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.: **323-8281**

SRP Section: **07.03– Engineered Safety Features Systems**

Application Section:

Date of RAI Issue: **11/30/2015**

Question No. 07.03-6

Provide justification for using one-out-of-two logic for some engineered safety features (ESF) control systems proposed in the APR1400 design.

10 CFR 50.55a(h)(3) states “Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603–1991 and the correction sheet dated January 30, 1995.” IEEE Std. 603-1991, Clause 6.7, requires, in part, that capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features shall continue to meet the requirements of Clauses 5.1 and 6.3. EXCEPTION: One-out-of-two portions of the sense and command features are not required to meet Clauses 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated.

There is an exception taken in APR1400 FSAR Tier 2, Section 7.3.1.3, for the balance of plant (BOP) ESF actuation system (ESFAS) function to use one-out-of-two logic, but the staff could not identify the justification for using this exception. Provide the necessary design information to justify this exception.

Response

The safety-related portion of the I&C system for the fuel handling area emergency ventilation actuation signal (FHEVAS) has the required redundancy to meet the single failure criteria of Clauses 5.1 in IEEE Std. 603. Having two divisions of initiating FHEVAS ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the other safety division will remain in service to perform the required ESFAS initiation.

The safety-related portion of the I&C system is designed as Class 1E, is seismic category I, and remains functional during and following a safe shutdown earthquake. Controls, interlocks, sensors, and devices of the safety-related I&C system for FHEVAS are also functionally checked, adjusted, and tested to provide reasonable assurance of intended operation and performance as described in Section 9.4.2.4.

Section 7.3.1.3 of DCD Tier 2 will be revised, as indicated in the attachment associated with this response.

Impact on DCD

Section 7.3.1.3 of DCD Tier 2 will be revised, as indicated in the attachment associated with this response.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical /Topical/Environmental Reports

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

logic conditions are satisfied. The selective 2-out-of-4 coincidence logic is performed in the redundant GCs which independently receives NSSS ESFAS initiation signals from four PPS divisions (Divisions A, B, C, and D) and performs a selective 2-out-of-4 coincidence logic on the initiating signals. Valid ESF-CCS system-level initiation signals are latched and require a manual reset. Two redundant GCs are provided for improved GC availability within each ESF-CCS division.

The selective 2-out-of-4 coincidence logic in the GC processors enhances the fault tolerance to maintain system-level availability and minimize the consequences of single failures. A failure of a processor in the PPS or data communication between the PPS and ESF-CCS is tolerated by the signal quality checking logic and the coincidence logic in the GC.

The redundant GCs provide ESF actuation signals to the redundant LCs in the respective division via SDLs. Each LC receives the ESF actuation signals from the GCs. There is no additional coincidence logic downstream of the GCs. See Figure 7.3-1 for a simplified functional diagram of the ESF-CCS.

All ESF actuation signals can be initiated using manual ESF system-level actuation switches on the safety console. In the ESF actuation logic, each signal also sets a latch to provide reasonable assurance that the system-level signal is not automatically reset once it has been initiated, as shown in Figure 7.3-3. Each ESF actuation signal, excluding the cycling portion of the AFAS, can be manually reset to restore the initiation logic to the non-actuated state from the OM or MTP when ESF actuation condition is cleared.

The BOP ESFAS receives process variable signals from the safety portion of the RMS, manual ESF system-level actuation switches, and manual channel bypass switches. The BOP ESFAS consists of 1-out-of-2 logics taken twice except the FHEVAS, which has one 1-out-of-2 logic.

Add following page

ESFAS Function

The ESFAS consists of six NSSS ESFAS signals and three BOP ESFAS signals. Manual ESF system-level actuation switches are provided on the safety console. The manual MSIS actuation switches are also provided on the remote shutdown console in the RSR.

a. SIAS

The safety-related portion of the I&C system for the FHEVAS has the required redundancy to meet the single failure criteria of Clauses 5.1 in IEEE Std. 603. Having two divisions of initiating FHEVAS ensures that if there is a loss of safety-related I&C equipment that takes one safety division out of service, the other safety division will remain in service to perform the required ESFAS initiation.

The safety-related portion of the I&C system is designed as Class 1E, is seismic Category I, and remains functional during and following a safe shutdown earthquake. Controls, interlocks, sensors, and devices of the safety-related I&C system for FHEVAS are also functionally checked, adjusted, and tested to provide reasonable assurance of intended operation and performance as described in Section 9.4.2.4.

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.: **323-8281**

SRP Section: **07.03 – Engineered Safety Features Systems**

Application Section:

Date of RAI Issue: **11/30/2015**

Question No. 07.03-13

Provide design information on how the signals from the non-safety-related diagnostic section of the component interface module (CIM) will not interfere with the safety functions of the ESF-CCS loop controllers.

10 CFR 50.55a(h)(3) states “Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under Part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995.” Clause 5.6.3, "[Independence] Between Safety Systems and Effects of Design Basis Event," of IEEE Std. 603-1991 requires the safety system design be such that credible failures in and consequential actions by other systems shall not prevent the safety systems from meeting the requirements of this standard.

Figure 4.2-1, “ Overview Diagram of CIM,” of Technical Report APR1400-E-J-NR-14001-P, Rev.0, “Component Interface Module,” identifies that signals from the diagnostic section of the CIM are inputs to the safety-related ESF-CCS loop controller. These diagnostic functions are non-safety related. Describe the measures taken to prevent those non-safety diagnostic signals from interfering with the safety functions of the ESF-CCS loop controllers.

Response

The diagnostic section of the component interface module (CIM) and the signals generated by that section are classified as safety grade, as stated in the third bullet of Section 4.2. That paragraph incorrectly states that the diagnosis section is software integrity level 3 (important to safety); but since the hardware of FPGA-based diagnosis section is designed as Class 1E, the application program of diagnostic function is qualified as software integrity level 3 grade (important to safety, ITS) of the software quality, and the engineering tool to configure the diagnostic logic in the FPGA is commercial grade software.

The diagnosis section generates signals that are transmitted to the Information Processing System (IPS) through the engineered safety features-component control system (ESF-CCS) loop controller (LC) and the maintenance and test panel (MTP) for the purpose of monitoring. These signals are used only for monitoring by the IPS; they do not perform any safety function within the ESF-CCS LC. Therefore, these signals completely bypass all component control logic functions within the ESF-CCS LC. This means there is no interface between these monitoring signals and any ESF-CCS LC logic functions

The signals that are used in the component control logic of the ESF-CCS LC (e.g., energized/de-energized, motor control center power fail, coil circuit open) are input to the ESF-CCS LC through the relays on the CIM module in Figure 4.2-1.

The third bullet of Section 4.2 will be revised as indicated in the attachment associated with this response.

TS

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical /Topical/Environmental Reports

Section 4.2 of Component Interface Module Technical Report, APR1400-E-J-NR-14001-NP, Rev.0 will be revised as indicated in the attachment associated with this response.

TS

Figure 4.1-1 Block Diagram of the CIM Interface

4.2. CIM Configuration

The overview diagram of the CIM is shown in Figure 4.2-1. As discussed earlier, the CIM consists of the priority logic section, base section, and diagnosis section. The purpose of each section is as follows:

TS

TS

TS

Figure 4.2-1 Overview Diagram of the CIM

Page intentionally blank

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.: **323-8281**

SRP Section: **07.03 - Engineered Safety Features Systems**

Application Section:

Date of RAI Issue: **11/30/2015**

Question No. 07.03-22

Describe how the APR1400 design meets the regulatory guidance in Branch Technical Position (BTP) 7-2, "Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines."

10 CFR 50.55a(h)(3) states that “Applications filed on or after May 13, 1999, for construction permits and operating licenses under this part, and for design approvals, design certifications, and combined licenses under Part 52 of this chapter, must meet the requirements for safety systems in IEEE Std. 603-1991 and the correction sheet dated January 30, 1995.” Clause 6.6, "Operating Bypasses," of IEEE Std. 603-1991 requires that, "Whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). If plant conditions change so that an activated operating bypass is no longer permissible, the safety system shall automatically accomplish one of the following actions: (1) Remove the appropriate active operating bypass(es); (2) Restore plant conditions so that permissive conditions once again exist; or (3) Initiate the appropriate safety function(s)."

Section 7.1.2.59, "Conformance with BTP 7-2," of APR1400 FSAR Tier 2 states the I&C systems are designed in accordance with BTP 7-2, but the staff found that there is no further design information provided in the application to substantiate the claimed conformance with regulatory guidance in BTP 7- 2. Provide necessary design information or clarification on how the design of APR1400 safety I&C systems conform to the regulatory guidance in BTP 7-2.

Response

The Branch Technical Position (BTP) 7-2, "Guidance on Requirements on Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines,” Revision 5 states that

“The following features should be incorporated into the design of MOIV systems for safety injection tanks to meet the intent of IEEE Std 279-1971 or IEEE Std 603-1991:

1. Automatic opening of the valves when either primary coolant system pressure exceeds a preselected value (to be specified in the technical specifications), or a safety injection signal is present. Both primary coolant system pressure and safety injection signals should be provided to the valve operator.

2. Visual indication in the control room of the open or closed status of the valve.

3. Bypassed and inoperable status indication in accordance to Regulatory Guide 1.47, "Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety System."

4. Utilization of a safety injection signal to remove automatically (override) any bypass feature that may be provided to allow an isolation valve to be closed for short periods of time when the reactor coolant system is at pressure (in accordance with provisions of the technical specifications).”

The conformance with BTP 7-2 will be described in DCD Tier 2, Subsection 7.6.1.3 as follows:

Position 1

The statement “Automatic opening of the SIT isolation valves when pressurizer pressure exceeds a determined value in Table 7.6-1 or SIAS is present is provided as shown in Figure 7.6-2.” will be added in DCD Tier 2, Subsection 7.6.1.3.

Position 2

The statement “The status indication of the SIT isolation valves is provided in the MCR.” will be added in DCD Tier 2, Subsection 7.6.1.3.

Position 3

The statement “The BISI of the SIT isolation valves is provided in the MCR.” will be added in DCD Tier 2, Subsection 7.6.1.3.

Position 4

DCD Tier 2, Subsection 7.6.1.3 states that

“As the RCS pressure is reduced during plant shutdown, the low pressurizer pressure trip setpoint is reduced to avoid inadvertent initiation of safety injection, the SITs are depressurized to a value below the SCS entry pressure, and the isolation valves are closed.

The SIT permissive interlocks are used to allow isolation of the SITs below the pressure required for mitigation following a loss of coolant accident (LOCA). See Figure 7.6-2 for the interlock logic.

The isolation valves are manually closed when RCS pressure drops below the setpoint in Table 7.6-1 so that the SITs cannot cause overpressurization of the SCS while the SITs are maintained above atmospheric pressure.

If the isolation valves are closed and a SIAS is initiated, the isolation valves automatically open. The SIAS overrides the interlock or any manual signal.”

DCD Tier 2, Subsections 7.1.2.59 and 7.6.1.3 will be revised to clearly indicate the conformance with BTP 7-2, as indicated in the attachment associated with this response.

Impact on DCD

DCD Tier 2, Subsections 7.1.2.59 and 7.6.1.3 will be revised, as indicated in the attachment associated with this response.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

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

guidance specified in NRC RG 1.180. The equipment qualification plan is described in Section 6 of the Safety I&C System Technical Report.

7.1.2.55 Conformance with NRC RG 1.189

The I&C systems that are applicable to NRC RG 1.189 (Reference 55), as shown in Table 7.1-1, are designed in accordance with NRC RG 1.189. The details of the conformance with NRC RG 1.189 are provided in Chapter 9.

7.1.2.56 Conformance with NRC RG 1.204

The I&C systems that are applicable to NRC RG 1.204 (Reference 56), as shown in Table 7.1-1, are designed in accordance with NRC RG 1.204. The details of the conformance with NRC RG 1.204 are provided in Chapter 8.

7.1.2.57 Conformance with NRC RG 1.206

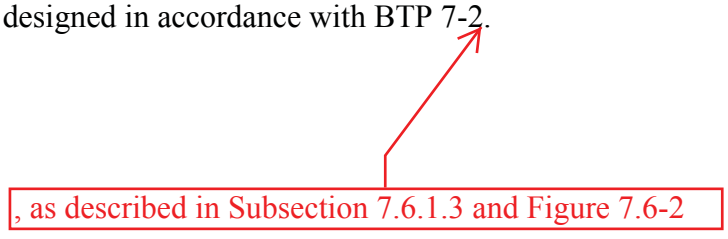
The APR1400 DCD including referenced technical reports is prepared in accordance with the guidance of NRC RG 1.206 (Reference 57) together with NUREG-0800 in order for NRC to evaluate and confirm the safety evaluation.

7.1.2.58 Conformance with BTP 7-1

The I&C systems that are applicable to BTP 7-1 (Reference 58), as shown in Table 7.1-1, are designed in accordance with BTP 7-1.

7.1.2.59 Conformance with BTP 7-2

The I&C systems that are applicable to BTP 7-2 (Reference 59), as shown in Table 7.1-1, are designed in accordance with BTP 7-2.



The SIT permissive interlocks are used to allow isolation of the SITs below the pressure required for mitigation following a loss of coolant accident (LOCA). See Figure 7.6-2 for the interlock logic.

The isolation valves are manually closed when RCS pressure drops below the setpoint in Table 7.6-1 so that the SITs cannot cause overpressurization of the SCS while the SITs are maintained above atmospheric pressure.

As RCS pressure increases, the valves automatically reopen at the set pressure.

The opening of the SIT isolation valves provides reasonable assurance that the SITs are available for injection during plant startup.

If the isolation valves are closed and an SIAS is initiated, the isolation valves automatically open. The SIAS overrides the interlock or any manual signal.

The alarm associated with the SITs is activated if the RCS pressure is increased to the determined values and the SITs have not been repressurized.

Physically separate and independent signals are provided for SIT isolation valve interlocks. Refer to Section 6.3 for SIS and Subsections 3.9.6.3.1 and 6.3.4 for valve tests.

7.6.1.4 Component Cooling Water Supply and Return Header Tie Line Isolation Interlocks

The CCW system removes heat from all safety components required for normal power plant operation, and normal and emergency shutdown of the plant, and transfers the heat to the essential service water through the CCW heat exchangers. The CCW system also provides cooling water for some non-safety components required for plant operation.

Non-essential supply and return header isolation valves are provided to isolate the non-essential supply and return headers from the essential supply and return headers in the event of an accident. These valves are two series electric motor operated valves and can be remotely operated.

These valves are automatically closed on an SIAS or low-low CCW surge tank level signal. The valve closure times are set to prevent complete loss of surge tank volume due to a

Automatic opening of the SIT isolation valves when pressurizer pressure exceeds a determined value in Table 7.6-1 or SIAS is present is provided, as shown in Figure 7.6-2. The status indication and BISI of the SIT isolation valves are provided in the MCR.