SUPPLEMENTAL RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

Korea Electric Power Corporation / Korea Hydro & Nuclear Power Co., LTD

Docket No. 52-046

RAI No.: **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.

Supplemental Response

In order to confirm the equipment and software diversity between the DAS and the PPS/ESF-CCS, the contents of Item 2 on Table 2.5.2-5 (2 of 3) of DCD Tier 1 will be revised to add the following acceptance criterion (refer to Attachment 1) :

- is developed by different hardware of programmable logic devices and different programmable tools than the hardware and the programmable tools which have applied for the PPS and ESF-CCS.

To clarify the design diversity and diversity attributes between the DAS and the PPS, Sections 6.2.1 and 8 (references), and Note (f) of Table C-1 of the D3 TeR will be revised as shown in Attachment 2.

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 1.

Impact on PRA

There is no impact on the PRA.

Impact on Technical/Topical/Environmental Reports

Sections 6.2.1 and 8(references), and Note (f) of Table C-1 will be revised as indicated in Attachment 2.

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.

- is developed by different hardware of programmable logic devices and different programmable tools than the hardware and the programmable tools which have applied for the PPS and ESF-CCS.

to separate control processors. The potential for simultaneous CCF errors in these multiple processors is minimized, since functional diversity is utilized and software execution is asynchronous.

Diversity - Diversity offers the final defense against CCFs. All critical safety functions, such as reactivity control, inventory control and heat removal, can be monitored, automatically controlled, and manual action taken to maintain the safety margins from both the control systems and the safety I&C systems (Table 6-1). These systems are functionally diverse, as are the fluid/mechanical systems

TS

The basis for the evaluation documented herein is that CCFs (however slight their potential and no matter how many evaluations are done or how they may occur) can be postulated to occur. As a result, the CCF coping analysis takes credit for diverse functions (automatic, manual, and indication) that are required to meet the applicable acceptance criteria following an initiating event concurrent with a postulated CCF in the protection system.

6.2 Diversity and Defense-in-Depth Analysis

The detailed D3 analysis in accordance with NUREG/CR-6303 guidelines is provided in Appendix C. The appendix demonstrates that the vulnerabilities to CCF have been adequately addressed in the APR1400, and the APR1400 I&C systems have sufficient diversity features using the guidelines 1 through 14 in NUREG/CR-6303 (Reference 13). Refer to Appendix C, Table C-1 for diversity attributes diverse I&C platforms against safety I&C system platform.

6.2.1 Diversity Evaluation between the DPS and the PPS

Detailed analysis results of diversity attributes between the DPS and the PPS are as follows:

Design Diversity – Diverse equipment platform based on different technology is applied to the DPS compared with the PPS. The PPS uses the PLC technology for the digital logic processing, whereas the DPS uses the FPGA logic controllers (FLC) technology for the digital logic processing. In addition, system architectures are diverse between the PPS and the DPS. Therefore, significant design diversity factors are provided between the PPS and the DPS.

of the common safety PLC platform

Functional diversity – The reactor trip mechanism of the DPS are diverse form that of the PPS. The PPS use the undervoltage trip mechanism, whereas the DPS use the shunt trip mechanism. Therefore, functional diversity is provided between the PPS and the DPS.

Signal diversity – There is no signal diversity between the PPS and the DPS. The safety class sensors and APC-S are shared by both the PPS and the DPS. The sensors and APC-S are analog type equipment. Therefore, these equipment are not affected by the software CCF.

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

21. Westinghouse Electric Company PM Letter, APR1400 Design Certification - AC160 EPLDs and Impact on D3 Analysis (WO-102), January 9, 2018

Table C-1 Diversity Attributes Between I&C System Platforms

Diverse I&C Platforms (Refer to Table A-1.)		Diversity Attributes against Common Safety PLC Platform					
		Design	Equipment	Functional	Human	Signal	S/W
Non-Safety DCS		O	O	O	O	O	O
FPGA	DPS	O	O	O	O		O
	DIS	O	O		O		O
Hardware Based Device (CIM)		O	O		O		N/A
Analog (Actuator)		O	O		O		N/A
Analog (Sensor)		O	O		O		N/A

O: Diverse, N/A: Not Applicable

Explanatory Notes:

a. The information provided in the table is with respect to the diversity features shared between the platforms, i.e., the reader should observe the information in each column for each diversity feature.

b. Non-safety DCS platform has functional diversity against the common safety PLC platform. The common safety PLC platform provides ON/OFF trip and monitoring functions, whereas the non-safety DCS platform provides continuous control and monitoring functions.

c. A different design team from the common safety PLC design team is responsible for the design of DPS and DIS, and the systems implemented on the Non-safety DCS platform. Detailed analysis results of diversity attributes between the DPS and the PPS are described in Section 6.2.

d. PPS sensor signals are also used in Non-safety DCS systems through qualified isolators.

e. Sensors and APC-S are shared by both PPS and DPS. The analog sensors and APC-S are analog equipment, and they are not affected by the software CCF.

f. There is no commonality in software modules used among the common safety PLC platform, the Non-safety DCS, and the FPGA platforms. Therefore, the occurrence of concurrent CCF of different platform equipment is not considered in the D3 analysis.

g. There are a few areas in which several diversity attributes are shared between platforms, but that is only because more than one platform is used within an actuation path. For example, for an ESFAS actuation path, the instrumentation channel contains analog sensors, APC-S, PPS, ESF-CCS, CIM, electrical panel, and ESF actuated devices. The complete instrumentation channel is designed within the same safety group, so there is human commonality in the design of the

The FLC for the DAS includes the diverse hardware of FPGA, and it does not include the same hardware of EPLDs which are used in the common safety PLC platform. In addition, the FPGA for the DAS is programmed by a diverse programming tool than that used to program the EPLD for the common safety PLC platform.