# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls – Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | **14.03.05** |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-18

Provide design descriptions and associated ITAAC to verify that the as-built safety I&C system software is only modified via a physical cable disconnect which can physically open the data transmission circuit to protect safety system software from unintended modifications

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications 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 5.6.3 ,requires the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. Digital I&C (DI&C) Interim Staff Guidance (ISG) DI&C-ISG-04 Revision 1, “Highly-Integrated Control Rooms – Communications Issues (HICRc)” provides guidance for achieving communications independence to meet the requirements of IEEE Std 603-1991, Clause 5.6. Section 1, "Interdivisional Communications," Staff Position 10 of this ISG states a physical cable disconnect, or a keylock, which can physically open the data transmission circuit or interrupt the hardwired logic connection should be provided to protect software from unintended modifications.

Technical Report APR1400-Z-J-NR-14001, Rev. 0, “Safety I&C System,” Appendix C, Section C.5.1.1 describes how software is physically loaded into the processor module (PM) and when physical connections are disconnected. Based on the staff’s review of the information provided in FSAR Tier 1, Section 2.5, the staff could not locate design descriptions or associated ITAAC to verify that the as-built safety I&C system is normally physically disconnected to protect safety system software from unintended modifications. In addition, clarify that no other means exist to modify safety I&C system software. Modify Tier 1 of the FSAR to include this information.

## Response

Technical Report APR1400-Z-J-NR-14001, Rev. 0 Appendix C, Section C.5.1.1 and C.5.1.3.7 to DI&C-ISG-04 position 10, "Safety I&C System," contains the following description:

> “The software is loaded into the PM by a serial connection between the portable workstation and the PM. This loading cable is always disconnected on each end to prevent inadvertent programming during plant operations.”

This means that a technician using an approved quality controlled procedure would bring the engineering station with software, open the safety cabinet door, and connect the serial connection cable to the PM to load the software into the PM by a serial connection. In addition, the MTP is not used for software loading.

In the APR1400 DCD Tier1, Section 2.5, item 12 states that "The cabinets listed in Table 2.5.1-1 have key locks and door open alarms, and are located in a vital area of the facility.” Hence, because of the administrative controls that will be in place, it is not necessary to add additional design description to ITAAC for the restriction of preventing unintended modifications.

Additionally, to provide a clear description for on-line software changes, the following sentence will be added in section 4.2.3.4 of Technical Report APR1400-Z-J-NR-14001-P:

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**

The Safety I&C System Technical Report APR1400-Z-J-NR-14001 will be revised as indicated in the attachment.

TS

# RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

**APR1400 Design Certification**

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

**Docket No. 52-046**

| | |
|---|---|
| **RAI No.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls – Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | **14.03.05** |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-19

Clarify whether a reactor trip signal and an engineered safety feature (ESF) initiation signal are automatically initiated for each trip condition listed in APR1400 FSAR Tier 1, Table 2.5.1-2, "Reactor Trip System Variables," and initiation condition listed in FSAR Tier 1, Table 2.5.1-3, "Engineered Safety Features Initiation Variables," respectively.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications 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 6.1, "Automatic Control," states, in part, that “Means shall be provided to automatically initiate and control all protective actions except as justified in [Clause] 4.5. The safety system design shall be such that the operator is not required to take any action prior to the time and plant conditions specified in [Clause] 4.5 following the onset of each design basis event. APR1400 FSAR Tier 1, Section 2.5.1.1, Item 4a states “The PPS provides an automatic reactor trip (RT) and ESF initiation signals, as indicated in Tables 2.5.1-2 and 2.5.1-3, if plant process signals reach predetermined setpoints.” The associated acceptance criterion for this design commitment states, “Each as-built RTSS opens upon receipt of the automatic reactor trip signal identified in Table 2.5.1-2 from respective division of the as-built RTS, and as-built ESF initiation signals are sent to ESF-CCS upon receipt of the automatic ESF initiation signal identified in Table 2.5.1-3.”

Based the design commitment and associated ITAAC presented, it is not clear whether a reactor trip signal and an ESF actuation signal are automatically initiated for each trip condition listed in FSAR Tier 1 Table 2.5.1-2 and initiation condition listed in FSAR Tier 1, Table 2.5.1-3, respectively. As such, the staff requests the applicant to clarify this information in the FSAR Tier 1, Section 2.5.1.1, Item 4a, and the corresponding ITAAC in order to demonstrate that the as-built system meets the requirements of IEEE Std. 603-1991, Clause 6.1.

## Response

In accordance with Clause 6.1 “Automatic Control” of IEEE Std. 603-1991, a reactor trip signal is automatically generated for each trip condition listed in Table 2.5.1-2 of DCD Tier 1 and an ESF initiation signal is automatically generated for each specified initiation condition listed in Table 2.5.1-3 of DCD Tier 1.

A reactor trip automatically occurs if any of the trip conditions listed in Table 2.5.1-2 of DCD Tier 1 occurs. Likewise, an ESF initiation signal is automatically generated if any of the initiation conditions listed in Table 2.5.1-3 of DCD Tier 1 occurs.

The test for each case can be performed using the simulated test signals as provided in item 4.a ITA in Table 2.5.1-5 of DCD Tier 1. In order to verify the design commitment item 4.a, verifying the open status of the trip circuit breaker in the Reactor Trip Switchgear System (RTSS) is already provided as the Acceptance Criteria. Likewise, verifying whether the ESF initiation signal is sent to the ESF-CCS is already provided as the Acceptance Criteria.

Section 2.5.1.1 and the associated ITAAC 4.a in Table 2.5.1-5 of DCD Tier 1 will be clarified to indicate that each condition listed in Tables 2.5.1-2 and 2.5.1-3 of DCD Tier 1 will provide a reactor trip and ESF initiation signal.

---

**Impact on DCD**

Section 2.5.1.1 and Table 2.5.1-5 of DCD Tier 1 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.

3.a Class 1E equipment identified in Table 2.5.1-1 is powered from its respective Class 1E train.

3.b Redundant Class 1E divisions listed in Table 2.5.1-1 and associated field equipment are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment.

3.c Communication independence is achieved between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1.

4.a The PPS provides an automatic reactor trip (RT) and ESF initiation signals, ~~as indicated~~ in Tables 2.5.1-2 and 2.5.1-3, if plant process signals reach predetermined setpoints.
for each condition listed

4.b Once RT is initiated (automatically or manually), the reactor trip breakers remain open until completion of the protective action, and do not automatically return to normal after the trip condition is reset.

4.c Manual reactor trip switches are provided in the MCR and the RSR for reactor trip.

5. The OM in the MCR displays the status information for variables listed in Tables 2.5.1-2 and 2.5.1-3.

6. Each local coincidence logic (LCL) receives trip signals from four channels of bistable processors (BPs) and utilizes a 2-out-of-4 coincidence logic to perform RPS and ESF initiation functions identified in Tables 2.5.1-2 and 2.5.1-3.

7.a The PPS provides manual trip bypasses on the MTP switch panel, for RT and ESF initiation identified in Tables 2.5.1-2 and 2.5.1-3, respectively.

7.b The PPS automatically removes the operating bypasses listed in Table 2.5.1-4 when permissive conditions are not met.

Table 2.5.1-5 (3 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 3.c Communication independence is achieved between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1. | 3.c Analyses, tests or a combination of analyses and tests of the as-built Class 1E equipment listed in Table 2.5.1-1 will be performed to verify its communication independence. | 3.c A report exists and concludes that data communication between redundant divisions of the Class 1E equipment listed in Table 2.5.1-1 or between non-safety systems and the Class 1E equipment listed in Table 2.5.1-1 does not inhibit the performance of the safety function. |
| 4.a The RTS provides an automatic reactor trip (RT) and ESF initiation signals, ~~as indicated~~ in Tables 2.5.1-2 and 2.5.1-3, if plant process signals reach predetermined setpoints. | 4.a A test of the as-built PPS will be performed using simulated test signals. | 4.a Each as-built RTSS opens upon receipt of the automatic reactor trip signal ~~identified~~ in Table 2.5.1-2 from respective division of the as-built RTS, and as-built ESF initiation signals are sent to ESF-CCS upon receipt of the automatic ESF initiation signal ~~identified~~ in Table 2.5.1-3. |
| 4.b Once reactor trip is initiated (automatically or manually), the reactor trip breakers remain open until completion of the protective action, and do not automatically return to normal after the trip condition is reset. | 4.b. A test of the as-built RT system will be performed by returning simulated signals to a level within the predetermined limits of plant process signals at the as-built PPS input for RT functions as identified in Tables 2.5.1-2 after the as-built reactor trip breakers are opened. | 4.b. As-built reactor trip breakers remain open upon receipt of simulated signals returned to a level within the predetermined limits of plant process signals for RT functions as identified in Table 2.5.1-2 after the as-built reactor trip breakers are opened. |
| 4.c Manual reactor trip switches are provided in the MCR and the RSR for reactor trip. | 4.c A test will be performed to verify the actuation of the as-built RTSS using the as-built manual initiation switches in the MCR and RSR. | 4.c Each as-built RTSS opens upon receipt of the corresponding as-built manual reactor trip signal in the MCR and RSR. |

for each condition listed

# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls – Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | **14.03.05** |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-21

Provide design information in APR1400 FSAR, Tier 2 to support the design commitment in APR1400 FSAR, Tier 1, Section 2.5.1.1, Item 23.

GDC 22 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.” APR1400 FSAR Tier 1, Section 2.5.1.1, Item 23, states that two sets of reactor trip switchgear system (RTSS) which consist of four reactor trip switchgears (RTSGs) are diverse [from] each other. The acceptance criterion for the corresponding ITAAC identified in APR1400 FSAR Tier 1, Table 2.5.1-5, Item 23, states, "Two sets of the as-built RTSS which consists of four RTSGs are diverse [from] each other: One set of RTSGs is supplied from a different manufacturer than the other set of RTSGs." APR1400 FSAR Tier 2, Section 7.2.1.9, states that for additional diversity, the RTSS consists of one set of four RTSGs (RTSS 1) and another set of four RTSGs (RTSS 2) with diverse design features. However, this section does not provide description of the attributes that make the design diverse (e.g. RTSGs supplied by different manufacturer). As such, the staff requests the applicant to provide descriptions of the attributes that make the design diverse in APR1400 FSAR Tier 2 to support the design descriptions in APR1400 FSAR Tier 1. Further, the staff requests the applicant to define the acronym “RTSG” as it is not defined in Tier 1 of this application.

## Response

The description which makes the two different sets of the RTSS design diverse, (e.g., that one set of four RTSGs be supplied by a different manufacturer than the other set of four RTSGs) will be added to Section 7.2.1.9 of DCT Tier 2.

Also, the term 'RTSG (reactor trip switchgear)' will be added to the acronym and abbreviation list in DCD Tier 1.

---

**Impact on DCD**

The acronym and abbreviation list in DCD Tier 1 and Section 7.2.1.9 of DCD Tier 2 will be modified 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.

RTSG | reactor trip switchgear

| | |
|---|---|
| RM | refueling machine |
| RMWT | reactor makeup water tank |
| R/O | reverse osmosis |
| RPCS | reactor power cutback system |
| RPS | reactor protection system |
| RRS | reactor regulating system |
| RSR | remote shutdown room |
| RSSH | resin sluice supply header |
| RSPT | reed switch position transmitter |
| RTSS | reactor trip switchgear system |
| RV | reactor vessel |
| SBCS | steam bypass control system |
| SBO | station blackout |
| SC | shutdown cooling |
| SCP | shutdown cooling pump |
| SCS | shutdown cooling system |
| SDCHX | shutdown cooling heat exchanger |
| SFHM | spent fuel handling machine |
| SFP | spent fuel pool |
| SFPCCS | spent fuel pool cooling and cleanup system |
| SG | steam generator |
| SGBS | steam generator blowdown system |
| SI | safety injection |
| SIAS | safety injection actuation signal |
| SIS | safety injection system |
| SIT | safety injection tank |
| SOV | solenoid-operated valve |
| SRDC | safety-related divisional cabinet |
| SSC | structures, systems, and components |
| SSE | safe shutdown earthquake |

Four redundant divisions of the RPS allow a division functional test during power operation while still meeting the single failure criteria.

7.2.1.9 Diversity and Defense-in-Depth

The PPS is designed to minimize credible multiple division failures originating from a postulated software common-cause failure. The diversity features for the PPS are as follows:

a. The software execution orders in the redundant BPs in a channel are different. In each channel, one BP executes a trip function in sequence 1 through N while the other BP executes trip functions in the reverse sequence (N through 1). The reverse trip function execution orders between redundant BPs provide software trajectory diversity for the PPS.

(one set of four RTSGs supplied by a different manufacturer than the other set of four RTSGs)

b. Each RTSS circuit breaker has diverse methods of being automatically opened via the shunt trip and undervoltage trip devices. The PPS interfaces with the UV trip device and the DPS interfaces with the shunt trip device. For additional diversity, the RTSS consists of one set of four RTSGs (RTSS 1) and another set of four RTSGs (RTSS 2) with diverse design features.

c. The PPS and the DPS are designed using different hardware and software to address postulated software common-cause failures, as described in Section 7.8.

The RPS provides the reactor trip echelon of defense, as described in the Diversity and Defense-in-Depth Technical Report (Reference 3).

The critical function success path for diversity is shown in Table 7.2-6.

7.2.1.10 Vital Instrument Power Supply

The vital instrument power supply is described in Subsection 8.1.3.2.

# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls – Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-22

Clarify how the requirements of 10 CFR Part 50, Appendix A, GDC 19 regarding the provision of equipment outside the control room to shutdown the reactor are verified in the as-built design.

GDC 19 states, in part, “A control room shall be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents…Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.”

The following design descriptions and corresponding ITAAC were provided in APR1400 FSAR Tier 1:

- Section 2.5.1.1, Item 8, and the corresponding design commitment in FSAR Tier 1, Table 2.5.1-5, Item 8, state, “Each PPS division is controlled from either the MCR [(main control room)] or RSR [(remote shutdown room)], as selected from MCR/RSR master transfer switches.” The ITA of this ITAAC states, “A test of the as-built PPS will be performed to demonstrate the transfer function between the MCR and RSR.” The acceptance criteria for this ITAAC states, “The as-built master transfer switches transfer controls between the MCR and RSR separately for each as-built PPS division, as follows: [1] Controls at the RSR are disabled when controls are active in the MCR. [2] Controls at the MCR are disabled when controls are active in the RSR.”

- Section 2.5.4.1, Item 8 and the corresponding design commitment in FSAR Tier 1, Table 2.5.4-4, Item 8, state, “Each ESF-CCS division is controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches.” The ITA of this ITAAC states, “A test of the as-built system for one control within each ESF-CCS division will be performed to demonstrate the transfer of control capability between the MCR and

RSR." The acceptance criteria for this ITAAC states, "The as-built master transfer switches transfer controls between the MCR and RSR separately for each as-built ESF-CCS division, as follows: [1] Controls at the RSR are disabled when controls are active in the MCR. [2] Controls at the MCR are disabled when controls are active in the RSR."

- APR1400 FSAR Tier 1, Section 2.5.5.1, Item 3, and the corresponding design commitment in FSAR Tier 1, Table 2.5.5-2, Item 3, state, "The PCS [(power control system)] and PCCS [(process-component control system)] are controlled from either the MCR or RSR, as selected from master transfer switches." The ITA of this ITAAC states, "A test of the as-built system will be performed to demonstrate the transfer of control capability between the MCR and RSR." The acceptance criteria for this ITAAC states, "The as-built MCR/RSR master transfer switches transfer controls between the MCR and the RSR for as-built PCS and P-CCS, as follows: [1] Controls at the RSR are disabled when controls are active in the MCR for the as-built PCS and P-CCS. [2] Controls at the MCR are disabled when controls are active in the RSR for the as-built PCS and P-CCS."

Based on the above descriptions, it is unclear whether this ITAAC is intended to verify that the RSR will have controls for the PPS, ESF-CCS, PCS and P-CCS to meet the requirements of the GDC 19 since the design description and corresponding ITAAC only focuses on verifying the operation of the transfer switch. As such, the staff requests the applicant to provide design descriptions and corresponding ITAACs to verify that the as-built RSR contain sufficient controls to meet the requirements of GDC 19.

## Response

ITAAC Item 8 provided in Table 2.5.1-5 of DCD Tier 1 will be revised to include the control functions based on the transfer capability between the MCR and the RSR to be consistent with the design commitment, Section 2.5.1.1 Item 8 and in compliance with GDC 19.

Regarding engineered safety features-component control system and control system not required for safety, the descriptions and its corresponding ITAACs are provided for each system which has sufficient controls required for safe shutdown throughout subsections of Sections 2.4, 2.6, and 2.11.

Initial test program will be performed to verify that the as-built RSR is designed with capability for cold shutdown of the reactor to meet the requirements of GDC 19 in accordance with the procedure described in Chapter 14.2.12.4.7 of DCD Tier 2.

---

**Impact on DCD**

DCD Tier 1 Table 2.5.1-5 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.

Table 2.5.1-5 (5 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 8. Each PPS division is controlled from either the MCR or the RSR as selected from master transfer switches. | 8. A test of the as-built PPS will be performed to demonstrate the transfer function between the MCR and the RSR. and control | 8. The as-built master transfer switches transfer controls between the MCR and the RSR separately for each as-built PPS division, as follows:<br>- Controls at the RSR are disabled when controls are active in the MCR.<br>- Controls at the MCR are disabled when controls are active in the RSR. and the MCR controls the PPS division |
| 9. The PPS utilizes a 2-out-of-4 coincidence logic when no channels are in trip channel bypass.<br>The PPS converts to a 2-out-of-3 coincidence logic whenever a trip channel bypass is present. | 9. A test will be performed using simulated input signals for RPS and ESFAS process inputs to each channel of the BPs. | 9. When a trip channel bypass is present, the PPS performs a coincidence signal utilizing 2-out-of-3 logic. and the RSR controls the PPS division. |
| 10. Accuracy, response time testing, surveillance testing, and maintenance are applied to determine setpoints for variables of RT and ESF initiation. | 10. Inspection will be performed for the setpoint calculations for RT and ESF initiation listed in Tables 2.5.1-2 and 2.5.1-3 respectively. | 10. A report exists and concludes that the setpoints for RT and ESF actuations listed in Tables 2.5.1-2 and 2.5.1-3 respectively account for accuracy, response time testing, surveillance testing, and maintenance. |

# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | **14.03.05** |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-23

Clarify how verification of adequate physical separation and electrical independence of the as-built Qualified Information and Alarm System-Safety (QIAS-P) are achieved as required by the IEEE Std 603-1991, Clause 5.6.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications 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 5.6.1, requires redundant portions of safety systems provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. IEEE Std 603-1991, Clause 5.6.3, requires that the safety system design to be such that credible failures in and consequential actions by other systems, as documented in Clause 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. IEEE Std. 603-1991, Clause 5.6.3.1, states, in part, “Isolation devices used to effect a safety system boundary shall be classified as part of the safety system.”

APR1400 FSAR Tier 1, Section 2.5.3.1, Item 3.b, states that the Class 1E equipment identified in Table 2.5.3-1, and associated equipment are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment. APR1400 FSAR Tier 1, Table 2.5.3-1, lists QIAS-P Processors for Divisions A and B, and QIAS-P Flat Panel Display (FPD), Division A and B. It is not clear, based on the design commitment, which equipment within Table 2.5.3-1 will be physically separated and electrically independent from one another (e.g. whether redundant divisions of QIAS-P equipment listed in Table 2.5.3-1 are physically separated and electrically independent from each other). In addition, the acceptance criterion provided for the corresponding ITAAC in APR1400 FSAR, Table 2.5.3-3, Item 3.b.i states, “the physical

separation of as-built redundant Class 1E equipment identified in Table 2.5.3-1 and associated field equipment is provided by distance or barriers." The staff finds that this acceptance criterion does not provide criteria for the amount of distance or barrier that would be adequate to meet the physical separation requirements of IEEE Std 603-1991, Clause 5.6. The acceptance criteria for verifying that physical separation requirements are met for the PPS and the ESF-CCS references RG 1.75 as the guidance for demonstrating that the provided distance or barriers is acceptable. In addition, this acceptance criterion also does not address physical separation of QIAS-P equipment from non-Class 1E equipment. The acceptance criterion provided for the ITAAC in APR1400 FSAR, Table 2.5.3-3, Item 3.b.ii states, "a report exists and concludes that independence of as-built redundant Class 1E equipment identified in Table 2.5.3-1, and associated field equipment is achieved by independent power sources and electrical circuits for each channel, and by fiber optic cable interfaces, conventional isolators, or other proven isolation methods or devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems." It is not clear to the staff what is meant by "conventional" isolators, or other "proven" isolation methods or devices. Specifically, are these "conventional" isolators, or other "proven" isolation methods or devices Class 1E qualified as required by IEEE Std 603-1991, Clause 5.6.3. As such, the staff requests the applicant to provide the following:

1. Clarify whether the design commitment in APR1400 FSAR Tier 1, Section 2.5.3.1, Item 3.b are intended to address physical separation and electrical isolation requirements for redundant divisions of safety equipment identified in APR1400 FSAR Tier 1, Table 2.5.3-1.

2. Provide criteria for determining what amount of distance or barrier (e.g. in accordance with RG 1.75, "Physical Independence of Electrical Systems") is adequate to meet the physical separation requirements of IEEE Std 603-1991, Clause 5.6.

3. Amend the acceptance criteria for physical separation to address physical separation of QIAS-P equipment from non-Class 1E equipment.

4. Clarify whether the conventional isolators, or other prevent isolation methods or devices used will be qualified as Class 1E isolation devices.

## Response

1. DCD Tier 1, Section 2.5.3.1 Item 3.b and the design commitment of Item 3.b in Table 2.5.3-3 are intended to address the physical separation and electrical isolation requirements for redundant divisions of the QIAS-P equipment listed in DCD Tier 1, Table 2.5.3-1, as well as the physical separation and electrical isolation requirements of them from non-Class 1E equipment (Refer to DCD Tier 2, Section 7.5.2.1 a.1) and 3)).

   Both DCD Tier 1, Section 2.5.3.1 Item 3.b, and the design commitment of Item 3.b in Table 2.5.3-3 will be revised to clarify the intent as indicated in the attached mark-up.

   The phrase 'and associated field equipment' will be deleted from all the related descriptions in DCD Tier 1, Section 2.5.3.1 and Table 2.5.3-3, because the associated field equipment is not within the QIAS-P boundary.

2. The acceptance criteria of Item 3.b.i in DCD Tier 1, Table 2.5.3-3 will be revised to provide the criteria on the amount of distance or barrier that is adequate to meet the physical separation requirements.

3. The acceptance criteria of Item 3.b.i and 3.b.ii in DCD Tier 1, Table 2.5.3-3 will be revised to address the physical separation of QIAS-P equipment from the non-Class 1E equipment.

4. As stated in DCD Tier 2, Section 7.5.2.1 a.4), all of the isolation devices used between the QIAS-P and IPS and between the QIAS-P and QIAS-N meet the requirements of IEEE Std 384.

For clarification, the acceptance criteria of Item 3.b.ii in DCD Tier 1, Table 2.5.3-3 will be revised to verify the application of Class 1E qualified isolation devices.

---

**Impact on DCD**

Section 2.5.3.1 and Table 2.5.3-3 of DCD Tier 1 will be revised as indicated in the attached mark-up.

**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 the Technical/Topical/Environmental Reports.

2.5.3 Qualified Indication and Alarm System

2.5.3.1 Design Description

The qualified indication and alarm system (QIAS) is a monitoring system that is used to display safety-related information and non-safety information.

The QIAS consists of the two subsystems as follows:

a. QIAS - P, Divisions A and B

b. QIAS - N

In this section, QIAS-N which is non-safety system is not described.

The QIAS-P equipment are located in the auxiliary building.

1. The seismic Category I equipment, identified in Table 2.5.3-1, can withstand seismic design basis loads without loss of its safety function.

2. QIAS-P equipment, identified in Table 2.5.3-1, can withstand the electrical surge, electromagnetic interference (EMI), radio frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist before, during, and following a postulated accidents without loss of its safety function for the time required to perform the safety function.

3.a Class 1E equipment identified in Table 2.5.3-1 is powered from its respective Class 1E train.

Redundant

divisions listed

3.b Class 1E ~~equipment identified~~ in Table 2.5.3-1, ~~and associated equipment~~ are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment.

4. The QIAS-P monitors and displays the accident monitoring instrumentation variables identified in Table 2.5.3-2.

5. The QIAS-P software is implemented according to the software lifecycle process.

Table 2.5.3-3 (2 of 3)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 3.a Class 1E equipment identified in Table 2.5.3-1 is powered from its respective Class 1E train. | 3.a Tests of the as-built Class 1E equipment will be performed using a simulated test signal. | 3.a The Class 1E equipment identified in Table 2.5.3-1 is powered from its respective Class 1E train. |
| 3.b Class 1E equipment identified in Table 2.5.3-1, and associated field equipment are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment. | 3.b.i Inspection for separation of the as-built redundant Class 1E equipment identified in Table 2.5.3-1, and associated field equipments will be performed. | 3.b.i The physical separation of as-built redundant Class 1E equipment identified in Table 2.5.3-1, and associated field equipment is provided by distance or barriers. |
| | 3.b.ii Analyses, tests or a combination of analyses and tests of the as-built redundant Class 1E equipment identified in Table 2.5.3-1, and associated field equipment will be performed to verify its electrical independence. | 3.b.ii A report exists and concludes that independence of as-built redundant Class 1E equipment identified in Table 2.5.3-1, and associated field equipment is achieved by independent power sources and electrical circuits for each channel, and by fiber optic cable interfaces, conventional isolators, or other proven isolation methods or devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems. |
| | 3.b.iii Testing, analysis or combination of testing and analysis will be performed for the electrical isolation devices. | 3.b.iii A report exists and concludes that the electrical isolation devices prevent credible faults from propagating into a safety system divisions. |
| 4. The QIAS-P monitors and displays the accident monitoring instrumentation variables identified in Table 2.5.3-2. | 4. Test of the as-built QIAS-P equipment will be performed to demonstrate the monitoring and display capability for each QIAS-P division using actual or simulated input signals. | 4. The QIAS-P monitors and displays the accident monitoring instrumentation variables identified in Table 2.5.3-2. |

To be revised as shown on the next page.

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 3.b Redundant Class 1E divisions listed in Table 2.5.3-1 ~~and associated field equipment~~ are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment. | 3.b.i Inspection for separation of the as-built redundant Class 1E divisions listed in Table 2.5.3-1 ~~and associated field equipment~~ will be performed. | 3.b.i The physical separation of the as-built redundant Class 1E divisions listed in Table 2.5.3-1 ~~and associated field equipment~~ is provided by distance or barriers in accordance with NRC RG 1.75 both at interfaces between redundant divisions and at interfaces between Class 1E systems and non-Class 1E systems. |
| | 3.b.ii Analyses, tests or a combination of analyses and tests of the as-built redundant Class 1E divisions listed in Table 2.5.3-1, ~~and associated field equipment~~ will be performed to verify its electrical independence. | 3.b.ii A report exists and concludes that independence of as-built redundant Class 1E divisions listed in Table 2.5.3-1, ~~and associated field equipment~~ is achieved by independent power sources and electrical circuits for each division, and by fiber optic cable interfaces and qualified isolation devices both at interfaces between redundant divisions and at interfaces between Class 1E systems and non-Class 1E systems. |
| | 3.b.iii Testing, analysis or combination of testing and analysis will be performed for the electrical isolation devices. | 3.b.iii A report exists and concludes that the electrical isolation devices prevent credible faults from propagating into a Class 1E system division. |

# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | **14.03.05** |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-26

Provide design descriptions and a corresponding ITAAC to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P.

10 CFR 50.55a(h)(3) states, in part, that an application filed on or after May 13, 1999, for design certifications 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 5.11, requires, in part that safety system equipment shall be distinctly identified for each redundant portion of a safety system in accordance with the requirements of IEEE Std 384-1981 and IEEE Std 420-1982. The staff could not identify any design descriptions or corresponding ITAACs to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P to meet the requirements of IEEE Std 603-1991, Clause 5.11. As such, the staff requests the applicant to provide design descriptions and a corresponding ITAAC to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P.

## Response

A design description and corresponding ITAAC will be added in Section 2.5.3.1 and Table 2.5.3-3 of DCD Tier 1 to verify that the as-built QIAS-P equipment are distinctly identified for each redundant portion of the QIAS-P.

**Impact on DCD**

Section 2.5.3.1 and Table 2.5.3-3 of DCD Tier 1 will be revised as indicated in the attached mark-up.

**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 the Technical/Topical/Environmental Reports.

2.5.3 Qualified Indication and Alarm System

2.5.3.1 Design Description

The qualified indication and alarm system (QIAS) is a monitoring system that is used to display safety-related information and non-safety information.

The QIAS consists of the two subsystems as follows:

a. QIAS - P, Divisions A and B

b. QIAS - N

In this section, QIAS-N which is non-safety system is not described.

The QIAS-P equipment are located in the auxiliary building.

1. The seismic Category I equipment, identified in Table 2.5.3-1, can withstand seismic design basis loads without loss of its safety function.

2. QIAS-P equipment, identified in Table 2.5.3-1, can withstand the electrical surge, electromagnetic interference (EMI), radio frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist before, during, and following a postulated accidents without loss of its safety function for the time required to perform the safety function.

3.a Class 1E equipment identified in Table 2.5.3-1 is powered from its respective Class 1E train.

3.b Class 1E equipment identified in Table 2.5.3-1, and associated equipment are physically separated and electrically independent from each other and physically separated and electrically independent from non-Class 1E equipment.

4. The QIAS-P monitors and displays the accident monitoring instrumentation variables identified in Table 2.5.3-2.

5. The QIAS-P software is implemented according to the software lifecycle process.

6. Redundant Class 1E equipment listed in Table 2.5.3-1 are provided with means of identification.

Table 2.5.3-3 (3 of 3)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 5. The QIAS-P software is implemented according to the software lifecycle process. | 5.a An inspection will be performed for the requirements phase result summary report of QIAS-P software. | 5.a The requirements phase result summary report exists and concludes that the plant requirements phase activities of QIAS-P software are performed. |
| | 5.b An inspection will be performed for the design phase result summary report of QIAS-P software. | 5.b The design requirements phase result summary report exists and concludes that the design phase activities of QIAS-P software are performed. |
| | 5.c An inspection will be performed for the implementation phase result summary report of QIAS-P software. | 5.c The implementation phase result summary report exists and concludes that the implementation phase activities of QIAS-P software are performed. |
| | 5.d An inspection will be performed for the test phase result summary report of QIAS-P software. | 5.d The test phase result summary report exists and concludes that the test phase activities of QIAS-P software are performed. |
| | 5.e An inspection will be performed for the installation and checkout phase result summary report of QIAS-P software. | 5.e The installation phase result summary report exists and concludes that the installation and checkout phase activities of QIAS-P software are performed. |

An ITAAC to be added to this Table as shown on the next page.

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 6. Redundant Class 1E equipment listed in Table 2.5.3-1 are provided with means of identification. | 6. An inspection of the as-built equipment for conformance with the identification requirements will be performed. | 6. The as-built equipment listed in Table 2.5.3-1 comply with the labeling and the color coding requirements. |

# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-31

Resolve discrepancies in terminology used between APR1400 FSAR Tier 1, Tier 2, and referenced documents, and provide additional information in Tier 2 to support the Tier 1 descriptions regarding the platforms used for the PCS and P-CCS

10 CFR Part 50, Appendix A, GDC 1, requires SSCs important to safety to be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. APR1400 FSAR Tier 1, Section 2.5.5.1, Item 2, and the corresponding design commitment in FSAR Tier 1, Table 2.5.5-1, Item 2 state, “The digital equipment and software used in the PCS and PCCS are independent from those of the [PPS] and the [ESF-CCS].” The acceptance criteria for this ITAAC will verify that the PCS and P-CCS use a platform which is independent from the platform used in the PPS and ESF-CCS and the design group(s) which developed the PCS and P-CCS software is independent from the design group(s) which developed the PPS and ESF-CCS software. APR1400 FSAR Tier 2, Section 7.7.1.1, "Control Systems," states that the control systems are implemented on a digital platform that is diverse in both hardware and software from the safety common platform. Section 4.1 of Technical Report APR1400-Z-J-NR-14002-P, Rev. 0, "Diversity and Defense-in-Depth” states, “The plant-wide data networks are composed of safety networks and non-safety networks. The safety network is independent and diverse from the non-safety network. The non-safety network utilizes different communication hardware, software and communication protocol from the safety network.” Section 6.1.2 (under "Diversity") of this technical report states, “In addition, to correspond with the hardware diversity of these fluid/mechanical systems, the APR1400 employs both hardware and software diversity between control and protection I&C systems to eliminate the potential for CCFs.” The staff could not find discussion of how the plant control system platform are diverse from the safety common platform in APR1400 FSAR Tier 2 or its referenced documents. In addition, APR1400 FSAR Tier 2 does not use the term “independent” (which is used in APR1400 FSAR Tier 1) when discussing the differences between platform and software used for the control system and the platform and software used for the PPS and ESF-CCS. As such, the staff requests the applicant to resolve this discrepancy in terminology, and

provide additional information in Tier 2 to support the Tier 1 descriptions regarding the platforms used for the PCS and P-CCS.

## Response

KHNP had previously addressed the discrepancies related the term “independent” in the response for RAI 68-7892, Question No.07.07-1 (ref. KHNP submittal MKD/NW-15-0101L dated September 2, 2015; ML15245A322).

The response provided was as follows:

> The statement in APR1400 DCD, Tier 1, Table 2.5.5-2, Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Item No. 2, “The digital equipment and software used in the PCS and P-CCS are independent from those of the plant protection system (PPS) and the engineered safety features-component control system (ESF-CCS),” is intended to indicate that safety and non-safety-related digital equipment and software are designed by different software design groups and on different platforms to achieve diversity.
>
> It is understood the word “independent” used in Subsection 2.5.5 and Table 2.5.5-2, Item No.2 cannot be used to describe diversity between the safety and non-safety I&C equipment and software, due to the definition of independence between safety systems and other systems as described in the IEEE Std. 603-1991.
>
> APR1400 DCD, Tier 1, Subsection 2.5.5 and Table 2.5.5-2 will be revised to clearly state diversity exists between the safety and non-safety systems.

The changes proposed by the response to RAI 68-7892 are provided for information in the attachment to this response and are believed to adequately address the terminology discrepancy discussed in this RAI.

As stated in DCD Tier 2, Section 7.1 in regard to the I&C platforms, the safety related I&C systems such as PPS, CPCS, ESF-CCS and QIAS-P are designed using a safety related qualified programmable logic controller (PLC) platform. The non-safety related I&C systems, such as P-CCS and PCS, are designed using a commercially distributed control system (DCS) platform.

Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System," states that the safety related PLC platform uses the Common Q$^{TM}$ platform. However, the non-safety related I&C systems such as P-CCS and PCS are not considered to be any specific DCS platform because the non-safety related I&C system design is considered to be platform-neutral.

The non-safety related I&C systems of the APR1400 will be designed by using different hardware and software from the Common Q$^{TM}$ platform to achieve adequate diversity in design as described in NUREG/CR 6303. Adequate diversity is assured by ITAAC Item No.2 in DCD Tier 1, Section 2.5.5.

---

**Impact on DCD**

There is no impact on the DCD.

**Impact on PRA**

There is no impact on the PRA.

**Impact on Technical Specifications**

There is no impact on the Technical Specifications.

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

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

## 2.5.5 Control System Not Required for Safety

### 2.5.5.1 Design Description

Control system which is not required for safety consists of power control system (PCS) and process-component control system (P-CCS).

The PCS includes the reactor regulating system (RRS), the digital rod control system (DRCS), and the reactor power cutback system (RPCS). The P-CCS includes nuclear steam sypply system (NSSS) process control system (NPCS) and balance of plant (BOP) control systems. The NPCS consists of the feedwater control system (FWCS), the steam bypass control system (SBCS), the pressurizer pressure control system (PPCS), the pressurizer level control system (PLCS), and other miscellaneous NSSS control systems which include reactor makeup control function of the chemical and volume control system (CVCS).

The PCS and P-CCS provide control of functions to maintain the plant within its normal operating range for all normal modes of plant operation.

Control and display interface devices for the PCS and P-CCS are provided in the main control room (MCR) and ~~in the~~ remote shutdown room (RSR) for control and monitoring of the PCS and P-CCS.

diverse

1. The major controllers of the PCS and NPCS are arranged in separate controller groups as identified in Table 2.5.5-1.

2. The digital equipment and software used in the PCS and P-CCS are ~~independent~~ from those of the plant protection system (PPS) and ~~the~~ engineered safety features-component control system (ESF-CCS).

3. The PCS and P-CCS are controlled from either the MCR or RSR, as selected from master transfer switches.

### 2.5.5.2 Inspection, Test, Analyses, and Acceptance Criteria

The inspections, tests, analyses, and associated acceptance criteria for the PCS and P-CCS are specified in Table 2.5.5-2..

MCR/RSR

Table 2.5.5-2

Control System Not Required for Safety ITAAC

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 1. The major controllers of PCS and NPCS are arranged in separate controller groups as identified in Table 2.5.5-1. | 1. Inspection of the as-built PCS and NPCS will be performed. | 1. The as-built PCS and NPCS are arranged in separate controller groups as identified in Table 2.5.5-1. |
| 2. The digital equipment and software used in the PCS and P-CCS are ~~independent~~ from those of the plant protection system (PPS) and ~~the~~ engineered safety features-component control system (ESF-CCS). | 2. Inspection of the as-built PCS and P-CCS equipment will be performed. Inspection of the design documentation will be performed to confirm that the software is developed ~~by independent design groups~~. | 2. The as-built digital equipment and software used in the PCS and P-CCS are ~~independent~~ from those of the PPS and ESF-CCS based on:<br>• PCS and P-CCS use a platform which is ~~independent~~ from the platform used in the PPS and ESF-CCS ~~and~~<br>• The design group(s) which developed the PCS and P-CCS software is ~~independent~~ from the design group(s) which developed the PPS and ESF-CCS software. |
| 3. The PCS and P-CCS are controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches. | 3. A test of the as-built system will be performed to demonstrate the transfer of control capability between the MCR and RSR. | 3. The as-built MCR/RSR master transfer switches transfer controls between the MCR and the RSR for as-built PCS and P-CCS, as follows:<br>• Controls at the RSR are disabled when controls are active in the MCR for the as-built PCS and P-CCS.<br>• Controls at the MCR are disabled when controls are active in the RSR for the as-built PCS and P-CCS. |

diverse

digital equipment and

on a different platform and by a different design group from those of the PPS and ESF-CCS.

different

.

# 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.:** | **317-8271** |
| **SRP Section:** | **14.03.05 – Instrumentation and Controls – Inspections, Tests, Analyses, and Acceptance Criteria** |
| **Application Section:** | **14.03.05** |
| **Date of RAI Issue:** | **11/17/2015** |

## Question No. 14.03.05-33

Modify the use of the term "ESF Initiation" to reflect the intent to reference a portion of the ESFAS.

10 CFR 52.47(a)(2) requires, in part, for the applicant to provide a description and analysis of the structures, systems, and components (SSCs) of the facility, with emphasis upon performance requirements, the bases, with technical justification therefor, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. It is expected that the standard plant will reflect through its design, construction, and operation an extremely low probability for accidents that could result in the release of significant quantities of radioactive fission products. The description shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. APR1400 FSAR Tier 1, Section 2.5.1.1 states that the ESF initiation is performed in sensors, the auxiliary processing cabinet-safety (APC-S) and the ESFAS portion of the PPS cabinets. It appears that the term "ESF initiation" is used to reference a portion of the ESFAS from sensors to the output of the PPS. However, the term “initiation” typically refers to a function and not a system. As such, the staff requests the applicant to modify the use of this term to reflect the intent of referencing a portion of the ESFAS.

## Response

The Engineered Safety Features (ESF) system described in Section 2.5.1.1 is to provide descriptions of the ESF initiation. Section 2.5.1 and Table 2.5.1-5 of DCD Tier 1 will be revised so that “RTS and ESF system” is used considering the system perspective, and “RT and ESF initiation” is used considering the functional perspective.

For consistency of terminology, the ESFAS initiation will be changed to ESF initiation in Section 2.5.4.1 and Table 2.5.4-4 of DCD Tier 1.

---

**Impact on DCD**

Section 2.5.1.1, Section 2.5.4.1, Table 2.5.1-5, and Table 2.5.4-4 of DCD Tier 1 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.

## 2.5 Instrumentation and Control

### 2.5.1 Reactor Trip System and Engineered Safety Features Initiation

#### 2.5.1.1 Design Description

The reactor trip system (RTS) consists of four channels of sensors, auxiliary process cabinet-safety (APC-S) cabinets, ex-core neutron flux monitoring system (ENFMS) cabinets, and four divisions of core protection calculator system (CPCS) cabinets, the reactor protection system (RPS) portion of plant protection system (PPS) cabinets, and reactor trip switchgear system (RTSS) cabinets.

The engineered safety features (ESF) system consists of four sensors, APC-S cabinets, and four divisions of the engineered safety features actuation system (ESFAS) portion of the PPS cabinets and engineered safety feature-component control system (ESF-CCS) cabinets. The ESF initiation is performed in sensors, APC-S cabinets and the ESFAS portion of the PPS cabinets. system (generating ESF initiation signal)

The Subsection 2.5.1 describes the RTS and ESF ~~initiation~~. The ESF-CCS is described in Subsection 2.5.4.

The RTS and ESF initiation equipment is located in the auxiliary building and reactor containment building.

The RTS and ESF system (generating ESF initiation signal) are

The operator module (OM), the maintenance and test panel (MTP), and the interface and test processor (ITP) which are part of the safety I&C system, provide monitoring and testing for the safety-related plant components and instrumentation.

~~The RTS and ESF initiation is~~ designed as follows:

1. The seismic Category I equipment, identified in Table 2.5.1-1 withstand seismic design basis loads without loss of safety function.

2. The Class 1E equipment identified in Table 2.5.1-1 withstand the electrical surge, electromagnetic interference (EMI), radio frequency interference (RFI), and electrostatic discharge (ESD) conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.

7.c The PPS provides indications of the bypassed or inoperable status indication (BISI) on the OM in the MCR for the variables identified in Tables 2.5.1-2 and 2.5.1-3 for RT and ESF initiation.

8. Each PPS division is controlled from either the MCR or the RSR as selected from master transfer switches.

9. The PPS utilizes a 2-out-of-4 coincidence logic when no channels are in trip channel bypass. The PPS converts to a 2-out-of-3 coincidence logic whenever a trip channel bypass is present.

10. Accuracy, response time testing, surveillance testing, and maintenance are applied to determine setpoints for variables of RT and ESF initiation.

11. ~~RTS and ESF initiation software~~ is implemented according to the software life cycle process.
The application software for RT and ESF initiation

12. The cabinets listed in Table 2.5.1-1 have key locks and door open alarms, and are located in a vital area of the facility.

13. The RT logic of the PPS is designed to fail to a safe state such that loss of electrical power to a division of PPS results in a trip condition for that division but the ESFAS logic of the PPS is designed to fail to a safe state such that loss of electrical power to a division of PPS does not result in ESF initiation for that division.

14. Redundant safety equipment listed in Table 2.5.1-1 is provided with means of identification.

15. The input signals of PPS through APC-S or ENFMS are derived from RT and ESF initiation measurement instrumentation that measures monitored variables identified in Tables 2.5.1-2 and 2.5.1-3.

16. The PPS provides RT and ESF initiation signals to meet the required response time for trip and initiation conditions identified in Tables 2.5.1-2 and 2.5.1-3.

17. The Class 1E equipment listed in Table 2.5.1-1 is protected from accident related hazards such as missiles, pipe breaks, and flooding.

18. The RTS and ESF ~~initiation~~ system instrumentation (referenced in Tables 2.5.1-2 and 2.5.1-3) monitors the normal operating, anticipated operational occurrence (AOO), and postulated accident (PA) events.

19. The Class 1E instrument identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function.

20 The PPS providing ~~RTS~~ RT and ESF initiation signals has the testing functions.

21 A single channel of RTS and ESF ~~initiation~~ system is bypassed to allow testing, maintenance or repair and this capability does not prevent the RTS and ESF ~~initiation~~ from performing its safety function.

22. Input sensors from each channel of the RTS and ESF ~~initiation~~ system as identified in Tables 2.5.1-2 and 2.5.1-3 are compared continuously in the information processing system (IPS) to allow detection of out-of-tolerance sensors.

23. Two sets of RTSS which consists of four RTSGs are diverse each other.

2.5.1.2 Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.5.1-5 specifies the inspections, tests, analyses, and associated acceptance criteria for the RTS and ESF ~~initiation~~ system.

Table 2.5.1-5 (4 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 5. The OM in the MCR displays the status information for the variables listed in Tables 2.5.1-2 and 2.5.1-3. | 5. A test of the as-built OM in the MCR will be performed to demonstrate the display capability. | 5. The as-built OM in the MCR have ability to display variables listed in Tables 2.5.1-2 and 2.5.1-3. |
| 6. Each local coincidence logic (LCL) receives trip signals from four channels of bistable processors (BPs) and utilizes 2-out-of-4 coincidence logic to perform RPS and ESF initiation functions identified in Tables 2.5.1-2 and 2.5.1-3. | 6. A test will be performed using simulated input signals for RPS and ESFAS process inputs to each channel of the BPs. | 6. Each division of LCL receives RPS and ESFAS trip signals from four channels of BP, performs 2-out-of-4 coincidence logic for each RPS and NSSS ESF ~~ESFAS~~ initiation function identified in Tables 2.5.1-2 and 2.5.1-3 and sends the RPS initiation signals to the RTSS and ESFAS initiation signals to the ESF-CCS. |
| 7.a The PPS provides manual trip bypasses on the MTP switch panel, for RT and ESF initiation identified in Tables 2.5.1-2 and 2.5.1-3 respectively. | 7.a A test of the as-built PPS system will be performed on the MTP switch panel by initiating manual bypass for RT and the ESF initiation as identified in Tables 2.5.1-2 and 2.5.1-3. | 7.a Trip signals are manually bypassed on the MTP switch panel as identified in Tables 2.5.1-2 and 2.5.1-3 for RT and ESF initiation. |
| 7.b The PPS automatically removes the operating bypasses listed in Table 2.5.1-4 when permissive conditions are not met. | 7.b A test of the as-built PPS operating bypasses listed in Table 2.5.1-4 will be performed. | 7.b The as-built PPS operating bypasses listed in Table 2.5.1-4 are accepted only when the variables are within operating bypass permissive range. When a variable exceeds the permissive setpoint, the operating bypass is automatically removed. |
| 7.c The PPS provides indications of the bypassed or inoperable status indication (BISI) on the OM in the MCR for the variables identified in Tables 2.5.1-2 and 2.5.1-3 for RT and ESF initiation. | 7.c A test of the as-built PPS system will be performed on the as-built OM in the MCR by initiating manual bypass for variables identified in Tables 2.5.1-2 and 2.5.1-3 for RT and the ESF initiation. | 7.c The as-built OM provides indications of the bypassed or inoperable status indication (BISI) for the variables identified in Tables 2.5.1-2 and 2.5.1-3 for RT and ESF initiation. |

The application software for RT and ESF initiation

Table 2.5.1-5 (6 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 11. ~~RTS and ESF initiation software~~ is implemented according to the software lifecycle process. | 11.a An inspection will be performed for the requirements phase result summary report. | 11.a The requirements phase result summary report exists and concludes that the plant requirements phase activities o are performed. |
| | 11.b An inspection will be performed for the design phase result summary report. | 11.b The design requirements phase result summary report exists and concludes that the design phase activities are performed. |
| | 11.c An inspection will be performed for the implementation phase result summary report. | 11.c The implementation phase result summary report exists and concludes that the implementation phase activities are performed. |
| | 11.d An inspection will be performed for the test phase result summary report. | 11.d The test phase result summary report exists and concludes that the test phase activities are performed. |
| | 11.e An inspection will be performed for the installation and checkout phase result summary report. | 11.e The installation phase result summary report exists and concludes that the installation and checkout phase activities are performed. |

Table 2.5.1-5 (8 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 16. The PPS provides RT and ESF initiation signals to meet the required response time for trip and initiation conditions identified in Tables 2.5.1-2 and 2.5.1-3. | 16.a Type tests and analyses will be performed on PPS to verify that the PPS initiates RT and the ESF initiation signals identified in Tables 2.5.1-2 and 2.5.1-3 within response time requirements described in the design basis. | 16.a A report exists and concludes that the PPS initiates the RT and the ESF ~~f~~initiation signals identified in Tables 2.5.1-2 and 2.5.1-3 within the response time requirements as described in the design basis. |
| | 16.b ~~Inspections~~ will be performed on the as-built ~~RTS~~ and ESF initiation signals identified as monitored variables in Tables 2.5.1-2 and 2.5.1-3 with response time requirements. | 16.b The as-built ~~RTS~~ and ESF initiation signals identified as monitored variables in Tables 2.5.1-2 and 2.5.1-3 with response time requirements are bounded by the tests. |
| 17. The Class 1E equipment listed in Table 2.5.1-1 is protected from accident related hazards such as missiles, pipe breaks, and flooding. | 17. Inspections and analyses will be performed on the locations of the as-built Class 1E equipment listed in Table 2.5.1-1. | 17. A report exists and concludes that the as-built equipment listed in Table 2.5.1-1 is protected from accident related hazards such as missiles, pipe breaks and flooding. |
| 18. The RTS and ESF ~~initiation~~ instrumentation (referenced in Tables 2.5.1-2 and 2.5.1-3) monitors the normal operating, anticipated operational occurrence (AOO), and postulated accident (PA) events. | 18. An inspection of the as-built RTS and ESF ~~initiation~~ instrumentation will be performed. | 18. The as-built RTS and ESF ~~initiation~~ instrumentation (referenced in Tables 2.5.1-2 and 2.5.1-3) functions during normal operation, AOO, and PA conditions. |

Delete.

Tests

RT

system

Table 2.5.1-5 (9 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 19. The Class 1E instruments identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function. | 19.a Type tests, analyses, or a combination of type tests and analyses will be performed on Class 1E instruments located in a harsh environment. | 19.a A report exists and concludes that the Class 1E instrument identified in Table 2.5.1-1 as being qualified for a harsh environment can withstand the environmental conditions that would exist before, during, and following a design basis accident without loss of safety function for the time required to perform the safety function. |
| | 19.b Inspections will be performed on the as-built Class 1E instruments identified in Table 2.5.1-1 and the associated wiring, cables, and terminations located in a harsh environment. | 19.b A report exists and concludes that the as-built Class 1E instruments and the associated wiring, cables, and terminations identified in Table 2.5.1-1 as being qualified for a harsh environment are bounded by type tests, analyses, or a combination of type tests and analyses. |
| 20. The PPS providing ~~RTS~~ and ESF initiation signals has the testing functions. | 20. Type tests and analyses of the PPS providing ~~RTS~~ and ESF initiation signals will be performed using simulated failure condition. | 20. A report exists and concludes that the PPS providing ~~RTS~~ and ESF initiation signals has the testing functions to detect malfunctioning components or modules and have them replaced, repaired, or adjusted. |

RT

Table 2.5.1-5 (10 of 10)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 21. A single channel of RTS and ESF ~~initiation~~ is bypassed to allow testing, maintenance or repair and this capability does not prevent the RTS and ESF ~~initiation~~ from performing its safety function. | 21. A test will be performed on the 2-out-of-4 voting logic in the as-built RTS and ESF ~~initiation~~ by providing simulated process signals, identified in Tables 2.5.1-2 and 2.5.1-3, to at least two of three non-bypassed channels of the as-built RTS and ESF ~~initiation~~ input under the manual single division bypass operation from the as-built the maintenance and test panel (MTP) in the MCR. | 21. When the 2-out-of-4 voting logic in the non-bypassed divisions of each as-built RTS and ESF ~~initiation~~ receives at least two of three actuation signals, identified in Tables 2.5.1-2 and Table 2.5.1-3, from the respective non-bypassed channels, the 2-out-of-4 voting logic in the non-bypassed divisions of each as-built RTS and ESF ~~initiation~~ provides the actuation signal for the reactor trip and automatic ESF functions identified in the tables. |
| 22. Input sensors from each channel of the RTS and ESF ~~initiation~~ as identified in Tables 2.5.1-2 and 2.5.1-3 are compared continuously in the information processing system (IPS) to allow detection of out-of-tolerance sensors. | 22. A test of the as-built IPS will be performed by providing The simulated inputs for each monitored variable identified in Tables 2.5.1-2 and 2.5.1-3 which includes one out-of-tolerance , at the as-built RTS and ESF ~~initiation~~ input. | 22. An alarm for the out-of-tolerance sensor detection is displayed on the as-built IPS in the MCR when the IPS receives simulated input signals for each monitored variable identified in Tables 2.5.1-2 and 2.5.1-3 which includes one out-of-tolerance signal. |
| 23. Two sets of RTSS which consists of four RTSGs are diverse each other. | 23. Inspection of the as-built RTSS equipment will be performed. | 23. Two sets of the as-built RTSS which consists of four RTSGs are diverse each other.: One set of RTSGs is supplied from a different manufacturer than the other set of RTSGs. |

system

system

system

system

## 2.5.4 Engineered Safety Features-Component Control System

### 2.5.4.1 Design Description

The engineered safety features (ESF) system consists of sensors, auxiliary process cabinet-safety (APC-S), the engineered safety features actuation system (ESFAS) portion of the plant protection system (PPS) and engineered safety features-component control system (ESF-CCS). The sensors, APC-S and the ESFAS portion of the PPS are described in Subsection 2.5.1. Subsection 2.5.4 describes the ESF-CCS.

The ESF-CCS provides automatic actuation of ESF systems. The ESF-CCS performs the nuclear steam supply system (NSSS) ESFAS function, balance of plant (BOP) ESFAS function, and emergency diesel generator (EDG) loading sequencer function.

The ESF-CCS generates the NSSS ESF actuation signals upon receipt of ~~ESFAS~~ ESF initiation signals from the PPS. The ESF-CCS generates the BOP ESF actuation signals upon receipt of initiation signals from the process and effluent radiation monitoring system (RMS).

The ESF-CCS generates the EDG loading sequencer signals upon receipt of loss of power to Class 1E train buses, safety injection actuation signal (SIAS), containment spray actuation signal (CSAS), and auxiliary feedwater actuation signal (AFAS).

The ESF-CCS provides the capability for manual actuation of ESF systems and manual control of ESF components.

The ESF-CCS consists of four divisions of group controller cabinets and loop controller cabinets. The ESF-CCS equipment and manual control components are identified in Table 2.5.4-1. The ESF-CCS components are located in auxiliary building.

The ESF-CCS design incorporates the following features: processors arranged in primary and standby processor configurations within each ESF-CCS division. ESFAS functions are divided into the ESF-CCS distributed segments which receive the ESF actuation signals from the PPS through the fiber optic cable. Separation is provided between protection ESFAS processing function and auxiliary functions of human-system interfaces, data communication and automatic testing. Serial data link support the transmission of protection data on a continuous cyclical basis independent of plant transients.

1. The seismic Category I equipment and components identified in Table 2.5.4-1 withstand seismic design basis loads without loss of the safety function.

2. Redundant Class 1E divisions listed in Table 2.5.4-1 and associated field equipment are physically separated and electrically isolated from each other and physically separated and electrically isolated from non-Class 1E equipment.

3. The Class 1E equipment and components identified in Table 2.5.4-1 are powered from its respective Class 1E train.

4. Each ESF-CCS division receives ~~ESFAS~~ initiation signals from four divisions of the PPS and performs selective 2-out-of-4 coincidence logic to perform NSSS ESF actuation functions identified in Table 2.5.4-2.

5. Each ESF-CCS division receives ~~ESFAS~~ initiation signals from two divisions of the RMS as shown in Tables 2.7.6.4-2 and 2.7.6.5-2 and performs 1-out-of-2 logic taken twice except the fuel handling area emergency ventilation actuation signal which has one 1-out-of-2 logic to perform the BOP ESF actuation functions identified in Table 2.5.4-2.

6. Upon receipt of a SIAS, CSAS, or AFAS, the ESF-CCS initiates an automatic start of the EDGs and automatic EDG loading sequencer of ESF loads identified in Table 2.5.4-2.

7. Upon detecting loss of power to Class 1E buses, the ESF-CCS initiates startup of the EDGs, shedding of electrical loads, transfer of Class 1E bus connections to the EDGs, and EDG loading sequencer to the reloading of safety-related loads to the Class 1E buses.

8. Each ESF-CCS division is controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches.

9. Once a BOP ESF actuation has been actuated (automatically or manually), the ESF actuation logic is latched in the actuated state and is not reset automatically

Table 2.5.4-4 (2 of 7)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 2. (cont.) | 2.b A test, analysis, or a combination of a test and analysis of the as-built redundant Class 1E divisions listed in Table 2.5.4-1and associated field equipment will be performed to verify its electrical independence. | 2.b A report exists and concludes that independence of as-built redundant Class 1E divisions listed in Table 2.5.4-1 and associated field equipment is achieved by independent power sources and electrical circuits for each division, and by fiber-optic cable interfaces, conventional isolators, or other qualified isolation methods or devices at interfaces between redundant divisions, and at interfaces between safety and non-safety systems. |
| | 2.c A test, analysis, or a combination of a test and analysis will be performed for the electrical isolation devices. | 2.c A report exists and concludes that the electrical isolation devices prevent credible faults from propagating into a safety system division. |
| 3. The Class 1E equipment and components identified in Table 2.5.4-1 are powered from its respective Class 1E train. | 3. A test of the as-built ESF-CCS will be performed by providing a simulated test signal in only one Class 1E train at a time. | 3. The Class 1E equipment and components identified in Table 2.5.4-1 are powered from its respective Class 1E train. |
| 4. Each ESF-CCS division receives ~~ESFAS~~ initiation signals from four divisions of the PPS and performs selective 2-out-of-4 coincidence logic to perform NSSS ESF actuation functions identified in Table 2.5.4-2. | 4. A test will be performed using simulated input signals for ESF actuation signal input to each division of the as-built ESF-CCS. | 4. Each ESF-CCS division receives ~~ESFAS~~ initiation signal from four divisions of the PPS and performs selective 2-out-of-4 coincidence logic for each NSSS ESF actuation function identified in Table 2.5.4-2 and sends the control signals to the ESF components. |

ESF

Table 2.5.4-4 (3 of 7)

| Design Commitment | Inspections, Tests, Analyses | Acceptance Criteria |
|---|---|---|
| 5. Each ESF-CCS division receives ~~ESFAS~~ initiation signals from two divisions of the RMS as shown in Tables 2.7.6.4-2 and 2.7.6.5-2 and performs 1-out-of-2 logic taken twice except the fuel handling area emergency ventilation actuation signal which has one 1-out-of-2 logic to perform the BOP ESF actuation functions identified in Table 2.5.4-2. | 5. A test will be performed using simulated input signals for initiation input to each division of the as-built ESF-CCS. | 5. Each ESF-CCS division receives ~~ESFAS~~ initiation signals from two divisions of the RMS, performs 1-out-of-2 logic taken twice except the fuel handling area emergency ventilation actuation signal which has one 1-out-of-2 logic for each BOP ESF actuation function identified in Table 2.5.4-2 and sends the control signals to the ESF components. |
| 6. Upon receipt of a SIAS, CSAS, or AFAS, the ESF-CCS initiates an automatic start of the EDGs and automatic EDG loading sequencer of ESF loads identified in Table 2.5.4-2. | 6. A test will be performed using simulated input signals for initiation input to each division of the as-built ESF-CCS. | 6. Each ESF-CCS division receives a SIAS, CSAS, or AFAS and initiate an automatic start of the EDGs and automatic loading sequencer of ESF loads identified in Table 2.5.4-2. |
| 7. Upon detecting loss of power to Class 1E buses, the ESF-CCS initiates startup of the EDGs, shedding of electrical loads, transfer of Class 1E bus connections to the EDGs, and EDG loading sequencer to the reloading of safety-related loads to the Class 1E buses. | 7. A test will be performed using simulated input signals for initiation input to each division of the as-built ESF-CCS. | 7. Each ESF-CCS division receives loss of power to Class 1E buses, and initiate an automatic start of the EDGs, shedding of electrical loads, transfer of Class 1E bus connections to the EDGs, and sequencing to the reloading of safety-related loads to the Class 1E buses. |
| 8. Each ESF-CCS division is controlled from either the MCR or RSR, as selected from MCR/RSR master transfer switches. | 8. A test of the as-built system for one control within each ESF-CCS division will be performed to demonstrate the transfer of control capability between the MCR and RSR. | 8. The as-built master transfer switches transfer controls between the MCR and RSR separately for each as-built ESF-CCS division, as follows:<br>a. Controls in the RSR are disabled when controls are active in the MCR.<br>b. Controls in the MCR are disabled when controls are active in the RSR. |