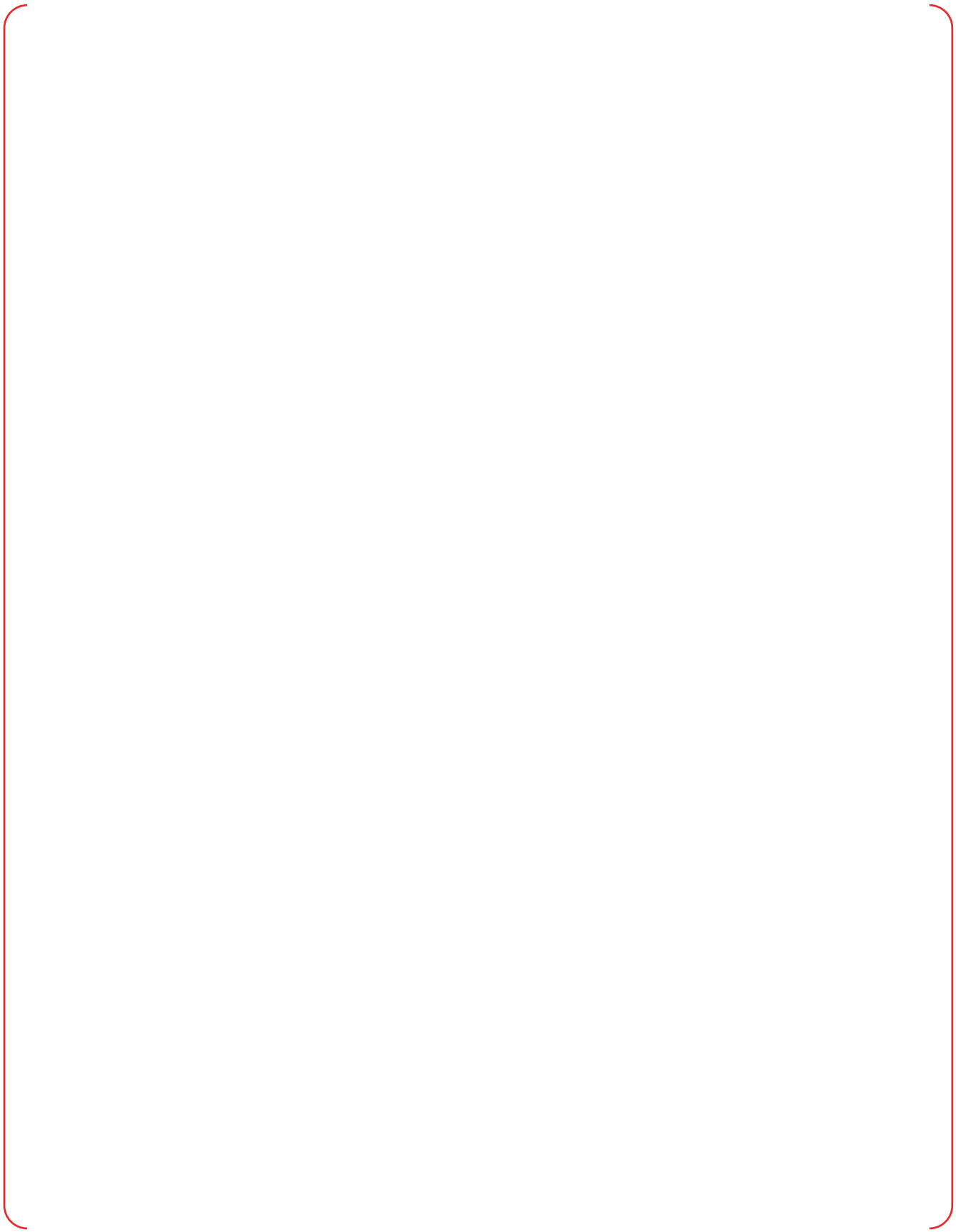


Figure 4-7 Watchdog Timer for PPS

Replace this figure with the figure on the next page.

TS



TS

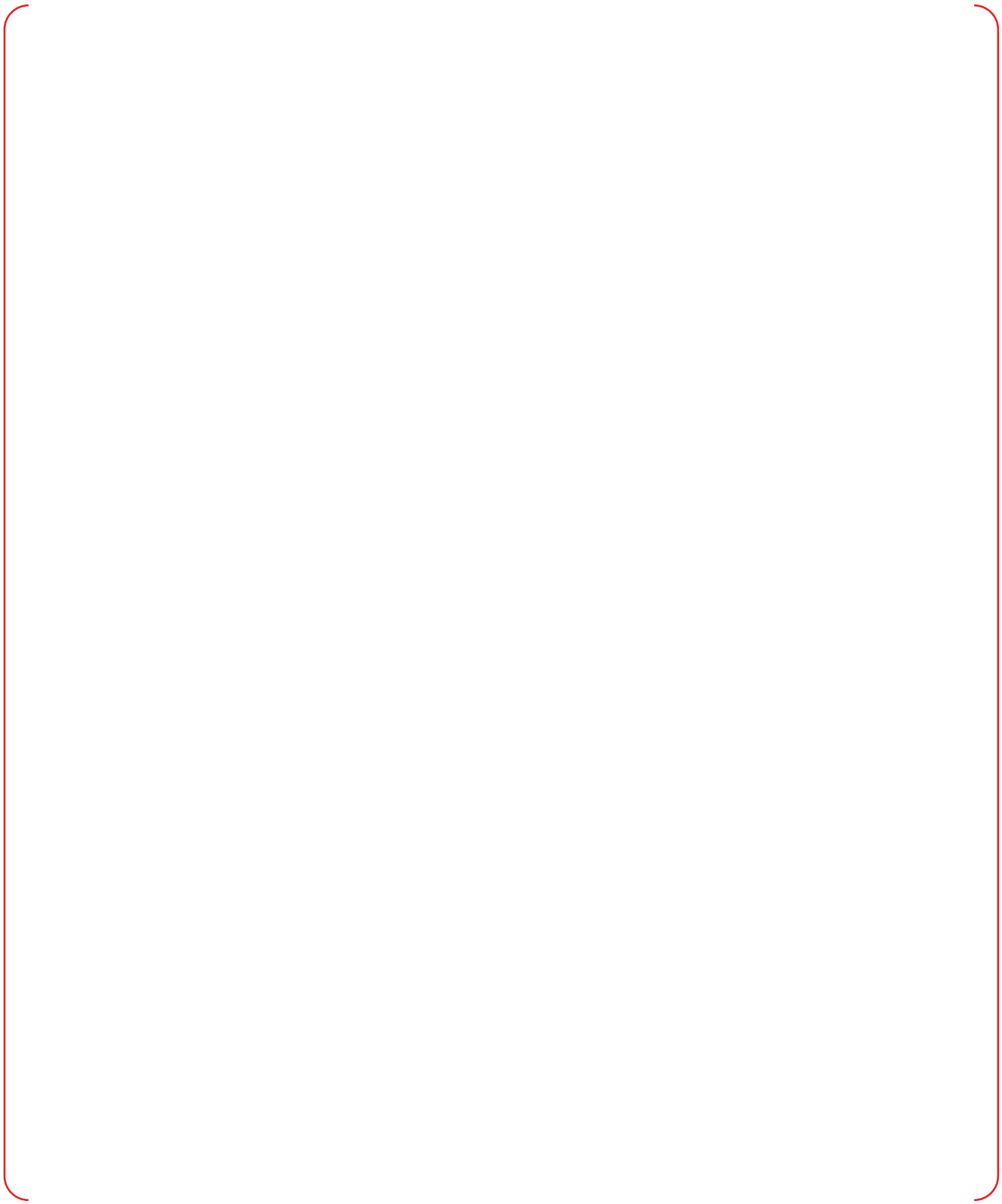


Figure 4-16 Watchdog Timer for ESF-CCS

Replace this figure with the figure on the next page.

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.:	**356-7881**
SRP Section:	**Section: 07 - Instrumentation and Controls - Overview of Review Process**
Application Section:	**Section 7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-16

Explain the redundant controller arrangement for non-safety control functions listed in the Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.”

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.3 states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. In Section 4.6, "Redundant Controller for Availability Enhancement," of Technical Report APR1400-Z-J-NR-14012-P, Rev.0, the applicant identifies the following functions as having completely redundant control loops with redundant controllers and two I/O modules, with the I/O modules operating concurrently for each control loop:

- Control logic for reactor coolant pumps
- Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers
- Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers

The applicant states this portion of the DCS architecture is for enhanced availability. The applicant does not mention other control functions having this type of communications configuration and it is unclear why these specific functions were acknowledged and others appear to be omitted. The applicant also does not present an argument or criteria that would suggest that these particular functions were necessary to implement in this format, or why other functions may not be implemented in this format.

1. Is the design description in Section 4.6 of Technical Report APR1400-Z-J-NR-14012-P, Rev.0, ″Control System CCF Analysis,” applicable to only the three control logic functions mentioned in this section?

2. Explain the basis for the three control functions in Section 4.6 having the stated level of controller redundancy. It is not clear the criterion the applicant uses to determine that these three functions require enhanced availability versus other non-safety functions, such as, pressurizer pressure/level control or feedwater control.

Response

1. Each distributed control system (DCS) controller of the power control system (PCS) and process-component control system (P-CCS) is provided a redundant processor, power supply, and data communication network.

   For nuclear steam supply system (NSSS) control functions, PCS and NPCS, (which include the reactor regulating system (RRS), reactor power cutback system (RPCS), digital rod control system (DRCS), pressurizer pressure control system (PPCS), pressurizer level control system (PLCS), steam bypass control system (SBCS), and feedwater control system (FWCS)), use a redundant control loop and control signal validation design as identified in Sections 4.8 and 5.1.1, Table 5.1-1, and Figure 4.1-3 6 of technical report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis.”

   For the reactor coolant pump (RCP) and balance of plant (BOP) control functions, the completely redundant control loop design is applicable to only the three control logics mentioned in Section 4.6 of technical report APR1400-Z-J-NR-14012-P, Rev.0, ″Control System CCF Analysis.” The completely redundant control loop design means that redundant controllers are provided with redundant I/O modules to enhance availability. The other BOP control loops do not have redundant I/O modules.

   Clarification regarding the redundant control loop design will be added to Section 4.6 of technical report APR1400-Z-J-NR-14012-P, Rev. 0, “Control System CCF Analysis,” as indicated in the attachment associated with this response.

2. Non-safety control functions of NSSS, such as pressurizer pressure/level control or feedwater control, require enhanced availability, while PCS and NPCS use the redundant control loop and control signal validation design described in the response to Item 1 of this response.

   For RCP and BOP control functions, the APR1400 provides completely redundant control loop design for the following non-safety control loops to improve the plant availability as follows:

   - Control logic for reactor coolant pumps

     The reactor coolant pumps are essential non-safety components that may significantly affect plant availability.

   - Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers

   - Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers

     The failure of these control loops can lead to the loss of non-safety main

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

Section 4.6 of technical report APR1400-Z-J-NR-14012-P/NP, Rev. 0, “Control System CCF Analysis” will be revised as indicated in the attachment associated with this response.

4.6. Redundant Controller for Availability Enhancement

The following equipment control logic circuits are designed as completely redundant control loop. The redundant control loop is provided with redundant controllers with two I/O modules. These control circuits perform their functions to be completely separated from each other. The redundant controllers and I/O modules access simultaneously the field data and if one controller or I/O module fail, the other controller or I/O module can perform automatically the functions of controller or data acquisition/signal initiation without bump.

- Control logic for RCPs
- Control logic for non-Class 1E 13.8 kV switchgear power circuit breakers
- Control logic for non-Class 1E 4.16 kV switchgear power circuit breakers

Any one failure is annunciated in the MCR and RSR.

4.7. Interlock/Permissive Functions by Separate Control Group or Safety system

TS

Each DCS controller of the PCS and P-CCS is provided with a redundant processor, power supply, and data communication network.

For NSSS control functions, PCS and NPCS use redundant control loop and control signal validation design, as identified in Sections 4.8 and 5.1.1, Table 5.1-1, and Figure 4.1-3.

For RCP and BOP control functions, the

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.: **356-7881**

SRP Section: **07 – Instrumentation and Controls – Overview of Review Process**

Application Section:

Date of RAI Issue: **01/04/2016**

Question No. 07-18

Describe the mechanisms in place that would allow operators to determine whether the QIAS-N and IFPDs have undergone a failure.

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std. 603-1991, Clause 5.6.3, states, in part, that the safety system design shall be such that credible failure in and consequential actions by other systems, as documented in Clause 4.8 of the design basis section of this standard, shall not prevent the safety systems from meeting the requirements of this standard. The QIAS-N and IFPDs, located in the main control room (MCR) provide alarm, display and controls for operators. In Section 7.7.1.4 of APR1400 FSAR Tier 2, regarding the IFPDs, the applicant states that, “If a data communication error occurs, an appropriate message is generated.” For information displays, the applicant does not appear to state in the licensing documentation how an operator can determine whether a failure such as a common cause failure has occurred such that the displays are frozen up or affected by some other means. Therefore, it is not apparent that an appropriate error message could be generated to alert the operator(s) to a random or common cause failure, for non-safety or safety-displays. Failures of the IFPDs are addressed in Technical Report APR1400-Z-J-NR-14012-P, Rev.0, “Control System CCF Analysis.” However this document does not address how operators would make the initial determination that IFPDs have experienced a failure of some type.

Describe the mechanisms, procedures, or processes in place for the APR1400 design that would allow operators to be alerted to a failure of either the QIAS-N or the IFPDs (e.g. frozen displays or controls).

Response

The applicant’s response to RAI 323-8281 07.03-19 describes the mechanisms that will alert operators when the information flat panel display (IFPD) is malfunctioning.

Subsequent to a failure of the QIAS-N, the QNX servers generate the QIAS-N trouble alarm and broadcast it to other subsystems on the QIAS-N network and the IPS on the Ethernet network through the multi-channel gateway. Each server also sends the QIAS-N health signals to the respective digital output channels of the I/O module. The I/O module channels are wired through isolation relays to the respective field terminals of the IPS.

The QNX servers:

- Monitor the QIAS-N MTP, controllers, Ethernet network, SDN communication, and generate QIAS-N trouble status signals.
- Block the QIAS-N health pulses if QIAS-N trouble is detected.
- Transfer the QIAS-N health status to the IPS
- Communicate the QIAS-N trouble status to the QIAS-N MTP via the SDN.
- Communicate the QIAS-N trouble status to the IFPDs, mini-LDP, and SDOP via the Ethernet network.
- The QIAS-N trouble status in indicated on the QIAS-N MTP displays.

The operator console controls the plant utilizing four ESCMs and four IFPDs and the associated mouse. An operator console is considered inoperable when one of the following occurs: 1) Three IFPDs and each mouse are unavailable, 2) Three ESCMs are unavailable, or 3) The workstation disable switch is unavailable.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical /Topical/Environmental Reports.

There is no impact on any Technical, Topical, or Environmental Report.