# 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.:** | **342-8291** |
| **SRP Section:** | **07.08 – Diverse Instrumentation and Control Systems** |
| **Application Section:** | **07.08** |
| **Date of RAI Issue:** | **12/18/2015** |

## Question No. 07.08-8

Clarify in APR1400 FSAR, Tier 2 how the reactor trip switchgear (RTSG) is diverse from reactor trip circuit breaker (RTCB).

10 CFR Part 50, Appendix A, GDC 22, “Protection system independence,” states, “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.” Item II.Q of the SRM to SECY-93-087, Position 3, states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.”

Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” Section 5.1, “Diverse Protection System,” states, “The DPS is designed to transmit reactor trip signals to a total of eight shunt trip devices of the RTSS-1 and RTSS-2 reactor trip breakers. The PPS transmits reactor trip signals to a total of eight undervoltage trip devices of the RTSS-1 and RTSS-2 reactor trip circuit breakers. Four trip circuit breakers of RTSS-1 are diverse from four trip circuit breakers of RTSS-2. This arrangement ensures the capability of the Diverse Protection System (DPS) to interrupt power to the control element drive mechanisms (CEDMs) regardless of the PPS failure to trip the reactor.” Describe the level and types of diversity between the RTSG and the RTCB. Update FSAR documents accordingly.

## Response

As shown in Figure 4-29, “Reactor Trip Switchgear System Configuration” of the Safety I&C System technical report, each reactor trip switchgear (RTSG) contains a reactor trip circuit breaker (RTCB) as part of the RTSG element.

Section 7.2.1.3 of DCD Tier 2 states that the RTSGs in reactor trip switchgear system 1 (RTSS 1) are supplied by a different manufacturer than the RTSGs in RTSS 2. Reasonable assurance that there is diverse design mechanism between RTSGs in RTSS1 and RTSGs in RTSS2 will be established at the component procurement stage. For clarification, the following wording will be modified to avoid confusion.

[Before]
The RTSS 1 breakers are supplied from a different manufacturer than the RTSS 2 breakers, thereby providing reasonable assurance that a different actuation mechanism is used on the two sets of breakers.

[After]
The **RTSGs in RTSS 1** are supplied from a different manufacturer than the **RTSGs in RTSS 2**, thereby providing reasonable assurance that a different actuation mechanism is used in the **RTCBs in the two different sets of RTSGs**.

Also, Section 7.2.1.9 of DCD Tier 2 also provides the descriptions on the diversity of the two different sets of RTSGs. The related mark-up is to be provided through the response to RAI 317-8271, Question 14.03.05-21.

---

**Impact on DCD**

DCD Tier 2, Section 7.2.1.3 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**

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

In addition to a coincidence trip signal, each LCL also provides trip channel bypass status outputs. The bypass status is provided to verify that a bypass has actually been entered into the coincidence logic. The bypass status is available for display at the MTPs, OMs, and IPS.

### 7.2.1.3 Initiation Circuits

The initiation circuit is located in each division of the PPS. The initiation circuit for the RPS function is composed of initiation relays, interposing relays, contacts from the manual initiation switches, and wiring.

The initiation circuit implements the following logical expression, as shown in Figure 7.2-10: (A1 OR A3) AND (A2 OR A4) where A1, A2, A3, and A4 are the output signals of the redundant LCLs (A1 and A3 from one rack; A2 and A4 from the other rack).

Figure 7.2-9 illustrates the interface between the initiation circuit outputs and the reactor trip breakers and the reactor trip breaker configuration applied to the RPS function.

Eight RTSGs are connected with 2-out-of-4 configuration, as shown in Figure 7.2-9. A full 2-out-of-4 RTSG configuration with eight RTSGs meets the single failure criterion during maintenance and testing.

There are separate initiation circuits for undervoltage and shunt-trip initiation. The PPS provides the undervoltage trip signals, and the diverse protection system (DPS) provides the shunt-trip signals to each RTSG for diversity.

RTSGs in RTSS 1

The RTSS consists of two sets of four reactor trip switchgears (RTSGs) (RTSS 1 and RTSS 2). The PPS interfaces with the undervoltage trip device and the DPS interfaces with the shunt trip device. The ~~RTSS 1 breakers~~ are supplied from a different manufacturer than the ~~RTSS 2 breakers~~, thereby providing reasonable assurance that a different actuation mechanism is used ~~on the two sets of breakers~~.

RTSGs in RTSS 2

If an initiation circuit fails, it is set as fail-safe (i.e., in a trip state), resulting in a partial trip (1 of 4) in the reactor trip breaker arrangement. The partial trip activates the alarm by opening one reactor trip breaker and is indicated by the IPS. The partial trip cannot be bypassed.

in the RTCBs in the two different sets of RTSGs

# 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.:** **342-8291**

**SRP Section:** **07.08 – Diverse Instrumentation and Control Systems**

**Application Section:** **07.08**

**Date of RAI Issue:** **12/18/2015**

---

## Question No. 07.08-10

Clarify that the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation function will go to completion.

10 CFR Part 50.62, “Requirements for reduction of risk from anticipated transients without scram (ATWS) events for light-water-cooled nuclear power plants,” require- ment (c)(1) states, “Each pressurized water reactor must have equipment from sensor output to final actuation device, that is diverse from the reactor trip system, to automatically initiate the auxiliary (or emergency) feedwater system and initiate a turbine trip under conditions indicative of an ATWS.

This equipment must be designed to perform its function in a reliable manner and be independent (from sensor output to the final actuation device) from the existing reactor trip system.” Item II.Q of the SRM to SECY-93-087, Position 3, states, “If a postulated common mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.”

Clarify whether the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation functions will go to completion. Update the FSAR documents and/or technical reports accordingly.

Clarify whether the ATWS mitigation logic and DAS is designed such that, once initiated, the mitigation functions will go to completion. Update the FSAR documents and/or technical reports accordingly.

## Response

The diverse actuation system (DAS) consists of the diverse protection system (DPS), the diverse indication system (DIS), and the diverse manual engineered safety features (ESF) actuation system (DMA).

The DPS provides the anticipated transient without scram (ATWS) mitigation functions required by 10 CFR Part 50.62 for the reduction of risk from ATWS events. In addition, the DPS is designed to meet the requirements Item II.Q of the SRM on SECY-93-087 to assist in mitigation of the effects of a postulated software common cause failure (CCF) of the digital computer logic within the plant protective system (PPS) and ESF component control system (ESF-CCS).

Once the diverse reactor trip signals are initiated automatically from the DPS cabinet, the diverse reactor trip function is completed by the actuation of shunt trip devices of reactor trip circuit breakers. The diverse reactor trip is completed when the reactor trip circuit breakers open. Deliberate operator action (i.e., reset of reactor trip circuit breakers) is required to clear the diverse reactor trip and close the reactor trip circuit breakers.

The AFWS actuation initiated by the DPS-AFAS has a cycling mechanism (or simply ‘cycling AFAS’ hereafter). The cycling AFAS is designed to cycle based on the steam generator (SG) level signals. The actuation of AFWS valves are cycled (i.e., not locked) by the cycling AFAS from the DPS. However, the actuation of AFWS pumps are not cycled (i.e., actuated continuously) once initiated by the DPS-AFAS. When the low SG level trip signals clear, the cycling AFAS is cleared until the SG level drops to the AFAS trip setpoint again.

Once the DPS-SIAS is initiated automatically from the DPS cabinet, it is maintained until operator resets it. The DPS-SIAS can be reset when the pressurizer pressure is increased above its setpoint.

The DMA switches are designed to permit the operator to actuate ESF systems in a timely manner from the MCR after a postulated CCF of the PPS and ESF-CCS. The DMA switches are normally disabled. The functions of the DMA switches could become enabled only by the actuation of the DMA enable switch.

The DMA switches provide ESF actuation as required by Item II.Q of the SRM on SECY-93-087, Position 4, and are listed in Appendix C of the D3 TeR.

The DMA switches send latch signals to the component interface module (CIM). Therefore, the ESF actuation initiated by the DMA switch continues until completion once initiated. These latch signals will be reset manually when the mitigation function is completed.

Based on above descriptions, the DAS including the DPS and DMA switches is designed such that, once initiated, the mitigation function continues until completion.

Sections 5.1 and 5.3 of APR1400-Z-J-NR-14002-P, “Diversity and Defense in Depth”, will be revised to include the additional explanations described above.

**Impact on DCD**

There is no impact on the DCD.

**Impact on PRA**

There is no impact on the PRA.

**Impact on Technical Specifications**

There is no impact on the Technical Specifications.

**Impact on Technical/Topical/Environmental Reports**

Sections 5.1 and 5.3 of D3 TeR, APR1400-Z-J-NR-14002, will be revised as indicated in the attachment associated with this response.

## 5 DIVERSE ACTUATION SYSTEM

The DAS consists of the DPS, DIS, and the DMA switches. Each subsystem is described in the following subsections. The DAS is implemented on a platform that is diverse from the common safety PLC platform. The DAS is designed to meet the quality assurance guidance of Generic Letter 85-06. Any software associated with the DAS is qualified as ITS.

### 5.1 Diverse Protection System

The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO concurrent

Once the diverse reactor trip signals are initiated automatically from the DPS cabinet, the diverse reactor trip function is completed by the actuation of shunt trip devices of reactor trip circuit breakers. The diverse reactor trip is completed when the reactor trip circuit breakers open. Deliberate operator action (i.e., reset of reactor trip circuit breakers) is required to clear the diverse reactor trip and close the reactor trip circuit breakers.

RPCS is out of service.

The DPS is designed to transmit reactor trip signals to total eight shunt trip devices of the RTSS-1 and RTSS-2 reactor trip breakers. The PPS transmits reactor trip signals to total eight undervoltage trip devices of the RTSS-1 and RTSS-2 reactor trip circuit breakers. Four trip circuit breakers of RTSS-1 are diverse from four trip circuit breakers of RTSS-2. This arrangement ensures the capability of the DPS to interrupt power to the control element drive mechanisms (CEDMs) regardless of the PPS failure to trip the reactor.

The DPS is implemented with a 2-out-of-4 voting logic to ensure a single failure within the DPS does not (a) cause a spurious actuation, and (b) preclude an actuation. The BP provides a channel trip signal to the LCL processor located in the four redundant channels. The LCL processor determines the local coincidence logic trip state and initiates reactor trip, turbine trip and ESF actuations based on the state of the four trip signals.

The DPS actuates the auxiliary feedwater system (AFWS) on low steam generator level in either steam generator when the level decreases below a predetermined value. The auxiliary feedwater actuation signals (AFAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the AFWS. Isolation is provided at the ESF-CCS loop controller (LC) cabinet to maintain electrical isolation between the DPS and the CIM.

The DPS also actuates the safety injection system (SIS) on low pressurizer pressure when the pressure decreases below a predetermined value. The safety injection actuation signals (SIAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the safety injection of reactor coolant. Isolation is provided at the ESF-CCS LC cabinet to maintain electrical isolation between the DPS and the CIM.

The DPS also automatically initiates a turbine trip whenever the DPS reactor trip conditions have been met. The DPS turbine trip signal is generated with three seconds of time delay after the initiation of DPS reactor trip signal.

The AFWS actuation initiated by the DPS-AFAS has a cycling mechanism (or simply 'cycling AFAS' hereafter). The cycling AFAS is designed to cycle based on the steam generator (SG) level signals. The actuation of AFWS valves are cycled (i.e., not locked) by the cycling AFAS from the DPS. However, the actuation of AFWS pumps are not cycled (i.e., actuated continuously) once initiated by the DPS-AFAS. When the low SG level trip signals clear, the cycling AFAS is cleared until the SG level drops to the AFAS trip setpoint again.

Once the DPS-SIAS is initiated automatically from the DPS cabinet, it is maintained until operator resets it. The DPS-SIAS can be reset when the pressurizer pressure is increased above its setpoint.

- DMA auxiliary feedwater actuation signal-1 (AFAS-1) switch - Division A
- DMA auxiliary feedwater actuation signal-2 (AFAS-2) switch - Division B

The DMA signals are hardwired directly to the CIM through the isolators. The CIMs interface directly with plant components through the component control circuitry. The CIMs receive component control signals from the ESF-CCS, DPS, and DMA switches.

The DMA switches also provide component-level manual stations to modulate control systems as follows:

- DMA auxiliary feedwater flow/steam generator 1 level manual station - Division A
- DMA auxiliary feedwater flow/steam generator 2 level manual station - Division B

The component-level manual stations of the DMA switches are only enabled when each DMA AFAS is activated in the same division. The component-level manual stations provide manual analog control and indication of auxiliary feedwater flow and steam generator level. The component-level manual stations are directly hardwired to the designated components.

The DMA switches send latch signals to the CIM. Therefore, the ESF actuation initiated by the DMA switch continues until completion once initiated. These latch signals will be reset manually when the mitigation function is completed.

# 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.:** | **342-8291** |
| **SRP Section:** | **07.08-11 – Diverse Instrumentation and Control Systems** |
| **Application Section:** | **07.08** |
| **Date of RAI Issue:** | **12/18/2015** |

## Question No. 07.08-11

Clarify why any system in the APR1400 design that doesn't have a "functional programmable unit," is not susceptible to a software CCF.

10 CFR 50, Appendix A, GDC 22, "Protection system independence" states, "The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function." Item II.Q of the SRM to SECY-93-087, Position 3, states, "If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

APR1400 FSAR, Tier 2, Section 7.8, "Diverse Instrumentation and Control Systems," states, "The diverse actuation system (DAS) consists of the diverse instrumentation and control (I&C) systems that are provided to protect against potential common-cause failure (CCF) of digital safety I&C systems including the plant protection system (PPS) and engineered safety features – component control system (ESF-CCS)." FSAR Tier 2, Section 7.8.1.3, "Diverse Indication System," (DIS) states in part that, "...the DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S) as well as in [the] qualified indication and alarm system-P (QIAS-P)." Section 4.1.1.5, "Auxiliary Process Cabinet - Safety," of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System," states, "There are no programmable digital devices in the APC-S." (Staff acknowledges that the response to Question 07.08-5, see below, will modify this statement.) In addition, Section 5.1 of Technical Report APR1400-Z-J-NR-14002-P, Rev.0, "Diversity and Defense in Depth," states, "The safety

class sensors and APC-S are analog equipment." Provide definition(s) for programmable devices versus non-programmable devices.

In the response to RAI 7880 dated 7/16/15 (ML15197A290), Question 07.08-5, the term "functional programmable unit" was introduced, including a definition for it. The term was defined as a computer that consists of one or more associated processing units and a peripheral equipment, as defined in Section 3.1.8 of IEEE Std 7-4.3.2-2003. The question response explains that if the equipment doesn't have any functional programmable units, it is not susceptible to a software CCF. The definition of functional programmable unit provided in the question response is vague. For instance, what is classified as a computer? As defined, one could interpret functional programmable unit to exclude programmable logic technology, such as field programmable gate arrays or programmable logic devices.

Branch Technical Position 7-19 of NUREG-0800, Section B.1.4, states "In this guidance, common software includes software, firmware, and logic developed from software-based development systems." Provide further clarification with regards to the APC-S and its non-susceptibility to software common cause failure in comparison to the definition used by the staff to consider components that are susceptible to software common cause failure. Inclusion of a diagram explaining the logic within the APC-S would be helpful. Update the FSAR documents and/or technical reports accordingly.

## Response

The APC-S is conventional analog equipment which does not include any 'functional programmable unit' which is defined in Section 3.1.8 of IEEE Std 7-4.3.2. In addition, the APC-S does not use any 'common software', such as software, firmware, and logic developed from software-based development systems. The signal conditioning/ splitting and isolating devices of the APC-S are conventional analog circuits which do not include any firmware or logic developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

To clarify the descriptions regarding the APC-S equipment in related documents, the DCD and TeR's will be revised as follows:

1. DCD Tier 2, Section 7.8.1.1:

   Current description: None (No detailed description about the APC-S components vs. a postulated software CCF possibility.)

   To be added as follows: The DPS receives analog signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S). The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

2. Section 4.1.1.5 of APR1400-Z-J-NR-14001-P, "Safety I&C System"

Current description: There are no programmable digital devices in the APC-S.

To be revised as follows: The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

3. Sections 5.1, 8, and 9 of APR1400-Z-J-NR-14002-P, “Diversity and Defense in Depth”:

Current Description of Section 5.1: The safety class sensors and APC-S are analog equipment. Therefore, these equipment are not affected by the software CCF.

To be revised as follows: The safety class sensors and the APC-S are conventional analog equipment which do not include any functional programmable unit which is defined in IEEE Std 7-4.3.2. In addition, the APC-S does not use any common software. The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which do not include any firmware or logic developed from software-based development systems. Therefore, the safety class sensors and APC-S are not susceptible to a postulated software CCF.

Current Description of Section 8: None

To be revised as follows:

19. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations"

20. IEEE 100 (Seventh Edition), "The Authoritative Dictionary of IEEE Standards Terms"

Current Description of Section 9: None

To be revised as follows:

3. Functional Programmable Unit: Computer that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs, and that can perform substantial computation, including numerous arithmetic or logic operations, without human intervention. Refer to Section 3.1.8 of IEEE Std 7-4.3.2-2003 (Reference 19).

4. Common Software: Common software includes software, firmware, and logic developed from software-based development systems. Refer to Section 1.4 of NUREG-0800, BTP 7-19 (Reference 9).

5. Firmware: The combination of a hardware device and computer instructions and data that reside as read-only software on that device. Refer to the explanation in IEEE 100 (Reference 20). Programmable Logic Devices (PLD), Field Programmable Gate Arrays (FPGA), and Application-Specific Integrated Circuits (ASIC) use software to develop the logic (called 'firmware') that later resides within the digital component. The firmware often

cannot be changed in an individual component. Refer to Section 3.8 of NUREG-0800, BTP 7-19.

---

**Impact on DCD**

DCD Tier 2, Section 7.8.1.1 will be revised as indicated in Attachment 1.

**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**

Safety I&C TeR, Section 4.1.1.5 will be revised as indicated in Attachment 2.
D3 TeR, Sections 5.1, 8, and 9 will be revised as indicated in Attachment 3.

## 7.8.1 System Description

### 7.8.1.1 Diverse Protection System

The DPS augments the PPS to meet the requirements of 10 CFR 50.62 for the reduction of risk from ATWS events. In addition, the DPS assists the mitigation of the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS.

The DPS design includes a reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation functions.

The DPS reactor trip provides a simple and diverse mechanism to decrease the risk from the ATWS events and mitigates the effects of a postulated software CCF of the digital computer logic within the PPS and ESF-CCS, concurrent with a steam line break inside containment.

The DPS turbine trip is automatically initiated whenever the DPS reactor trip conditions are met.

The DPS auxiliary feedwater system (AFWS) actuation provides additional reasonable assurance that an ATWS event could be mitigated if it occurred.

The DPS safety injection system (SIS) actuation assists the mitigation of the effects of a large break loss of coolant accident (LOCA) event with a concurrent software CCF within the PPS and ESF-CCS.

The DPS automatic trip/actuation setpoints are specified to provide reasonable assurance that the PPS initiates an automatic trip/actuation signal prior to the DPS if a postulated software CCF has not degraded the PPS.

The DPS is composed of four channels with one cabinet per channel, and each DPS cabinet is located in a separate room. Each DPS channel is powered from two redundant non-Class 1E vital buses that are independent from Class 1E vital buses. Each DPS channel can be tested manually without causing component actuation during plant operations.

The DPS receives analog signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S). The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

system via SDN, APC-S via hardwired interface, and process instrumentation directly. The safety FPDs for the QIAS-P are installed on the MCR SC.

The QIAS-P transmits data to the QIAS-P safety FPD via the SDN for RG 1.97, Rev. 4, Types B and C variables.

The QIAS-P also transmits the sensor signals and their calculated variables to the IPS and QIAS-N through the MTP and ITP, respectively. In the case of the IPS, this data communication is a unidirectional protocol from the MTP. In the case of the ITP, the SDL data communication is used to transmit data to the QIAS-N.

#### 4.1.1.5 Auxiliary Process Cabinet - Safety

The APC-S consists of four redundant channels designated as Class 1E. It receives safety-related sensor signals and distributes them to the PPS, CPCS, ESF-CCS, QIAS-P, and DIS via hardwired interfaces.

It includes signal conditioning/splitting equipment and the associated power supplies for sensor input. Qualified isolation devices are provided within the APC-S to interface safety signals to the non-safety systems.

~~There are no programmable digital devices in the APC-S.~~

The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which are not developed from software-based development systems. Therefore, the APC-S is not susceptible to a postulated software CCF.

#### 4.1.1.6 Ex-co~~re Neutron Flux Monitoring System~~

The ENFMS pro
from the reactor

The ENFMS consists of four redundant safety channels.

#### 4.1.1.7 Component Interface Module

The CIM is a hardware based safety module for ESF component control (i.e., there is no software). The CIM is implemented using simple hardware-based non-digital technology, so that there is no potential for a software design defect that could result in a CCF of the CIM. The CIM receives component control signals from the ESF-CCS, DPS, DMA switches, and front panel control switch. The CIM prioritizes between input signals according to prioritization and transmits an output signal to the plant component according to the priority mode.

#### 4.1.1.8 Reactor Trip Switchgear System

The RTSS consists of four divisions. The RTSS is designed as Class 1E. The RTSS receives the reactor trip signals from the PPS, manual reactor trip switches, and the DPS through hardwired cables. The PPS interfaces with the undervoltage trip device of RTSS breakers. The DPS interfaces with the shunt trip device of the RTSS breakers. The RTSS disconnects the power to the DRCS for dropping CEAs into the reactor core by RPS signals from the PPS or manual reactor trip signals from the MCR or RSR.

### 4.1.2 Non-safety Control and Monitoring System

#### 4.1.2.1 Power Control System

The PCS integrates control systems that are designed to control the reactor power level, which includes the RRS, RPCS and DRCS.

# 5 DIVERSE ACTUATION SYSTEM

The DAS consists of the DPS, DIS, and the DMA switches. Each subsystem is described in the following subsections. The DAS is implemented on a platform that is diverse from the common safety PLC platform. The DAS is designed to meet the quality assurance guidance of Generic Letter 85-06. Any software associated with the DAS is qualified as ITS.

## 5.1 Diverse Protection System

The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO concurrent with a failure of the protection system. In addition, the DPS is designed to mitigate the consequences of a DBE concurrent with a postulated CCF of the safety I&C system digital computer.

The DPS initiates a reactor trip when either high pressurizer pressure or high containment pressure exceeds the pre-determined value. The DPS also initiates a reactor trip on a turbine trip if the RPCS is out of service. The DPS reactor trip on a turbine trip is manually enabled from the MCR when the RPCS is out of service.

The DPS is designed to transmit reactor trip signals to total eight shunt trip devices of the RTSS-1 and RTSS-2 reactor trip breakers. The PPS transmits reactor trip signals to total eight undervoltage trip devices of the RTSS-1 and RTSS-2 reactor trip circuit breakers. Four trip circuit breakers of RTSS-1 are diverse from four trip circuit breakers of RTSS-2. This arrangement ensures the capability of the DPS to interrupt power to the control element drive mechanisms (CEDMs) regardless of the PPS failure to trip the reactor.

The DPS is implemented with a 2-out-of-4 voting logic to ensure a single failure within the DPS does not (a) cause a spurious actuation, and (b) preclude an actuation. The BP provides a channel trip signal to the LCL processor located in the four redundant channels. The LCL processor determines the local coincidence logic trip state and initiates reactor trip, turbine trip and ESF actuations based on the state of the four trip signals.

The DPS actuates the auxiliary feedwater system (AFWS) on low steam generator level in either steam generator when the level decreases below a predetermined value. The auxiliary feedwater actuation signals (AFAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the AFWS. Isolation is provided at the ESF-CCS loop controller (LC) cabinet to maintain electrical isolation between the DPS and the CIM.

The DPS also actuates the safety injection system (SIS) on low pressurizer pressure when the pressure decreases below a predetermined value. The safety injection actuation signals (SIAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the safety injection of reactor coolant. Isolation is provided at the ESF-CCS LC cabinet to maintain electrical isolation between the DPS and the CIM.

The DPS also automatically initiates a turbine trip whenever the DPS reactor trip conditions have been met. The DPS turbine trip signal is generated with three seconds of time delay after the initiation of DPS reactor trip signal.

The DPS is implemented on a non-safety platform. Each DPS channel is powered from two non-Class 1E vital buses, which are independent from Class 1E vital buses. The DPS uses signals from safety class sensors through isolators located at the APC-S. ~~The safety class sensors and APC-S are analog equipment. Therefore, these equipment are not affected by the software CCF.~~ The configuration and interface of the DPS are shown in Figure 5-1.

The safety class sensors and the APC-S are conventional analog equipment which do not include any functional programmable unit which is defined in IEEE Std 7-4.3.2. In addition, the APCS does not use any common software. The signal conditioning/splitting and isolating devices of the APC-S are conventional analog circuits which do not include any firmware or logic developed from software-based development systems. Therefore, the safety class sensors and APC-S are not susceptible to a postulated software CCF.

## 8 References

1. APR1400-E-J-NR-14001-P, "Component Interface Module", Rev. 0, November 2014
2. APR1400-Z-A-NR-14019, "CCF Coping Analysis", Rev. 0, November 2014
3. APR1400-Z-J-NR-14001-P, "Safety I&C System", Rev. 0, November 2014
4. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations"
5. 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants"
6. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety-Related", April 1985
7. SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs", April 1993, and the associated Staff Requirements Memorandum, July 1993
8. IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits"
9. NUREG-0800, "Standard Review Plan," Chapter 7, BTP 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," Rev. 6
10. NUREG-0800, "Standard Review Plan," Chapter 18, Appendix 18-A, "Crediting Manual Operator Actions in Diversity and Defense-in-Depth (D3) Analyses"
11. ANSI/ANS 58.8-1994, "Time Response Design Criteria for Safety-Related Operator Actions"
12. NUREG-0711, "Human Factors Engineering Program Review Model", Rev. 2, February 2004
13. NUREG/CR-6303, "Method for Performing Diversity and Defense-in Depth Analyses of Reactor Protection Systems", October 1994
14. APR1400-Z-J-NR-14003-P, "Software Program Manual", Rev. 0, November 2014
15. 10 CFR 50, Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants"
16. APR1400 DC Quality Assurance Manual
17. APR1400-K-Q-TR-11005-N, "KHNP Quality Assurance Program Description for the APR1400 Design Certification"
18. ANSI/ANS-58.11-1995 (R2002), "Design Criteria for Safe Shutdown following Selected Design Basis Events in Light Water Reactors"
19. IEEE Std 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computer in Safety Systems of Nuclear Power Generating Stations"
20. IEEE 100 (Seventh Edition), "The Authoritative Dictionary of IEEE Standards Terms"

KEPCO

## 9 Definitions

1. Safe shutdown: A unit shutdown with: (1) the reactivity of the reactor kept to a margin below criticality, consistent with technical specifications; (2) the core decay heat removed at a controlled rate, sufficient to prevent core or reactor coolant system thermal design limits from being exceeded; radioactive material releases controlled to keep doses within prescribed limits; and (4) operation within design limits of structures, systems, and components necessary to maintain these conditions. Refer to ANSI/ANS-58.11-1995 (Reference 18). Safe shutdown means hot shutdown unless otherwise specified in this document.

2. Hot shutdown: In a PWR, the condition, consistent with technical specifications, in which the reactor is subcritical and the reactor coolant system average temperature is below the temperature required to permit operation of the residual heat removal system (e.g., 350°F) but above the temperature specified in the technical specification (e.g., 200°F). Refer to ANSI/ANS-58.11-1995 (Reference 18).

3. Functional Programmable Unit: Computer that consists of one or more associated processing units and peripheral equipment, that is controlled by internally stored programs, and that can perform substantial computation, including numerous arithmetic or logic operations, without human intervention. Refer to IEEE Std 7-4.3.2-2003 (Reference 19).

4. Common Software: Common software includes software, firmware, and logic developed from software-based development systems. Refer to Section 1.4 of NUREG-0800, BTP 7-19 (Reference 9).

5. Firmware: The combination of a hardware device and computer instructions and data that reside as read-only software on that device. Refer to the explanation in IEEE 100 (Reference 20). Programmable Logic Devices (PLD), Field Programmable Gate Arrays (FPGA), and Application-Specific Integrated Circuits (ASIC) use software to develop the logic (called 'firmware') that later resides within the digital component. The firmware often cannot be changed in an individual component. Refer to Section 3.8 of NUREG-0800, BTP 7-19.

# 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.:** | **342-8291** |
| **SRP Section:** | **07.08 – Diverse Instrumentation and Control Systems** |
| **Application Section:** | **07.08** |
| **Date of RAI Issued:** | **12/18/2015** |

## Question No. 07.08-12

Clarify whether the Diverse Indication System (DIS) manual transfer switch for heated junction thermocouple (HJTC) control is safety or non-safety related and address the potential for a software CCF of the QIAS-P to affect the transfer of HJTC control to the DIS.

10 CFR Part 50, Appendix A, GDC 22, “Protection system independence,” states, “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.” Item II.Q of the SRM to SECY-93-087, Position 3, states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.” Position 4, states, “A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.”

Based on the staff’s evaluation, 1) clarify whether the DIS manual transfer switch for HJTC control is safety or non-safety related equipment. 2) Explain whether a software CCF of the QIAS-P could adversely affect the manual switch or the transfer of HJTC control to the DIS. In other words, could such a failure adversely affect the DIS from performing its diverse functions? 3) Provide diagram(s) illustrating the interface between QIAS-P and DIS with the manual transfer switch to illustrate such design aspects as safety classification, signal flow and type of signals. 4) Update the FSAR documents and/or technical reports accordingly.

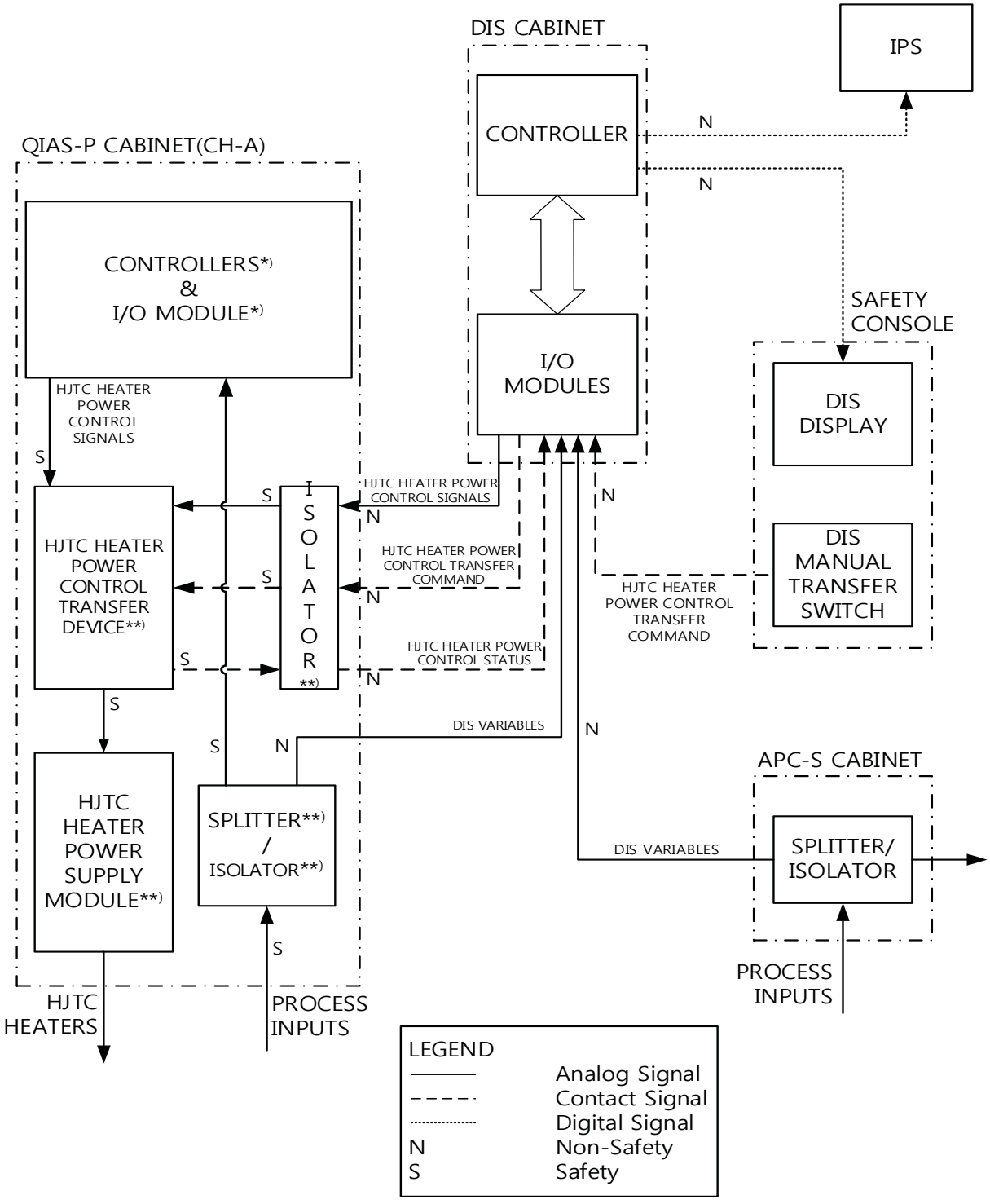
## Response

1. The DIS manual transfer switch for the HJTC heater power control is classified as non-safety related equipment since the DIS is designed to be a non-safety system.

2. The QIAS-P is composed of a software-driven part and an analog part. The software-driven part performs engineering unit conversions, calculations, and displays for information and alarm, and is implemented on the safety I&C common platform which is susceptible to a postulated software CCF. The analog part includes the signal processing and conditioning circuits for both input signals from field sensors and transmitters and output signals for the HJTCs. The analog part of the QIAS-P also includes signal splitting and isolation devices both for forwarding CET/HJTC signals to the DIS and for exchanging signals associated with the HJTC heater power control during a postulated software CCF of the software-driven part of the QIAS-P (refer to the attached DIS signal block diagram for further signal details.). The analog part includes no software-driven functions, and so is not susceptible to a postulated software CCF. A postulated software CCF of the software-driven part of the QIAS-P does not affect the function of the signal splitting and isolation devices for forwarding CET/HJTC signals to the DIS and for exchanging signals associated with the HJTC heater power control in the analog part of the QIAS-P (i.e., the HJTC heater power control transfer device and the HJTC heater power supply module shown in Figure 5-4). The software-driven part of the QIAS-P has neither an electrical link nor a signal interface with the DIS, and all the signal interfaces between the QIAS-P and DIS satisfy the physical separation and electrical isolation requirements of IEEE Std 384-1992, as endorsed by USNRC RG 1.75.

   Consequently, a postulated software CCF of the software-driven part of the QIAS-P does not adversely affect the DIS's ability to perform its diverse function of the HJTC heater power control, or operation of the manual transfer switch to switch the HJTC heater power control from the QIAS-P to the DIS.

3. Refer to the following diagram:




*Note: The symbols *) and **) marked at the end of the components in the QIAS-P Cabinet denote the software-driven part and the analog one, respectively.*

Figure: DIS Signal Block Diagram

4. Refer to Attachments 1, 2 & 3 to this response.

**Impact on DCD**

There is no impact on the DCD.

**Impact on PRA**

There is no impact on the PRA.

**Impact on Technical Specifications**

There is no impact on the Technical Specifications.

**Impact on Technical/Topical/Environmental Reports**

The ‘LIST OF FIGURES’ of APR1400-Z-NR-14002 (Rev. 0) will be revised as indicated in Attachment 1. Section 5.2 of APR1400-Z-NR-14002 (Rev. 0) will be revised as indicated in Attachment 2. Figure 5-4 of APR1400-Z-NR-14002 (Rev. 0) will also be newly added as shown in Attachment 3.

## LIST OF TABLES



## LIST OF FIGURES

### 5.2 Diverse Indication System

The DIS is diverse from the QIAS-P and QIAS-N. The DIS is also diverse from the IPS.

The DIS provides plant operators with the following information that is not susceptible to a postulated CCF in the safety I&C systems. Typical DIS variables are listed in Appendix C and the display parameters are as follows:

- Inadequate core cooling (ICC) monitoring information
- Accident monitoring information
- Emergency operation-related information

the safety I&C systems. The detailed signal interfaces between the DIS and the QIAS-P are shown in Figure 5-4; safety classification, signal flow, and type of signals are also provided in the figure.

The DIS independently calculates a representative core exit temperature, saturation margins and reactor vessel levels for the display. It also provides the heated junction thermo-couple (HJTC) heater power control function for the reactor vessel level detector as a backup of the QIAS-P calculated function which is potentially lost due to a postulated CCF of ~~the safety I&C systems~~.

The DIS is a single channel of non-safety equipment to meet the requirements of BTP 7-19 Point 4 position on D3 for the safety I&C systems. It receives analog inputs from signal splitters/isolators in the APC-S as well as in the QIAS-P channel A via hardwired interface and displays them on the non-safety DIS FPD at the MCR safety console.

All the software associated with the DIS is classified as ITS.

Figure 5-2 shows that the DIS is independent and diverse from the safety I&C system platform.

### 5.3 Diverse Manual ESF Actuation

The DAS includes conventional DMA switches on the MCR safety console for manual actuation of the ESF components which are required to cope with a DBE concurrent with a postulated CCF in the safety I&C systems. The DMA switches are classified as non-safety system, but designed with Class 1E hardware with augmented quality.

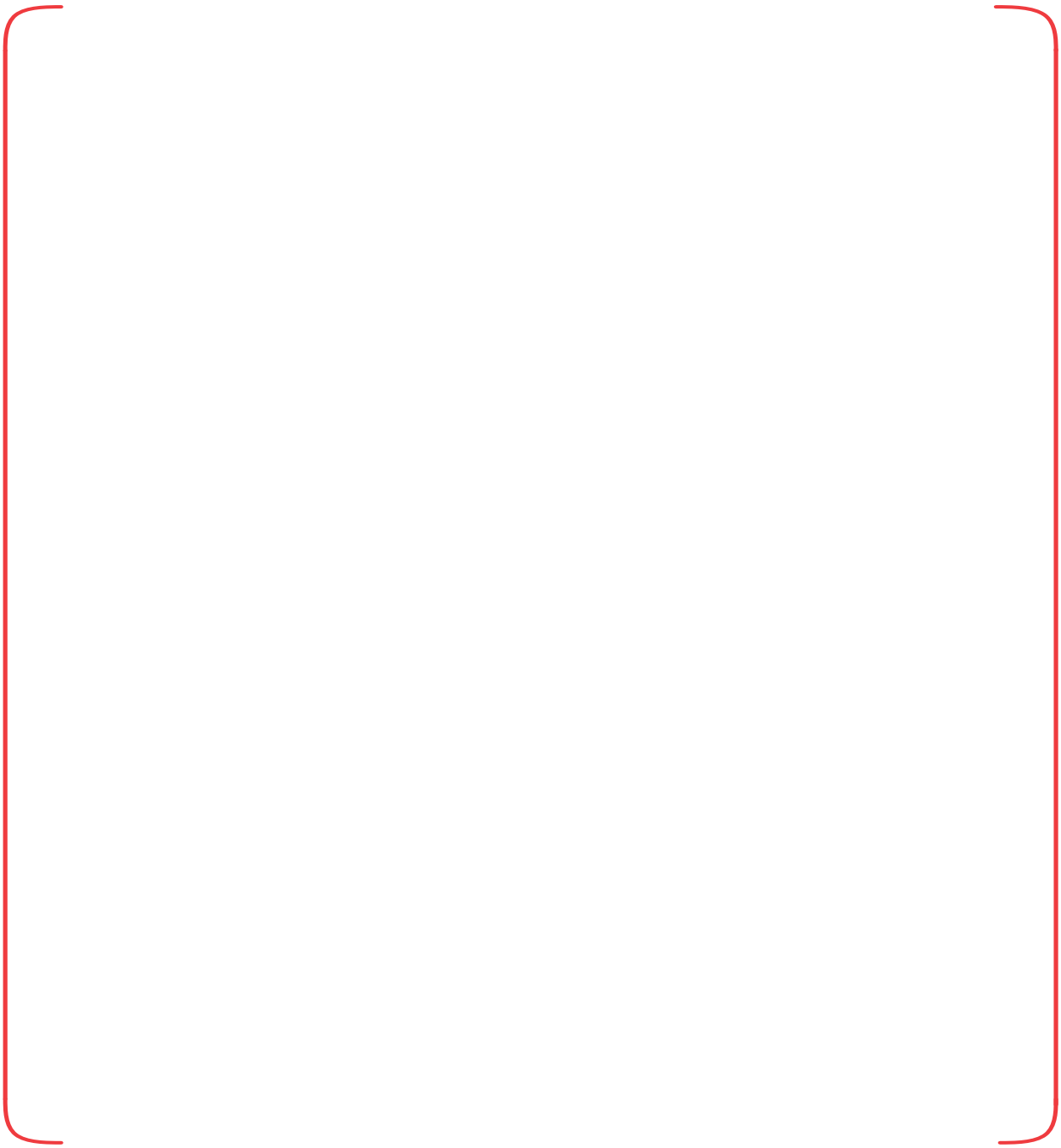
The DMA switches are normally disabled. The functions of the DMA switches could become enabled only by the actuation of DMA enable switch. The DMA enable switch is under operator administrative control, and it is not enabled unless operators conclude that safety I&C systems have a CCF. Refer to Figure 5-3, which shows the interfaces between the DMA switches and the ESF components.

The DMA switches are diverse from the manual and automatic logic functions performed by the PPS and ESF-CCS. The DMA switches provide the ESF actuation as required by SRM on SECY-93-087, and are listed in Appendix C.

The DMA switches provide system-level conventional switches as follows:

- DMA safety injection actuation signal (SIAS) switch - Divisions A and C
- DMA containment spray actuation signal (CSAS) switch - Divisions A and C
- DMA containment isolation actuation signal (CIAS) switch - Division A
- DMA main steam isolation signal (MSIS) switch (1A, 1B, 2A, and 2B) - Division A

TS



Note: The symbols *) and **) marked at the end of the components in the QIAS-P Cabinet denote the software-driven part and the analog one, respectively.

**Figure 5-4. DIS Signal Block Diagram**

# 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.:** **342-8291**

**SRP Section:** **07.08 – Diverse Instrumentation and Control Systems**

**Application Section:** **07.08**

**Date of RAI Issue:** **12/18/2015**

---

## Question No. 07.08-13

Clarify whether a software CCF of a safety-related I&C system could result in a loss of power to the DAS and consequently prevent the DAS from performing its diverse functions.

10 CFR Part 50, Appendix A, GDC 22, “Protection system independence,” states, “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.” Item II.Q of the SRM to SECY-93-087, Position 3, states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.” Position 4, states, “A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.”

Discuss the potential for a software CCF in a safety-related I&C system to compromise the ability of the safety-related I&C system to perform its function and simultaneously result in a loss of power to the DAS and consequently prevent the DAS from performing its diverse functions. In other words, provide analysis demonstrating that the DAS power supply is protected in all cases of a software CCF of the safety-related I&C systems. The response should include clarification as to how the DAS will be powered in a loss-of-offsite power scenario, alternate power sources that are available to power the DAS, and why they are not susceptible to a software CCF of any safety-related I&C system in the plant. Update the FSAR documents and/or technical reports accordingly.

## Response

The diverse actuation system (DAS) consists of the diverse protection system (DPS), the diverse indication system (DIS), and the diverse manual engineered safety features (ESF) actuation switches (DMA switches).

The power source for the DPS and the DIS is the non-Class 1E 120 Vac Instrumentation and Control (I&C) power system which supplies continuous, reliable, and regulated AC power to the plant non-safety I&C equipment.

The power source for the DMA switches is the Class 1E 120 Vac I&C power system which supplies continuous, reliable, and regulated AC power to the plant safety I&C equipment including the PPS and ESF-CCS.

Both Class 1E and non-Class 1E 120 Vac I&C power systems consist of inverters, regulating transformers, manual/automatic transfer switches, and distribution panels, as shown in DCD Tier 2, Figures 8.3.2-3 and 8.3.2-4, respectively.

The non-Class 1E 120 Vac I&C power system with the backup of battery power continuously provides 120 Vac power to the DPS and the DIS during a loss-of-offsite power (LOOP) event. The battery capacities related with the Class 1E and non-Class 1E 120 Vac I&C power systems are described in Table 8.3.2-4 of DCD Tier 2.

The non-Class 1E 120 Vac I&C power system, which provides its output power to the DPS and the DIS, is independent from the Class 1E 120 Vac I&C power system. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the Class 1E I&C systems. Therefore, the non-Class 1E 120 Vac I&C power system is not susceptible to a postulated software CCF caused by any of the safety-related I&C systems.

The Class 1E 120 Vac I&C power system continuously provides 120 Vac power to the interposing relays of the component interface module (CIM) that interfaces with the DMA switches. The Class 1E 120 Vac I&C power system is provided power from the DC control center of the Class 1E 125 Vdc power system. Following a LOOP event, the emergency diesel generator (EDG) provides power to the dc control center. If there is a station blackout (SBO) due to EDG failure concurrent with a LOOP event, the alternate alternating current gas turbine generator (AAC GTG) provides power to the DC control center for either the A or the B safety train. In addition, the Class 1E 125 Vdc power system has battery backup power. The design information regarding the Class 1E 125 Vdc power system and the Class 1E 120 Vac I&C power system is described in Section 8.3.2.1.2 of DCD Tier 2.

The Class 1E 120 Vac I&C power system provides its output power to Class 1E I&C systems, including the APC-S, PPS, CIM, and ESF-CCS. The Class 1E 120 Vac I&C power system does not use any firmware or software within the system. In addition, the equipment platform for the Class 1E 120 Vac I&C power system is diverse from that for the safety-related I&C systems. Therefore, a software CCF which occurs within the safety-related I&C systems does not cause a failure of the Class 1E 120 Vac I&C power system.

The characteristics of the DAS power supply systems are summarized as follows:

- Backup/alternate power sources are available during LOOP event (i.e., battery backup for the DPS and DIS; and battery and EDG backups for the DMA switches)

- No software CCF is possible; the power supply systems do not use common software or firmware used in the safety related I&C systems.

Based on the above analyses, DAS power can be continuously supplied regardless of a postulated software CCF or LOOP event.

Section 5.1 of APR1400-Z-J-NR-14002-P, “Diversity and Defense in Depth (D3)”, will be revised to include the following description as shown in Attachment:

- The non-Class 1E vital buses are connected with the non-Class 1E 120 Vac I&C power system which has battery backup power. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the safety related I&C systems. Therefore, the power supply to the DPS is not impacted by a postulated software CCF or loss of off-site power (LOOP) event.

Section 5.2 of the D3 TeR will be revised to include the following description as shown in Attachment:

- The DIS is powered by the non-Class 1E 120 Vac I&C power system which has battery backup power. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the safety related I&C systems. Therefore, the power supply to the DIS is not impacted by a postulated software CCF or LOOP event.

Section 5.3 of the D3 TeR will be revised to include the following description as shown in Attachment:

- The Class 1E 120 Vac I&C power system continuously provides 120 Vac power to the interposing relays of the component interface module (CIM) that interfaces with the DMA switches. The Class 1E 120 Vac I&C power system is provided power from the DC control center of the Class 1E 125 Vdc power system. Following a LOOP event, the emergency diesel generator (EDG) provides power to the dc control center. If there is a station blackout (SBO) due to EDG failure concurrent with a LOOP event, the alternate alternating current gas turbine generator (AAC GTG) provides power to the DC control center for either the A or the B safety train. In addition, the Class 1E 125 Vdc power system has battery backup power. The design information regarding the Class 1E 125 Vdc power system and the Class 1E 120 Vac I&C power system is described in Section 8.3.2.1.2 of DCD Tier 2.

---

**Impact on DCD**

There is no impact on the DCD

**Impact on PRA**

There is no impact on the PRA

**Impact on Technical Specifications**

There is no impact on the Technical Specifications.

**Impact on Technical/Topical/Environmental Reports**

The D3 TeR, APR1400-Z-J-NR-14002, will be revised, as indicated in the attachment associated with this response.

## Acronyms and Abbreviations

| | |
|---|---|
| AC | alternating current |
| ADV | atmospheric dump valve |
| AFAS | auxiliary feedwater actuation signal |
| AFWS | auxiliary feedwater system |
| AMI | AAC : alternate alternating current |
| AOO | anticipated operational occurrence |
| APC-S | auxiliary process cabinet – safety |
| APR1400 | Advanced Power Reactor 1400 |
| ATWS | anticipated transients without scram |
| BOP | balance of plant |
| BP | bistable processor |
| CCF | common-cause failure |
| CEA | control element assembly |
| CEDM | control element drive mechanism |
| CET | core exit thermocouple |
| CFR | code of federal regulations |
| CH. | channel |
| CIAS | containment isolation actuation signal |
| CIM | component interface module |
| CPCS | core protection calculator system |
| CPM | control panel multiplexer |
| CSAS | containment spray actuation signal |
| CVCS | chemical and volume control system |
| D3 | diversity and defense-in-depth |
| DAS | diverse actuation system |
| DBE | design basis event |
| DC | direct current |
| DCD | design control document |
| DCN-I | data communication network - information |
| DCS | distributed control system |
| D/G | diesel generator |
| DIS | diverse indication system |
| DMA | diverse manual ESF actuation |
| DPS | diverse protection system |
| DRCS | digital rod control system |

| | |
|---|---|
| EDG | emergency diesel generator |
| EMC | electromagnetic compatibility |
| EMI | electromagnetic interference |
| ENFMS | ex-core neutron flux monitoring system |
| EOP | emergency operating procedure |
| ESCM | ESF-CCS soft control module |
| ESF | engineered safety features |
| ESFAS | engineered safety features actuation system |
| ESF-CCS | engineered safety features – component control system |
| FIDAS | fixed in-core detector amplifier system |
| FLC | FPGA-based logic controller |
| FPD | flat panel display |
| FPGA | field programmable gate array |
| FWCS | feedwater control system |
| GDC | general design criteria |
| GL | generic letter |
| HDL | hardware description language |
| HFE | human factors engineering |
| HJTC | heated junction thermocouple |
| HSI | human-system interface |
| I&C | instrumentation and control |
| ICC | GTG : gas turbine generator |
| IEEE | Institute of Electrical and Electronics Engineers |
| IFPD | information flat panel display |
| IPS | Information Processing System |
| IRWST | in-containment refueling water storage tank |
| ITP | interface and test processor |
| ITS | important to safety |
| KHNP | Korea Hydro & Nuclear Co., Ltd. |
| LC | loop controller |
| LCL | local coincidence logic |
| LDP | large display panel |
| LOCA | loss of coolant accident |
| MCR | main control room |
| MG Set | motor generator set |
| MI | minimum inventory |

LOOP : loss-of-offsite power

# 5 DIVERSE ACTUATION SYSTEM

The DAS consists of the DPS, DIS, and the DMA switches. Each subsystem is described in the following subsections. The DAS is implemented on a platform that is diverse from the common safety PLC platform. The DAS is designed to meet the quality assurance guidance of Generic Letter 85-06. Any software associated with the DAS is qualified as ITS.

## 5.1 Diverse Protection System

The DPS is designed to mitigate the effects of an ATWS event characterized by an AOO concurrent with a failure of the protection system. In addition, the DPS is designed to mitigate the consequences of a DBE concurrent with a postulated CCF of the safety I&C system digital computer.

The DPS initiates a reactor trip when either high pressurizer pressure or high containment pressure exceeds the pre-determined value. The DPS also initiates a reactor trip on a turbine trip if the RPCS is out of service. The DPS reactor trip on a turbine trip is manually enabled from the MCR when the RPCS is out of service.

The DPS is designed to transmit reactor trip signals to total eight shunt trip devices of the RTSS-1 and RTSS-2 reactor trip breakers. The PPS transmits reactor trip signals to total eight undervoltage trip devices of the RTSS-1 and RTSS-2 reactor trip circuit breakers. Four trip circuit breakers of RTSS-1 are diverse from four trip circuit breakers of RTSS-2. This arrangement ensures the capability of the DPS to interrupt power to the control element drive mechanisms (CEDMs) regardless of the PPS failure to trip the reactor.

The DPS is implemented with a 2-out-of-4 voting logic to ensure a single failure within the DPS does not (a) cause a spurious actuation, and (b) preclude an actuation. The BP provides a channel trip signal to the LCL processor located in the four redundant channels. The LCL processor determines the local coincidence logic trip state and initiates reactor trip, turbine trip and ESF actuations based on the state of the four trip signals.

The DPS actuates the auxiliary feedwater system (AFWS) on low steam generator level in either steam generator when the level decreases below a predetermined value. The auxiliary feedwater actuation signals (AFAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the AFWS. Isolation is provided at the ESF-CCS loop controller (LC) cabinet to maintain electrical isolation between the DPS and the CIM.

The DPS also actuates the safety injection system (SIS) on low pressurizer pressure when the pressure decreases below a predetermined value. The safety injection actuation signals (SIAS) generated independently by the DPS and the ESF-CCS are prioritized in the CIM, so that either system actuates the safety injection of reactor coolant. Isolation is provided at the ESF-CCS LC cabinet to maintain electrical isolation between the DPS and the CIM.

The DPS also automatically initiates a turbine trip whenever the DPS reactor trip conditions have been met. The DPS turbine trip signal is generated with three seconds of time delay after the initiation of DPS reactor trip signal.

The DPS is implemented on a non-safety platform. Each DPS channel is powered from two non-Class 1E vital buses, which are independent from Class 1E vital buses. The DPS uses signals from safety class sensors through isolators located at the APC-S. The safety class sensors and APC-S are analog equipment. Therefore, these equipment are not affected by the software CCF. The configuration and interface of the DPS are shown in Figure 5-1.

The non-Class 1E vital buses are connected with the non-Class 1E 120 Vac I&C power system which has battery backup power. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the safety related I&C systems. Therefore, the power supply to the DPS is not impacted by a postulated software CCF or loss of off-site power (LOOP) event.

### 5.2 Diverse Indication System

The DIS is diverse from the QIAS-P and QIAS-N. The DIS is also diverse from the IPS.

The DIS provides plant operators with the following information that is not susceptible to a postulated CCF in the safety I&C systems. Typical DIS variables are listed in Appendix C and the display parameters are as follows:

The DIS is powered by the non-Class 1E 120 Vac I&C power system which has battery backup power. In addition, the non-Class 1E 120 Vac I&C power system does not use any software or firmware used in the safety related I&C systems. Therefore, the power supply to the DIS is not impacted by a postulated software CCF or LOOP event.

The DIS independently calculates a representative core exit temperature, saturation margins and reactor vessel levels for the display. It also provides the heated junction thermo-couple (HJTC) heater power control function for the reactor vessel level detector as a backup of the QIAS-P calculated function which is potentially lost due to a postulated CCF of the safety I&C systems.

The DIS is a single channel of non-safety equipment to meet the requirements of BTP 7-19 Point 4 position on D3 for the safety I&C systems. It receives analog inputs from signal splitters/isolators in the APC-S as well as in the QIAS-P channel A via hardwired interface and displays them on the non-safety DIS FPD at the MCR safety console.

All the software associated with the DIS is classified as ITS.

Figure 5-2 shows that the DIS is independent and diverse from the safety I&C system platform.

### 5.3 Diverse Manual ESF Actuation

The DAS includes conventional DMA switches on the MCR safety console for manual actuation of the ESF components which are required to cope with a DBE concurrent with a postulated CCF in the safety I&C systems. The DMA switches are classified as non-safety system, but designed with Class 1E hardware with augmented quality.

The DMA switches are normally disabled. The functions of the DMA switches could become enabled only by the actuation of DMA enable switch. The DMA enable switch is under operator administrative control, and it is not enabled unless operators conclude that safety I&C systems have a CCF. Refer to Figure 5-3, which shows the interfaces between the DMA switches and the ESF components.

The DMA switches are diverse from the manual and automatic logic functions performed by the PPS and ESF-CCS. The DMA switches provide the ESF actuation as required by SRM on SECY-93-087, and are listed in Appendix C.

The DMA switches provide system-level conventional switches as follows:

- DMA safety injection actuation signal (SIAS) switch - Divisions A and C
- DMA containment spray actuation signal (CSAS) switch - Divisions A and C
- DMA containment isolation actuation signal (CIAS) switch - Division A
- DMA main steam isolation signal (MSIS) switch (1A, 1B, 2A, and 2B) - Division A

- DMA auxiliary feedwater actuation signal-1 (AFAS-1) switch - Division A
- DMA auxiliary feedwater actuation signal-2 (AFAS-2) switch - Division B

The DMA signals are hardwired directly to the CIM through the isolators. The CIMs interface directly with plant components through the component control circuitry. The CIMs receive component control signals from the ESF-CCS, DPS, and DMA switches.

The DMA switches also provide component-level manual stations to modulate control systems as follows:

- DMA auxiliary feedwater flow/steam generator 1 level manual station - Division A
- DMA auxiliary feedwater flow/steam generator 2 level manual station - Division B

The component-level manual stations of the DMA switches are only enabled when each DMA AFAS is activated in the same division. The component-level manual stations provide manual analog control and indication of auxiliary feedwater flow and steam generator level. The component-level manual stations are directly hardwired to the designated components.

The Class 1E 120 Vac I&C power system continuously provides 120 Vac power to the interposing relays of the component interface module (CIM) that interface with the DMA switches. The Class 1E 120 Vac I&C power system is provided power from the DC control center of the Class 1E 125 Vdc power system. Following a LOOP event, the emergency diesel generator (EDG) provides power to the dc control center. If there is a station blackout (SBO) due to EDG failure concurrent with a LOOP event, the alternate alternating current gas turbine generator (AAC GTG) provides power to the DC control center for either the A or the B safety train. In addition, the Class 1E 125 Vdc power system has battery backup power. The design information about the Class 1E 125 Vdc power system and the Class 1E 120 Vac I&C power system is described in Section 8.3.2.1.2 of DCD Tier 2.

# 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.:** **342-8291**

**SRP Section:** **07.08 – Diverse Instrumentation and Control Systems**

**Application Section:**

**Date of RAI Issue:** **12/18/2015**

---

## Question No. 07.08-14

Clarify whether the Diverse Manual ESF [Engineered Safety Features] Action (DMA) enable switch is susceptible to a software CCF the safety system (including the PPS and ESF-CCS) and consequently prevent the DMA switches from performing their diverse functions.

10 CFR Part 50, Appendix A, GDC 22, “Protection system independence,” states, “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.” Item II.Q of the Staff Requirements Memorandum (SRM) to SECY-93-087, Position 3, states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.” Position 4, states, “A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions.”

Describe why the DMA enable switch is not susceptible to a software CCF in the safety I&C systems (including the PPS and ESF-CCS) and consequently prevents the DMA switches from performing their diverse functions. In the description, provide analysis and diagrams as necessary to illustrate the independence and the interface between the DMA enable switch and the safety-related I&C systems. In addition, is the DMA enable switch credited for the mitigation of a design bases event which occurs concurrent with a software CCF of the safety system? Update the FSAR documents and/or technical reports accordingly.

## Response

Diverse manual engineered safety features (ESF) actuation (DMA) enable switches are essential pieces of equipment which are used to enable the function of the DMA switches for the mitigation of a design bases event which occurs concurrent with a software common-cause failure (CCF) of the common safety I&C platform.

The DMA enable switch can block the hardwired signal form the DMA switch to the component interface module (CIM) by using an AND gate function, as shown in APR1400-Z-J-NR-14002-P, “Diversity and Defense-in-Depth”, Figure 5-3. The AND gate function is implemented by a simple configuration using conventional hardwired switches, as shown in figure 07.08-14-1.

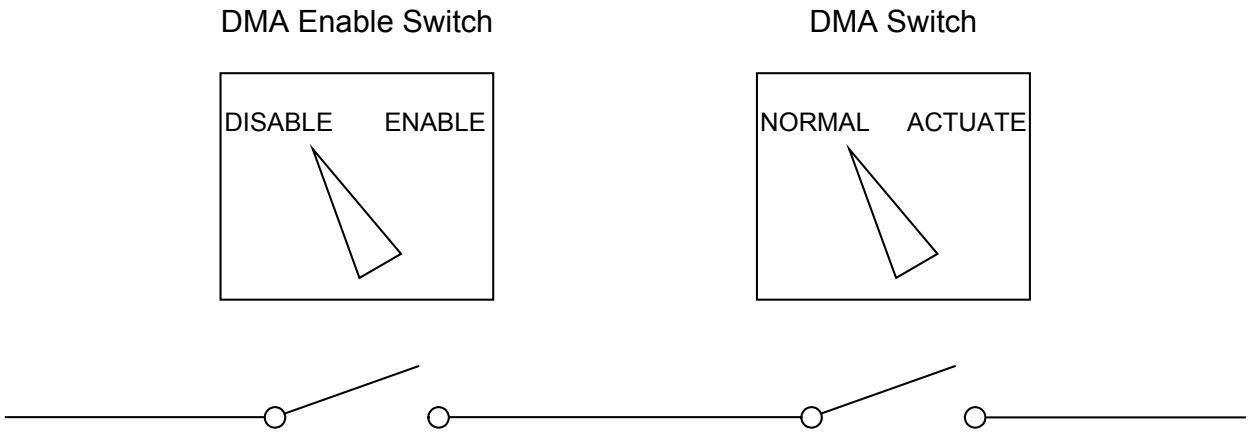



**Figure 07.08-14-1 Configuration of DMA Switch and DMA Enable Switch**

A DMA enable switch has contacts that are connected to each contact of the DMA switches in series, as shown in figure 07.08-14-1. The DMA enable switch can switch these contacts at the same time to enable the function of DMA switches. The operator needs to turn the DMA enable switch to “Enable” and then turn the DMA switch to “Actuate” to send an actuation signal. These actuation signals of the DMA switches are input to the CIM in the engineered safety features-component control system (ESF-CCS) loop controller (LC) cabinets through an interposing relay for isolation. Therefore, the signals from the DMA enable switch and the DMA switch are isolated from the safety I&C systems.

The DMA switches are normally disabled. The functions of the DMA switches can be enabled when the DMA enable switch is switched to enable mode by administratively controlled operator action. The function of the DMA switches is blocked unless operators conclude that safety I&C systems have a CCF. However, this block function is implemented by a simple configuration and the DMA enable switches and DMA switches do not use a software device in order to not be susceptible to a software CCF.

Technical report APR1400-Z-J-NR-14002-P/NP, Rev.0, “Diversity and Defense-in-Depth,” Subsection 5.3 will be revised to include this information, as indicated in the attachment associated with this response.

**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**

Technical report APR1400-Z-J-NR-14002-P/NP, Rev.0, “Diversity and Defense-in-Depth,” Subsection 5.3 will be revised as indicated in the attachment associated with this response.

## LIST OF TABLES



## LIST OF FIGURES

### 5.2 Diverse Indication System

The DIS is diverse from the QIAS-P and QIAS-N. The DIS is also diverse from the IPS.

The DIS provides plant operators with the following information that is not susceptible to a postulated CCF in the safety I&C systems. Typical DIS variables are listed in Appendix C and the display parameters are as follows:

- Inadequate core cooling (ICC) monitoring information
- Accident monitoring information
- Emergency operation-related information

The DIS independently calculates a representative core exit temperature, saturation margins and reactor vessel levels for the display. It also provides the heated junction thermo-couple (HJTC) heater power control function for the reactor vessel level detector as a backup of the QIAS-P calculated function which is potentially lost due to a postulated CCF of the safety I&C systems.

The DIS is a single channel of non-safety equipment to meet the requirements of BTP 7-19 Point 4 position on D3 for the safety I&C systems. It receives analog inputs from signal splitters/isolators in the APC-S as well as in the QIAS-P channel A via hardwired interface and displays them on the non-safety DIS FPD at the MCR safety console.

All the software associated with the DIS is classified as ITS.

Figure 5-2 shows that the DIS is independent and diverse from the safety I&C system platform.

### 5.3 Diverse Manual ESF Actuation

Replace with "A" on the next page

The DAS includes conventional DMA switches on the MCR safety console for manual actuation of the ESF components which are required to cope with a DBE concurrent with a postulated CCF in the safety I&C systems. The DMA switches are classified as non-safety system, but designed with Class 1E hardware with augmented quality.

~~The DMA switches are normally disabled. The functions of the DMA switches could become enabled only by the actuation of DMA enable switch. The DMA enable switch is under operator administrative control, and it is not enabled unless operators conclude that safety I&C systems have a CCF. Refer to Figure 5-3, which shows the interfaces between the DMA switches and the ESF components.~~

The DMA switches are diverse from the manual and automatic logic functions performed by the PPS and ESF-CCS. The DMA switches provide the ESF actuation as required by SRM on SECY-93-087, and are listed in Appendix C.

The DMA switches provide system-level conventional switches as follows:

- DMA safety injection actuation signal (SIAS) switch - Divisions A and C
- DMA containment spray actuation signal (CSAS) switch - Divisions A and C
- DMA containment isolation actuation signal (CIAS) switch - Division A
- DMA main steam isolation signal (MSIS) switch (1A, 1B, 2A, and 2B) - Division A

"A"

DMA enable switches are essential pieces of equipment which are used to enable the function of the DMA switches for the mitigation of a design bases event which occurs concurrent with a software CCF of the common safety I&C platform.

The DMA enable switch can block the hardwired signal form the DMA switch to the CIM by using an AND gate function, as shown in Figure 5-3. The AND gate function is implemented by a simple configuration using conventional hardwired switches, as shown in Figure 5-4.

A DMA enable switch has contacts that are connected to each contact of the DMA switches in series, as shown in Figure 5-4. The DMA enable switch can switch these contacts at the same time to enable the function of DMA switches. Therefore, the operator needs to turn the DMA enable switch to “Enable” and then turn the DMA switch to “Actuate” to send an actuation signal. These actuation signals of the DMA switches are input to the CIM in the ESF-CCS LC cabinets through an interposing relay for isolation. Therefore, the signals from the DMA enable switch and the DMA switch are isolated from the safety I&C systems.

The DMA switches are normally disabled. The functions of the DMA switches can be enabled when the DMA enable switch is switched to enable mode by administratively controlled operator action. The function of the DMA switches is blocked unless operators conclude that safety I&C systems have a CCF. However, this block function is implemented by a simple configuration and the DMA enable switches and DMA switches do not use a software device in order to not be susceptible to a software CCF.

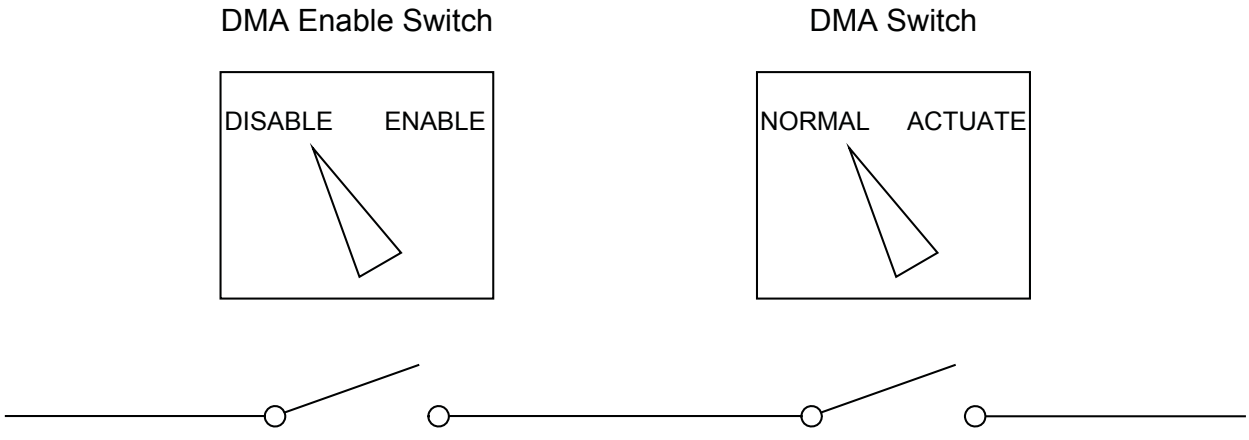



**Figure 5-4 Configuration of DMA Switch and DMA Enable Switch**

New figure is added on page 22 of technical report, APR1400-Z-J-NR-14002-P/NP, "Diversity and Defense-in-Depth."

# 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.:** **342-8291**

**SRP Section:** **07.08 – Diverse Instrumentation and Control Systems**

**Application Section:** **07.08**

**Date of RAI Issue:** **12/18/2015**

---

## Question No. 07.08-15

Describe why a safety injection into the RCS due to a spurious Diverse Protection System (DPS) safety injection actuation, and during reactor coolant system (RCS) heatup and cooldown conditions, does not cause any significant risk to plant safety.

10 CFR Part 50, Appendix A, GDC 22, “Protection system independence,” states, “The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function.” Item II.Q of the Staff Requirements Memorandum (SRM) to SECY-93-087, Positions 3, states, “If a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.”

Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” Appendix A, Section 1.8, “Potential Effects of CCF: Failure to Actuate and Spurious Actuation,” describes the effects and details of a spurious DPS safety injection actuation during the RCS normal operating condition and during the RCS heatup and cooldown conditions.
The guidance of NUREG-800, Section 7.8, states, in part, the diverse I&C systems design should limit the potential for inadvertent actuation and challenges to safety systems. Describe why a safety injection into the RCS due to spurious DPS safety injection actuation, for RCS heatup and cooldown conditions, does not cause any significant risk to plant safety. Is this situation bounded by the safety analysis or another analysis? Update the FSAR documents and/or technical reports accordingly.

## Response

Sections 15.5.1.2 and 15.5.1.3.3 of DCD Tier 2 explain the sequence of events and systems operation, and the results of an inadvertent operation of the emergency core cooling system, which is identified as the safety injection system (SIS), as follows:

> "Inadvertent operation of the SIS is only of consequence when it occurs below the SI pump shutoff head pressure. Above that pressure, there will be no injection of fluid into the system. Below the SI pump shutoff head pressure when the shutdown cooling system is isolated, the SI flow will increase RCS inventory and pressure until the pressure reaches the pump shutoff head pressure. During shutdown cooling system operation, the increase in RCS inventory and pressure will be mitigated by the shutdown cooling system relief valves."
>
> "Plant operation above the SI pump shutoff head pressure will not be impacted by the inadvertent operation of the SIS. Below the SI pump shutoff head pressure when the shutdown cooling system is isolated, there will be an RCS inventory and pressure increase. This increase will be terminated when the pressure rises above the shutoff head pressure. Due to the pressure increase caused by this transient at low RCS temperatures, there is an approach to the brittle fracture limits of the RCS. If the SIS inadvertently actuates during shutdown cooling operation, the shutdown cooling relief valves mitigate the pressure transient."

Based on the DCD Tier 2 safety analysis results, the D3 TeR describes that a safety injection into the RCS due to spurious DPS safety injection actuation during the RCS heatup and cooldown conditions does not cause any significant risks to plant safety.

Appendix A, Section 1.8 of APR1400-Z-J-NR-14002-P, "Diversity and Defense in Depth", will be revised as follows:

Current description:

The spurious DPS safety injection actuation during the RCS heatup and cooldown conditions can result in actual safety injection to the RCS. But, the safety injections in this RCS heatup or cooldown conditions do not cause any significant risks to the plant safety.

To be revised as follows:

The spurious DPS safety injection actuation during the RCS heatup and cooldown conditions can result in actual safety injection to the RCS. The spurious initiation of the safety injection actuation signal (SIAS) from the DPS can cause the operation of the safety injection system (SIS). Inadvertent operation of the SIS is only of consequence when it occurs below the SI pump shutoff head pressure. Above that pressure, there will be no injection of fluid into the system. Below the SI pump shutoff head pressure when the shutdown cooling system is isolated, the SI flow will increase RCS inventory and pressure until the pressure reaches the pump shutoff head pressure. During shutdown cooling system operation, the increase in RCS

inventory and pressure will be mitigated by the shutdown cooling system relief valves. Therefore, the safety injections in this RCS heatup or cooldown conditions do not cause any significant risks to the plant safety.

---

**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**

Appendix A, Section 1.8 of the D3 TeR, APR1400-Z-J-NR-14002, will be revised, as indicated in the attachment associated with this response.

TS