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.: **33-7880**

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

Application Section: **Table 2.5.2.5 of DCD Tier 1**

Date of RAI Issued: **06/16/2015**

Question No. 07.08-1

Clarify what is meant by diverse design group.

10 CFR Part 50, Appendix A, General Design Criterion (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) (ML003708056) to SECY-93-087 (ML003708021), 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.”

Section 5.1 of Technical Report APR1400-Z-J-NR-14002-P, Rev.0, “Diversity and Defense in Depth,” states, “The DPS [Diverse Protection System] is designed to mitigate the consequences of a DBE [design basis event] concurrent with a postulated CCF [common-cause failure] of the safety I&C [instrumentation and control] system digital computer.” The DPS is part of the Diverse Actuation System. The acceptance criteria for the DPS Inspection, Tests, Analyses, and Acceptance Criteria (ITAAC) Item 2 on Table 2.5.2-5 (2 of 3) of the APR1400 FSAR, Tier 1, states, “The as-built DPS is developed by diverse design group from the design group(s)

which developed the PPS [Plant Protection System] and ESF-CCS [Engineered Safety Features - Component Control System] software." Based on the staff's evaluation, the staff requests the applicant to provide definition(s) for diverse design group. Specifically, what criteria would the groups need to meet in order to be considered diverse from one another (e.g., level of communication, organizational separation, etc.) Update final safety analysis report (FSAR) and technical reports accordingly.

Response

NUREG/CR-6303, Paragraph 2.6.1 states, "Using separate designers to design functionally diverse safety systems may reduce the possibility of similar design errors." Although the DPS is classified as non-safety system, the DPS design is performed by a different design team than that which is used to design the PPS or the ESF-CCS.

The following criteria are applied for the definition of "different design team":

- The DPS and PPS/ESF-CCS engineers belong to different engineering teams within the same Instrumentation and Control (I&C) engineering department.

- Communications between the DPS and PPS/ESF-CCS design teams are controlled by the project office.

- Different system testers are assigned to test the DPS and PPS/ESF-CCS during development.

Item 2 on Table 2.5.2-5 (2 of 3) of DCD Tier 1 will be revised as follows:

Current description: The as-built DPS is developed by diverse design group from the design group(s) which developed the PPS and ESF-CCS software.

To be revised as follows: The as-built DPS is developed by a different design team than the design teams which developed the PPS and ESF-CCS.

Impact on DCD

Item 2 on Table 2.5.2-5 (2 of 3) of DCD Tier 1 will be revised as indicated in Attachment.

Impact on PRA

There is no impact on the PRA.

Impact on Technical/Topical/Environmental Reports

There is no impact on the Technical/Topical/Environmental Reports.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Table 2.5.2-5 (2 of 3)

Design Commitment	Inspections, Tests, Analyses	Acceptance Criteria
2. The DPS is physically separate, electrically independent, and diverse from the PPS and ESF-CCS including a diverse method for the reactor trip, the turbine trip, the auxiliary feedwater actuation and safety injection actuation.	2. Inspection of the as-built DPS, PPS and ESF-CCS equipment and design documentation will be performed.	2. The as-built DPS: - is physically separated from the the as-built PPS and ESF-CCS, - utilizes diverse software and hardware from the the as-built PPS and ESF-CCS, - is powered from diverse power buses from the the as-built PPS and ESF-CCS, and - initiates reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation by diverse methods from the the as-built PPS and ESF-CCS. - ~~is developed by diverse design group from the design group (s) which developed the PPS and ESF-CCS software.~~
3. The DPS provides the automatic functions as shown in Table 2.5.2-2, if plant process signals exceed predetermined setpoints.	3. A test of the as-built DPS will be performed using simulated test signals.	3. The as-built DPS initiates the functions identified in Table 2.5.2-2 when the plant process signals reach predetermined setpoint.
4. The DPS utilizes a 2-out-of-4 coincidence logic for automatic initiation of protective functions shown in Table 2.5.2-2.	4. A test of the as-built DPS will be performed using simulated test signals.	4. The DPS coincidence logic produces an initiation when any two channels are in a trip state for a protective function.
5. The DPS cabinets listed in Table 2.5.2-1 are located in separate rooms.	5. Inspection of the as-built DPS equipment will be performed.	5. The DPS cabinets are located in separate rooms.

is developed by a different design team than the design teams which developed the PPS and ESF-CCS.

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.: **33-7880**

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

Application Section: **2.5.2.1 of DCD Tier 1**

Date of RAI Issued: **06/16/2015**

Question No. 07.08-2

Clarify the apparent inconsistency between Tier 1 and Tier 2 information with regards to the purpose and scope of the Diverse Actuation System (DAS).

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, 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.”

APR1400 FSAR, Tier 2, Section 7.8, 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).” However, APR1400 FSAR Tier 1, Section 2.5.2.1, states, “The diverse actuation system (DAS) is a non-safety system which provides a diverse mechanism to decrease risk from the anticipated transients without scram (ATWS) events. The DAS also assists the mitigation of the effects of a

postulated software common cause failure (CCF) within the plant protection system (PPS) and the engineered safety features component control system (ESF-CCS)." There is inconsistency between the information provided within the Tier 1 and Tier 2 documents. As indicated by the Tier 2 statement, DAS mitigates the effects of postulated CCF within the entire digital safety I&C systems, whereas the Tier 1 description is limited to the PPS and ESF-CCS. Based on the staff's evaluation, the staff requests the applicant to correct/update the Tier 1 information wherever applicable, such that Tier 1 information is consistent with Tier 2 information.

Response

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

For consistency between DCD Tier 1 and 2, the Diversity and Defense-in-Depth (D3) Technical Report (TeR) and DCD Tier 1 will be revised as follows:

1. Section 2.5.2.1 of DCD Tier 1:

   Current description: The DAS also assists the mitigation of the effects of a postulated software common cause failure (CCF) within the plant protection system (PPS) and the engineered safety features component control system (ESF-CCS).

   To be revised as follows: The DAS also mitigates the effects of a postulated software common cause failure (CCF) within digital safety I&C systems.

2. Section 3.3.1 of APR1400-Z-J-NR-14002-P, "Diversity and Defense in Depth":

   Current Description: The DAS is designed to comply with the requirements of defense against a postulated CCF in the protection systems.

   To be revised as follows: The DAS is designed to comply with the requirements of defense against a postulated CCF within digital safety I&C systems.

Impact on DCD

DCD Tier 1, Section 2.5.2.1 will be revised as indicated in Attachment 1.

Impact on PRA

There is no impact on the PRA.

Impact on Technical/Topical/Environmental Reports

D3 TeR, Section 3.3.1 will be revised as indicated in Attachment 2.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

2.5.2 Diverse Actuation System

2.5.2.1 Design Description

The diverse actuation system (DAS) is a non-safety system which provides a diverse mechanism to decrease risk from the anticipated transients without scram (ATWS) events. ~~The DAS also assists the mitigation of the effects of a postulated software common cause failure (CCF) within the plant protection system (PPS) and the engineered safety features component control system (ESF-CCS).~~

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

The DAS also mitigates the effects of a postulated software common cause failure (CCF) within digital safety I&C systems.

The DPS initiates reactor trip, turbine trip, auxiliary feedwater actuation, and safety injection actuation. The DPS consists of four channels of non-safety equipment.

The DMA switches are provided to permit the operator to actuate ESF systems from the MCR after a postulated software CCF of the PPS and ESF-CCS.

The DIS provides functions to monitor critical variables and to control heated junction thermocouple (HJTC) heater power when the CCF of digitalized safety I&C systems occurs.

1. The seismic Category I equipment identified in Table 2.5.2-1 can withstand seismic design basis loads without loss of protective function.

2. The DPS is physically separate, electrically independent, and diverse from the PPS and ESF-CCS including a diverse method for the reactor trip, the turbine trip, the auxiliary feedwater actuation and safety injection actuation.

3. The DPS provides the automatic functions as shown in Table 2.5.2-2, if plant process signals exceed predetermined setpoints.

4. The DPS utilizes a 2-out-of-4 coincidence logic for the initiation of automatic functions shown in Table 2.5.2-2.

5. The DPS cabinets listed in Table 2.5.2-1 are located in separate rooms.

The DMA switches provide the operator with the capability to actuate the engineered safety features (ESF) systems from the main control room (MCR). The DMA switches are diverse from the manual and automatic logic functions performed by digital equipment in the PPS and ESF-CCS.

c. GDC 19, “Control Room”

The MCR safety console is equipped with manual reactor trip initiation switches, manual ESF actuation switches and PPS operator modules (OMs) shared with the ESF-CCS and core protection calculator system (CPCS). Monitoring of the plant is accomplished through the use of the qualified indication and alarm system – P (QIAS-P), qualified indication and alarm system – non-safety (QIAS-N) and information processing system (IPS) displays. The DAS (including DPS, DMA switches, and DIS) equipment are provided to protect against a DBE concurrent with a postulated CCF in the safety I&C systems.

d. GDC 21, “Protection System Reliability and Testability”

The DAS is designed to meet the reliability goal of the plant I&C systems.

e. GDC 22, “Protection System Independence”

The independence between the DAS and the protection systems conforms to the independence requirements of IEEE Std 384-1992 (Reference 8) and IEEE Std 603-1991 (Reference 4).

f. GDC 24, “Separation of Protection and Control System”

The electrical, physical and communication isolations are maintained between the safety I&C systems and the DAS which is a non-safety system.

Where safety sensors are shared between the DAS and the safety I&C systems, the qualified isolators in the auxiliary process cabinet–safety (APC-S) prevent adverse interaction with the safety functions induced by DAS failures.

g. GDC 29, “Protection Against Anticipated Operational Occurrences”

Plant initiating events have been analyzed and the safety I&C systems protect the plant against AOO. The DAS, which is diverse from the safety I&C systems and not subject to CCF in the safety I&C systems, provides backup safety functions for AOO.

3.3 Regulatory Guidances and Reports

3.3.1 SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” 1993, Item II.Q, “Defense against Common-Mode Failures in Digital Instrumentation and Control Systems”, and the associated Staff Requirements Memorandum (SRM), 1993 (Reference 7).

Design features for D3 for the PPS and ESF-CCS are implemented in accordance with SRM on SECY-93-087, as referenced by NUREG-0800.

~~The DAS is designed to comply with the requirements of defense against a postulated CCF in the protection systems.~~

The DAS is designed to comply with the requirements of defense against a postulated CCF within digital safety I&C systems.

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.: 33-7880

SRP Section: 07.08 – Diverse Instrumentation and Control Systems

Application Section: 07.08

Date of RAI Issued: 06/16/2015

Question No. 07.08-3

In case of a potential CCF of the Qualified Indication and Alarm System - P (QIAS-P), demonstrate that the Diverse Indication System (DIS) would still be able to conform to Position 4 of SRM to SECY 93-087 and satisfy the requirements of 10 CFR 50, Appendix A, GDC 22.

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, 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.” Positions 4 states that 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. These credited displays and controls shall be independent and diverse from the safety-related computer system.

APR1400 FSAR, Tier 2, Section 7.8, states, in part, the DAS consists of the diverse I&C systems that are provided to protect against potential CCF of digital safety I&C systems. APR1400 FSAR, Tier 2, Section 7.8.1.3, states, “The DIS provides functions to monitor critical variables following a postulated software CCF of safety I&C systems.”

Figure 5-2 “Diversity Features between QIAS and DIS” of the Diversity and Defense in Depth (D3) Technical Report (TeR), shows that the DIS receives Core Exit Thermocouples (CETs)/Heated Junction Thermocouples (HJTCs) hardwired signal inputs from the QIAS-P.

1. Confirm whether the applicant takes credit for CETs/HJTCs signal inputs to the DIS in their CCF Coping Analysis.

2. Explain why the CETs/HJTCs signals are routed through the QIAS-P instead of the APC-S (other DIS input variables come from the APC-S) and demonstrate that by routing the signals through QIAS-P, the DIS would still be able to meet Position 4 of SRM to SECY 93-087 in case of a potential CCF of the QIAS-P.

3. Would the DIS still receive the CETs/HJTCs hardwired signals in case of a postulated CCF of the QIAS-P?

4. Verify the origin of the CETs/HJTCs signals before the signals are received by the QIAS-P.

Response

1. The DIS receives its hardwired signal inputs from the analog part of the qualified indication and alarm system - P (QIAS-P) which employs no functional programmable unit. The display parameters provided by the DIS are credited in the CCF Coping Analysis because the DIS is diverse from the safety computer systems. The CETs/HJTCs signal inputs to the DIS are also credited in the CCF Coping Analysis. These signal inputs are used to measure the temperature of the Reactor Coolant System (RCS) and the coolant level of the Reactor Vessel (RV), which are essential indication parameters used to reach shutdown cooling entry conditions.

2. The routing of the CETs/HJTCs signals through the QIAS-P is designed for simplicity, as determined by engineering judgment. As designed, the DIS needs just 8 CETs and 16 HJTCs out of 61 CETs and 32 HJTCs, which are necessary for the QIAS-P. In addition, there is no difference in functionality, performance, and conformance to relevant standards between the routing of the CETs/HJTCs signals through the QIAS-P to the DIS and that through the APC-S.

   With the routing of the CETs/HJTCs signals through the QIAS-P to the DIS, the DIS is able to meet Position 4 of SRM on SECY 93-087 in case of a potential CCF of the QIAS-P.

   The DIS is independent from the safety-related computer system including the QIAS-P, because the entire signal path from field sensors to input modules of the DIS uses hardwires and analog components without involvement of the computer

part of the QIAS-P. All the CET and HJTC signals come from field sensors to the QIAS-P via hardwires. The signals to be delivered to the DIS are routed through pairs of signal splitters and isolators which are just CCF-free analog components, and then routed to the output terminals in the QIAS-P cabinet.

The DIS is also implemented with equipment which are diverse from those of the safety computer system including the QIAS-P.

3. Yes. The entire signal path from field sensors to input modules of the DIS uses hard wires and analog components without involvement of the computer part of the QIAS-P. Therefore, even in case of a postulated CCF of the QIAS-P, the signal path will not be affected and the DIS will still receive the CET and HJTC signals.

4. The CET and HJTC signals come from sensors in the reactor vessel and go directly to the QIAS-P.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA. .

Impact on Technical/Topical/Environmental Reports

There is no impact on any Technical, Topical or Environmental Reports

Impact on Technical Specifications

There is no impact on the Technical Specifications.

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.: 33-7880

SRP Section: 07.08 – Diverse Instrumentation and Control Systems

Application Section: SRP 07.08

Date of RAI Issued: 06/16/2015

Question No. 07.08-4

Demonstrate how the DIS is independent from the APC-S and QIAS-P when it receives signals from those systems. 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, 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.” Positions 4 states that 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. These credited displays and controls shall be independent and diverse from the safety-related computer system.

The DIS is part of the DAS. APR1400 FSAR, Tier 2, Section 7.8.1.3, states, “The DIS provides functions to monitor critical variables following a postulated software CCF of safety I&C systems. Because the DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S) as well as in qualified indication and alarm system – P (QIAS-P), the DIS is independent from the APC-S and QIAS-P.” Receiving hardwired signal inputs from isolation devices does not necessarily demonstrate independence; particularly with respect to data that could be corrupted,

incorrect, or missing from the receiving systems. In addition, while there may be electrical isolation, there could be functional dependence between the systems. Based on the staff's evaluation, the staff requests the applicant to demonstrate the communication and functional independence between the DIS and the APC-S and QIAS-P.

Response

The APC-S is a safety-related CCF-free analog system that provides signal conditioning/splitting for the field sensor signals. The APC-S also provides isolation functions when signals are split to non-safety systems such as the DIS, using the analog components, which have no functional programmable unit. The QIAS-P is divided into computer and analog parts. The computer part provides safety-related displays in accordance with its own design requirements. The analog part is CCF-free and provides signal conditioning/splitting for the CETs/HJTCs, isolation functions for split signals sent to the DIS, and exchanges signals associated with the manual switchover of the HJTC heater power control with the DIS during CCF of the computer part of the QIAS-P. As mentioned above, the input signals of the DIS are flowing through the APC-S and the analog part of the QIAS-P, which are CCF-free. During CCF conditions, the DIS can perform its required functions since the APC-S and the analog part of the QIAS-P are able to provide the hard-wired input signals to the DIS without being affected by the CCF. Therefore, there is functional independence between the systems.

Position 4 states that the displays and controls shall be independent and diverse from the safety computer system. The safety computer system in the APR1400 I&C design including the PPS, CPCS, ESF-CCS, and the digital part of the QIAS-P can be affected by the CCF. This safety computer system has neither a communication link nor an interface with the DIS. Moreover, the safety computer system is designed to use a different platform (safety common platform based on the PLC) from that of the DIS, which utilizes a FLC-based platform. Consequently, the DIS is independent and diverse from the safety computer system. In addition, the DIS is receiving only the hardwired analog signal inputs, not the digital signal at all, from the APC-S and the analog part of the QIAS-P

Random failures of the APC-S and the analog part of the QIAS-P are not assumed to occur at the same time as the CCF of the safety computer systems. The APC-S and the analog part of the QIAS-P can provide the input signals irrespective of the CCF, which allows the DIS to perform required functions. Accordingly, the DIS is functionally independent from the safety computer systems, including the computer part of the QIAS-P.

To accommodate the staff's request, and more clearly communicate the acceptability of the APR1400 design, Section 7.8.1.3 will be modified to state the following: "The DIS

provides functions to monitor critical variables following a postulated software CCF of safety I&C systems. The DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet - safety (APC-S) and the analog part of the qualified indication and alarm system - P (QIAS-P). The APC-S employs no functional programmable unit. Thus, the APC-S is not susceptible to a postulated software CCF. The QIAS-P is composed of two parts which have no functional interaction with each other. One part is a computer part which employs the functional programmable units~~,~~ is susceptible to a postulated software CCF. The other one is an analog part which employs no functional programmable unit, and is not susceptible to a postulated software CCF. In addition, the safety computer systems including the computer part of the QIAS-P are designed under the safety common platform (i.e., PLC-based), while the DIS is designed under the different FLC-based platform. Therefore, the DIS is independent and diverse from the computer part of the QIAS-P. Moreover, to meet the independence requirements between the safety systems and the non-safety systems, the DIS is electrically isolated and physically separated from the APC-S and the analog part of the QIAS-P. ”

Impact on DCD

Section 7.8.1.3 of DCD Tier 2 will be modified as indicated in Attachment.

Impact on PRA

There is no impact on the PRA.

Impact on Technical/Topical/Environmental Reports

There is no impact on the Technical/Topical/Environmental Reports.

Impact on Technical Specifications

There is no impact on the Technical Specification.

independently by the DPS and ESF-CCS is prioritized in the CIM using state-based priority logic, so that either system can actuate the SIS. Isolation is provided at the ESF-CCS loop controller cabinet to maintain electrical isolation between the DPS and CIM. See Figure 7.8-5 for the DPS-SIAS.

The DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet – safety (APC-S) and the analog part of the qualified indication and alarm system – P (QIAS-P). The APC-S employs no functional programmable unit. Thus, the APC-S is not susceptible to a postulated software CCF. The QIAS-P is composed of two parts which have no functional interaction with each other. One part is a computer part which employs the functional programmable units. The computer part is susceptible to a postulated software CCF.
The other one is an analog part which employs no functional programmable unit, and is not susceptible to a postulated software CCF. In addition, the safety computer systems including the computer part of the QIAS-P are designed under the safety common platform(i.e., PLC-based), while the DIS is designed under the different FLC-based platform. Therefore, the DIS is independent and diverse from the computer part of QIAS-P. Moreover, to meet the independence requirements between the safety-related systems and the non-safety systems, the DIS is electrically isolated and physically separated from the APC-S and the analog part of the QIAS-P."

Each signal of the DMA switches actuates necessary ESF systems to perform the ESF functions. The functions of the DMA switches are enabled by the DMA enable switch on the safety console. The DMA switches block diagram is shown in Figure 7.8-6.

the safety computer systems tion System

The DIS provides functions to monitor critical variables following a postulated software CCF of ~~safety I&C systems~~. ~~Because the DIS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet safety (APC-S) as well as in qualified indication and alarm system P (QIAS-P), the DIS is independent from the APC-S and QIAS-P. The DIS is diverse from the QIAS-P~~.

The DIS provides control functions of heater power for the proper heated junction thermocouple (HJTC) output signal level to assist the mitigation of the effects of a postulated software CCF of ~~the QIAS-P~~. The control function is manually transferred from ~~the QIAS-P~~ to the DIS by the DIS manual transfer switch.

the computer part of the QIAS-P

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.: **33-7880**

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

Application Section: **7.8 of DCD Tier 2**

Date of RAI Issued: **06/16/2015**

Question No. 07.08-5

Define what the applicant considers to be programmable devices and analog equipment.

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, 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.” Positions 4 states that 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. These credited displays and controls shall be independent and diverse from the safety-related computer system.

APR1400 FSAR, Tier 2, Section 7.8, 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, 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 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.” Provide definition(s) for programmable devices versus non-programmable devices. 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 analog equipment. Does analog equipment and nonprogrammable devices mean the same? Update FSAR and technical reports accordingly.

Response

Use of ‘analog equipment’ and ‘non-programmable devices’ described in current TeR’s are synonymous. For the clarification of APC-S equipment, the description of analog equipment or non-programmable devices in current TeR’s will be revised using the description with ‘functional programmable unit’. A functional programmable unit is a computer that consists of one or more associated processing units and peripheral equipment, as defined in Section 3.1.8 of IEEE Std 7-4.3.2-2003.

To clarify the descriptions regarding APC-S equipment in various documents, the following revisions will be made:

1. DCD Tier 2, Section 7.8.1.1:

Current description: None (No detailed description about the APC-S equipment.)

To be added as follows: The DPS receives its hardwired signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S). The APC-S does not include any functional programmable unit.

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 APC-S does not include any functional programmable unit. Therefore, the APC-S is not susceptible to software CCF. A functional programmable unit is a computer that consists of one or more associated processing units and peripheral equipment.

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

Current Description: 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 APC-S include no functional programmable unit. Therefore, these pieces of equipment are not susceptible to software CCF. A functional programmable unit is a computer that consists of one or more associated processing units and peripheral equipment.

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/Topical/Environmental Reports

Safety I&C TeR, Section 4.1.1.5 will be revised as indicated in Attachment 2.

D3 TeR, Section 5.1 will be revised as indicated in Attachment 3.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

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 its hardwired signal inputs from isolation devices in the auxiliary process cabinet-safety (APC-S). The APC-S does not include any functional programmable unit.

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.~~

4.1.1.6 Ex-core Neutron Flux Monitoring System

The APC-S does not include any functional programmable unit. Therefore, the APC-S is not susceptible to software CCF. The functional programmable unit is a computer that consists of one or more associated processing units and peripheral equipment.

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.

KEPCO (

The safety class sensors and APC-S include no functional programmable unit. Therefore, these pieces of equipment are not susceptible to software CCF. A functional programmable unit is a computer that consists of one or more associated processing units and peripheral equipment.