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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**07.02**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-1

For all figures in:

- APR1400 Final Safety Analysis Report (FSAR), Tier 2, Chapter 7, Rev. 0,
- Technical Report APR1400-Z-J-NR-14001, Revision 0, “Safety I&C System,” and
- Technical Report APR1400-F-C-NR-14003, Rev. 0, “Functional Design Requirement for a CPCS [Core Protection Calculator System] for APR1400,”

where the figures display only one division/channel (i.e., FSAR, Tier 2, Figure 7.2-10, “PPS Channel A Trip Path Diagram”) and where the schematics or diagrams of the figure display differences between the divisions/channels (i.e., FSAR, Tier 2, Figure 7.2-32, “Functional Logic Diagram for CWP”), insert a caption on the figures explaining whether the schematic or diagram shown is identical for all divisions/channels or insert a caption that describes what the differences are between the divisions/channels.

The regulatory requirements of 10 CFR 52.47(a)(2) state that the design “…descriptions shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations.” Standard Review Plan (SRP) Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the design basis information provided for each design basis item, taken alone and in combination, should have one and only one interpretation and that information provided for the design basis items should be technically accurate. The NRC staff was not able to understand the system design or system functional design requirements for figures displaying differences between divisions/channels and for figures displaying only one division/channel of safety system functionality. Update the FSAR and technical reports accordingly.

Response

The schematics or diagrams, not identifying whether it applies to all channels or divisions, in the figures of DCD Tier 2 Chapter 7, Safety I&C Technical Report, and Functional Design Requirement for a Core Protection Calculator System (CPCS) are identical for all channels or divisions.

The trip path shown in Figure 7.2-10 of DCD Tier 2 is identical for all PPS channels. The functional logic diagram for CWP in Figure 7.2-32 of DCD Tier 2 identifies the difference between divisions in the figure. Therefore, no caption or description is required to be inserted to these cases.

The description of identification is inserted into Figure 7.2-28 of DCD Tier 2 as shown in the attached mark-up for the case where some portion of the diagram shown in the figure is specific to certain channels or divisions. In this case, the manual reactor trip in RSR is applicable only for PPS divisions A and B. The remaining portion of the diagram in this figure is identical for all PPS divisions.

No additional figures in DCD Tier 2 are found to be applicable to have a caption describing the differences between channels or divisions.

No figures in Safety I&C System Technical Report are found to be applicable to have a caption describing the differences between channels or divisions.

No figures in Functional Design Requirement for a CPCS for APR1400 are found to be applicable to have a caption describing the differences between channels or divisions.

The following phrase is added to Section 7.1 of DCD Tier 2:
“All figures provided in Chapter 7 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference.”

The following phrase is added to Section 4.1 of Safety I&C System Technical Report:
“All figures provided in Section 4 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference.”

The following phrase is added to Section 1.2 of Functional Design Requirement for a CPCS for APR1400:
“All figures provided in this document are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference.”

Impact on DCD

Section 7.1 and Figure 7.2-28 of DCD Tier 2 will be revised as indicated on 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

Section 4.1 of the Safety I&C System Technical Report(APR1400-Z-J-NR-14001-NP, Rev.0) will be revised as indicated on the attached mark-up.

Section 1.2 of Functional Design Requirement for a CPCS for APR1400(APR1400-F-C-NR-14003-NP, Rev.0) will be revised as indicated on the attached mark-up.

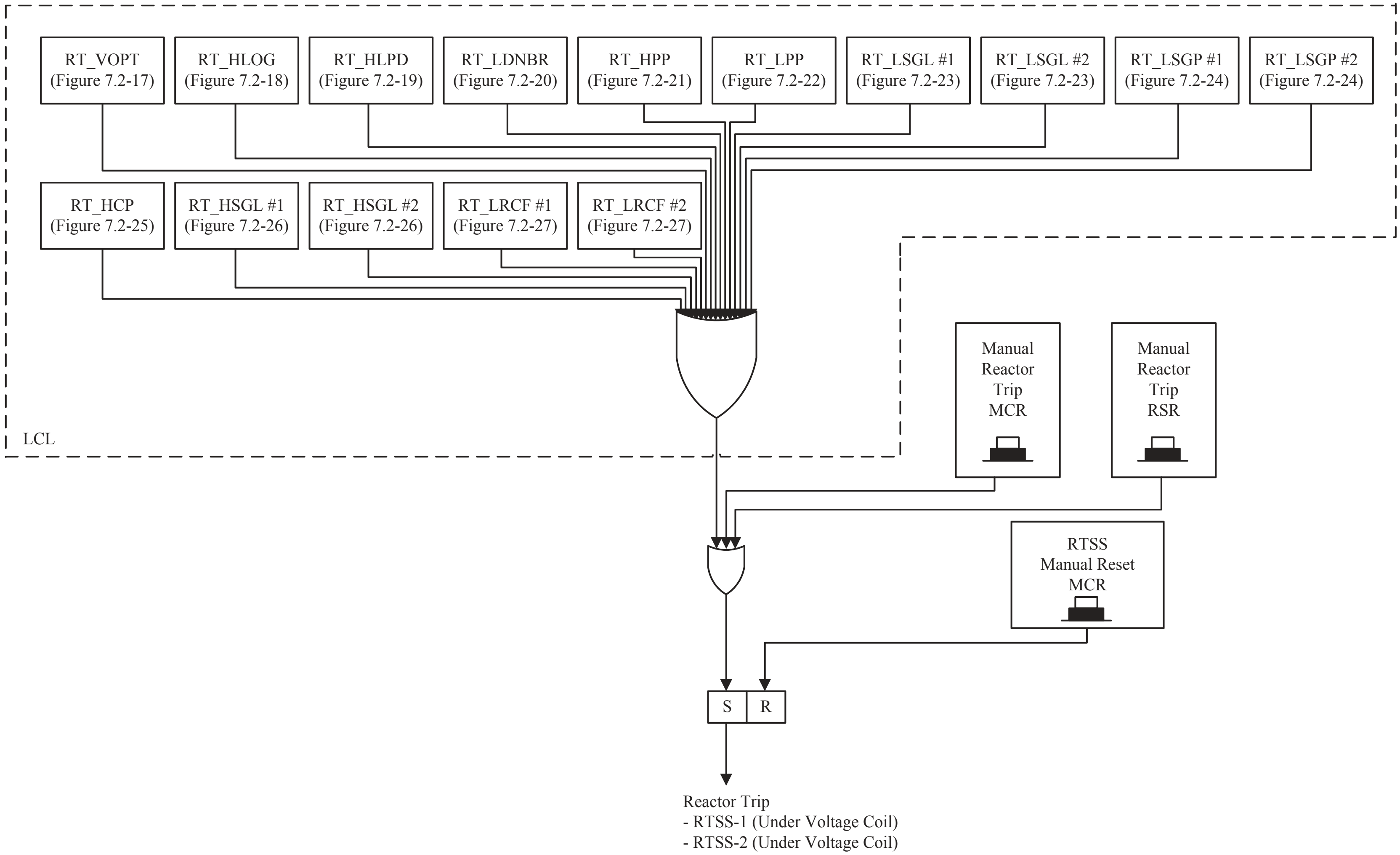
RT_VOPT (Figure 7.2-17)
RT_HLOG (Figure 7.2-18)
RT_HLPD (Figure 7.2-19)
RT_LDNBR (Figure 7.2-20)
RT_HPP (Figure 7.2-21)
RT_LPP (Figure 7.2-22)
RT_LSGL #1 (Figure 7.2-23)
RT_LSGL #2 (Figure 7.2-23)
RT_LSGP #1 (Figure 7.2-24)
RT_LSGP #2 (Figure 7.2-24)
RT_HCP (Figure 7.2-25)
RT_HSGL #1 (Figure 7.2-26)
RT_HSGL #2 (Figure 7.2-26)
RT_LRCF #1 (Figure 7.2-27)
RT_LRCF #2 (Figure 7.2-27)
LCL
Manual Reactor Trip MCR
Manual Reactor Trip RSR
RTSS Manual Reset MCR
S
R
Reactor Trip
- RTSS-1 (Under Voltage Coil)
- RTSS-2 (Under Voltage Coil)

Figure 7.2-28 Functional Logic Diagram for Reactor Trip Signal Generation

Note:
The manual reactor trip switches in the RSR are provided only for divisions A and B.

CHAPTER 7 – INSTRUMENTATION AND CONTROLS

7.1 Introduction

The APR1400 instrumentation and control (I&C) system uses advanced design features such as digital data communication, a network-based distributed digital control system, and a compact workstation-based human-system interface (HSI) in the control room.

The I&C architecture of the APR1400 is implemented by two major independent and diverse platforms: (1) safety-qualified programmable logic controller (PLC) platform for the safety systems and (2) non-qualified distributed control system (DCS) platform for the data processing system and non-safety control systems. In addition, independent systems such as the turbine/generator (T/G) control and protection system, the nuclear steam supply system (NSSS) monitoring system, and the balance of plant (BOP) monitoring system perform the required functions of a portion of the I&C systems.

Table 3.2-1 provides the safety classifications and quality groups of the APR1400 systems.

Safety Systems

The safety systems are implemented by safety-grade hardware and previously developed software components that are dedicated or qualified for use in nuclear power plants. The PLC platform is loaded with the APR1400-specific application software to implement various safety functions.

The components of the safety system are qualified to satisfy nuclear requirements such as environmental, seismic, electromagnetic interference (EMI), and radio frequency interference (RFI) qualifications. The safety system software is designed, verified, and validated using the industry standard for software development and the verification and validation (V&V) process as described in the Software Program Manual Technical Report (Reference 1). The qualified PLC platform applies to the following safety systems:

a. Plant protection system (PPS)

b. Core protection calculator system (CPCS)

c. Engineered safety features – component control system (ESF-CCS)

All figures provided in Chapter 7 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided to indicate the difference.

communication via the serial data link (SDL, i.e., HSL) from safety systems to non-safety systems (i.e., QIAS-N) and buffering circuit using dual-ported memory are commonly used to prevent endangering the safety function. The other means from safety to non-safety data communication is via the plant computer datalink using the unidirectional protocol from the MTP.

- The DPS is diverse from the safety I&C system in aspects of trip mechanism, hardware and software.
- In addition to the DPS, the hardwired DMA switches and the DIS are provided on the MCR SC to cope with CCF of the safety I&C system.

4.1.1 Safety I&C Systems

4.1.1.1 Plant Protection System

The PPS consists of four redundant divisions that perform the necessary bistable, coincidence, initiation logic, maintenance and test function.

The PPS initiates reactor trip and system-level ESF actuation functions when a safety limit is exceeded by the plant conditions. To detect such conditions, the system utilizes measurements of the reactor core, reactor coolant system, main steam supply system, and containment building parameters.

Each PPS redundant division receives the process and discrete signals directly from field sensors or via the APC-S, ENFMS, and CPCS. The PPS provides the reactor trip signals to the RTSS using hardwired cables and ESFAS initiation signals to the ESF-CCS via fiber optic SDLs.

4.1.1.2 Engineered Safety Features - Component Control System

The ESF-CCS consists of four independent divisions that perform additional 2-out-of-4 voting logic, component control logic, and priority logic function.

The group controller (GC) of each ESF-CCS division receives four division ESFAS initiation signals derived from the ESFAS portion of the PPS and performs additional selective 2-out-of-4 coincidence logic to generate the ESF actuation signal. The GC also receives two division ESFAS initiation signals derived from the radiation monitoring system (RMS) and performs 1-out-of-2 logic to generate the ESF actuation signal. The ESF actuation signals are transmitted to the loop controller (LC) of the ESF-CCS. The LC executes the component control logic and outputs the component control signal to the CIM. The component control logic includes the priority logic for the operator’s manual control signal and ESF actuation signal. The ESF-CCS soft control module (ESCM) on the operator console generates a component control signal of safety components by manual operator actions.

4.1.1.3 Core Protection Calculator System

The CPCS has four redundant channels that compute the DNBR and LPD values using process values, reactor coolant pump (RCP) speed, CEA position and ex-core neutron flux.

The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed a safety limit, a trip signal is transmitted to the PPS using hardwired cables.

4.1.1.4 Qualified Indication and Alarm System - P

The QIAS-P, which has two independent divisions A and B, is implemented on the common PLC platform for the safety system. The QIAS-P processes the plant parameters that are input from the safety I&C

All figures provided in Section 4 are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided in the figure to indicate the difference.

1.0 INTRODUCTION

1.1 PURPOSE

The purpose of this document is to provide a description of the Core Protection Calculator System (CPCS) Algorithm functional design with Common Qualified (Common Q) platform. The Functional Design Requirements described in this document when implemented with appropriate data base and addressable constants meet the design bases for CPCS given in Section 2.

1.2 SCOPE

The CPCS design consists of three major components: executive software, application software, and hardware. This functional design requirements document provides the following:

1) A description of reactor protection algorithms to be implemented as the application software,

2) The requirements on protection program interfaces, system interfaces, protection program timing, and system initialization,

3) A description of CEA Penalty Factor Algorithm to be implemented in the Core Protection Calculator System of the Reactor Protection System,

4) A description of algorithms to initiate alarms for CEA sensor failure and CEA deviation,

5) A description of diagnostic failed sensor data stack,

Items (1) through (5) establish functional requirements affecting the three major CPCS components.

1.3 APPLICABILITY

This document is a generic description of CPCS Functional Design Requirements. This document is prepared based on the Ref. 1.4.1.

It is currently applicable to Advanced Power Reactor 1400 (APR1400).

1.4 REQUIRED REFERENCES

1.4.1 KNF, "Functional Design Requirements for a Core Protection Calculator System for Shinkori Nuclear Power Plant Units 3&4," KNF-S34ICD-08005, Rev. 01, September 2010.

All figures provided in this document are identical for all channels or divisions. If a figure provided is not identical for all channels or divisions, a note is provided in the figure to indicate the difference.

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**07.02**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-2

Define the reverse order logic trip operation of the reactor protection system (RPS) bistable processors (BP) as software diversity per the software diversity guidance of NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems,” December 1994.

10 CFR Part 50, Appendix A, GDC 22, "Protection System Independence" states, in part, that 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. The guidance of NUREG/CR-6303, states in Section 3.2.6, “Software Diversity,” that software must differ significantly in parameters, dynamics, and logic, to be considered diverse. Technical Reports APR1400-Z-J-NR-14001-P, Rev. 0, "Safety I&C System," and APR1400-Z-J-NR-14002-P, Rev. 0, "Diversity and Defense in Depth" both state that each BP within a division processes the bistable logic trip function in the reverse order to that of the other BP for software functional diversity (i.e. BP1 in Rack 1 executes sequence 1 through N while BP2 in Rack 2 executes in the reverse sequence, N through 1). NUREG/CR-6303 does not list a diversity category as "software functional diversity," but does identify software diversity and functional diversity. Clarify whether the diversity described is software diversity, functional diversity, or if it accomplishes both, and provide the basis for the determination. In addition, describe how effective the reverse order of operation would be at addressing software faults (e.g., what types of faults does it address and how does the relatively short operational cycles (in the order of milliseconds) impact the effectives of this type of diversity). Update the applicable technical reports accordingly.

Response

Clarification

The "reverse order of operation" is applied to increase the degree of "software diversity" between BP1 and BP2.

The guidance of NUREG/CR-6303 describes in Section 3.2.6 "Software Diversity," that the use of different order of execution increases diversity.

The term "software functional diversity" in the Safety I&C System Technical Report and the term "functional diversity" in the Diversity and Defense in Depth Technical Report are used to indicate that the "reverse order of operation" between BP1 and BP2 increases the degree of software diversity. For clarity and consistency, both terms will be modified to "software diversity" as follows:

[Section 4.2.2.1 of the Safety I&C System Technical Report]
Before: "for software functional diversity"
After: "to increase the degree of software diversity"

[Section 6.1.2 of the Defense in Depth Technical Report]
Before: "provides functional diversity within the PPS"
After: "increases the degree of software diversity"

Reverse order of Operation

The effectiveness of the reverse order of operation described in Section 4.2.2.1 of the Safety I&C System Technical Report can be illustrated with the following case:

> *For this particular case, it is assumed that there are a total of 20 respective BP trip parameter logics to be executed in both BP1 and BP2 application software for the PPS. Another assumption of this case is that the application program no longer continues, but repeats over and over from the start of the program to the error point.*
>
> *If BP trip parameter logic #4 has an error in both BP1 and BP2 application software, then BP1 happens to execute the BP trip parameter logics #1 through #3 only, not being able to execute #4 through #20. This will continue over and over in each scan cycle time until the error in BP trip parameter logic #4 is fixed. In the meantime, BP2 executes the BP trip parameter logics #20 through #5 only, not being able to execute #4 through #1.*
>
> *This covers all the BP trip parameter logics except for the trip parameter logic with the error (#4).*

The above case is unlikely to occur and is only assumed to be the case for illustration of the effectiveness of the reverse order of operation of BPs.

The proper safety functions performed by all BP trip parameter logics would not be achieved if the reverse order of operation is not applied to the BPs. With this type of diversity, the safety function for BP trip parameters would be successfully achieved except for the BP trip parameter with the error.

The length of the operational cycle time does not affect the effectiveness of reverse order of operation because it is a matter of execution order in the BP trip parameter logics, not a matter of length of the operational cycle time.

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 4.2.2.1 of the Safety I&C System Technical Report(APR1400-Z-J-NR-14001-NP, Rev.0) and Section 6.1.2 of the Diversity and Defense in Depth Technical Report(APR1400-Z-J-NR-14002-NP, Rev.0) will be modified as indicated on the attached mark-up.

- The heartbeat signal of the BP is supervised by the LCL to ensure appropriate trip signals are generated for the reactor trip function.

- Each PPS LCL RT processor is supervised by the built-in watchdog timer (WDT). The contacts outputs of WDT are hardwired in series to the RPS initiation circuit to ensure appropriate trip signals are generated for the reactor trip function as shown in Figure 4-7. The detailed information on hardware watchdog timer configuration and relations to fail-safe operation are provided in Reference 12.

The hardware and software for the PPS meet the SFC outlined in IEEE Std. 603-1991 and IEEE Std. 379 as endorsed by RG 1.53 and RG 1.153.

The PPS is designed to detect any error condition of the PPS through the self-diagnostic and supervisory functions such as I/O module diagnostic, processor module diagnostic, application program CRC, communication error CRC, and etc. The detailed information is provided in Reference 12.

The PPS software execution is deterministic to ensure predictable system performance and response under worst-case plant loading condition. The task scheduler schedules the execution of the application programs and periodic system software tasks based on predefined priorities. The detailed information of the deterministic performance and the deterministic performance is provided in Reference 12.

Each PPS division contains a BP and LCL racks. Each BP sends its bistable trip status to each redundant LCL processors in the same division via non-fiber optic SDL and to other redundant divisions' LCL racks via fiber optic SDL. The redundant LCL racks within each division receive the bistable trip signals and perform the 2-out-of-4 local coincidence logic for each RT and ESFAS function. Each LCL rack has digital output (DO) module(s) whose outputs are combined to form the selective 2-out-of-4 coincidence initiation circuit. The configuration is shown in Figure 4-5.

The system, including the processor modules, is subject to continuous hardware monitoring and annunciation of failures to maximize system availability. A watchdog timer within the processor modules monitors the operability of the processor modules (PMs). Refer to Section 5.2.1.3 in Reference 12.

The PPS has redundancy and diversity features. Redundant PPS analog input parameters considering DBEs are assigned to each analog input module for minimizing the effects of a single failure of an analog input (AI) module as shown in Figure 4-5. Each BP processes the bistable logic in the reverse order to that of the other BP ~~for software functional~~ to increase the degree of software diversity. The design includes redundant BP racks in each division. The independent configuration of the I/O and communication devices in redundant cabinets is provided.

The selective 2-out-of-4 initiation logic combination of RPS initiation signals is designed to permit testing of the LCL processor without causing RT initiation in a division and still permit valid trip signals to propagate to the RTSS. This design provides hot swap capability for a single PLC module, without causing an output initiation signal. A design goal is to enhance the system's fault tolerance by accommodating a single processor module or SDL data communication link failure in the division without causing a division trip or component actuation (i.e., reactor trip circuit breaker opening or auxiliary feedwater pump/valve operation).

The PPS provides alarms to the QIAS-N and IPS to indicate system abnormalities. The PPS provides status alarms to the QIAS-N via the SDN (to the ITP), and SDL (from the ITP to the QIAS-N). The PPS also provides status alarms to the IPS via the MTP and divisionalized gateways to the DCS network

The PPS cabinets are powered by a single 120 Vac vital bus. The PPS is configured with redundant internal power supplies in each cabinet. The DC output is auctioneered. This makes the PPS safety

6 DIVERSITY AND DEFENSE-IN-DEPTH ANALYSIS

6.1 Design Approach

The APR1400 design methods and features related with the D3 include the following:

6.1.1 Elimination of Predictable CCFs

The hardware related failures due to common stressors are avoided through environmental, seismic, EMI qualification, aging analyses, and spatial separation of equipment. These are considered predictable CCFs because the testing is designed to reveal susceptibility to external effects that could affect redundant hardware elements in a system (and thus disable the system). Fire is an external effect that is defended by separation of redundant elements of a system, such as placing them in different rooms.

6.1.2 Design of Highly Reliable Software

A rigorous software lifecycle design process is used to minimize postulated CCF errors for the APR1400 safety I&C systems. This approach is summarized as follows:

Deterministic Design – The algorithm execution in the APR1400 safety I&C systems is deterministic. This means that data is updated on a continuous cycle and programs execute on a continuous basis. This approach makes the software easier to design, verify and validate. The potential for hidden errors is significantly lower than in other designs that include event based execution, or event based data communication

Simplicity – The reactor protection and ESF actuation functions are accomplished with PLCs. PLCs are widely used, simple, proven digital devices that utilize logic without branching, interrupts or other complex features. Programming and testing PLCs to accomplish the required functions is easily understood and verified.

Field Proven Products - Operating system software for the APR1400 safety I&C system is selected with field experience in similar applications. These products are mature and, therefore, demonstrated to be free of design errors.

Verification and Validation (V&V) - For custom (application) software, a comprehensive V&V program is employed, including independent document reviews and independent tests. Application software is subject to a documented and rigorous V&V program. Independence is maintained between software development and verification personnel. The configuration controls are also imposed throughout the software life cycle. A rigorous software life cycle design process and associated independent V&V program minimizes the potential for CCF errors throughout the software lifecycle design process as described in the Software Program Manual Technical Report (Reference 14).

Segmentation - Within the APR1400 safety I&C systems, functions are divided among separate processors. There are two (2) bistable racks per PPS channel. Each rack includes one (1) bistable processor (BP) and its own input modules. Both BPs share all monitored process input parameters. One (1) BP executes its trip function in sequence 1 through N while the other BP in the channel executes its trip functions in the reverse sequence N through 1. This approach ~~provides functional diversity within the PPS~~. The trip outputs from each BP are provided to all LCL racks in four (4) redundant PPS channels. Within ESF-CCS, its functions such as the SIAS and AFAS are distributed

increases the degree of software diversity

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**DCD Tier 2, Section 7.2**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-3

Provide diagrams and figures that graphically display and demonstrate the relationship between (1) regulating Control Element Assembly (CEA), (2) shutdown CEAs, (3) part-strength CEAs, (4) full-strength CEAs, (5) 4 finger CEAs, (6) 12 finger CEAs, (7) CEA groups (as listed in Technical Report APR1400-FC-NR-14003-P, Rev. 0, “Functional Design Requirements for a Core Protection Calculator System for APR1400”), (8) CEA control groups, and (9) CEA subgroups. In addition, the diagrams and figures should demonstrate how CEAs are operated and positioned as a unit.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 25, “Protection System Requirements For Reactivity Control Malfunctions,” states that the protection system shall be designed to assure that specified acceptable fuel design limits are not exceeded for any single malfunction of the reactivity control systems, such as accidental withdrawal. SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the design basis information provided for each design basis item should be complete and sufficient to enable the detailed design of the I&C system to be carried out. The NRC staff was not able to identify diagrams or figures that would graphically demonstrate CEA functional design and operation as it relates to Core Protection Calculator System (CPCS) operation and safety system failure mode and effects analysis. Provide diagrams and figures to demonstrate CEA functional design in accordance with CPCS safety system operation and failure mode analysis and update the application accordingly.

Response

a) Relationship between groups, subgroups, and CEAs

The Control Element Assembly (CEA) pattern is based on 93 CEA locations as shown in Figure 4.3-35 of DCD Tier 2. The CEA pattern utilizes twelve-finger and four-finger CEAs. The CEA pattern consists of 48 twelve-finger Full-Strength CEAs, 33 four-finger Full Strength

CEAs, and 12 four-finger Part Strength CEAs. The CEAs are divided into four quadrant symmetric sets that are symmetrical about the center of the reactor core. A subgroup is composed of four CEAs, one from each quadrant set. In addition, the center CEA is assigned to regulating group 5, creating one subgroup of 5 CEAs. Table 4-3 of Technical Report APR1400-F-C-NR-14003-P, Rev.0 shows CEA subgroup assignments. Subgroups are combined to form control groups. There are three control group types: regulating, shutdown and part-strength. The number of control groups is 8, consisting of 5 (1, 2, 3, 4 and 5) regulating groups, 2 (A and B) shutdown groups and 1 (P) part-strength group. Figure 4.3-36 of DCD Tier 2 and Table 4-4 of Technical Report APR1400-F-C-NR-14003-P, Rev.0 show CEA group assignments. CEAs can be driven as groups, not as subgroups, in the raised or lowered direction.

There are 5 groups of CEAs designated as regulating CEAs. The main function of regulating CEAs is to control the neutron flux level in the reactor core. The regulating CEAs are normally used to follow load changes and routine power adjustments. There are 2 groups of CEAs designated as shutdown CEAs. Their main function is to provide a safe shutdown margin at all times during normal operation. The shutdown CEAs normally are fully withdrawn during power operation. There is 1 group of CEAs designated as part-strength CEAs. The main function of part-strength CEAs is to assist in control of the axial power distribution within the reactor core during power maneuvering operations. The part-strength CEAs are manually positioned in the core to make adjustments to the core power or axial power distribution. The reactor trip signal from the PPS interrupts power to the control element drive mechanism (CEDM) coils, allowing all CEAs to drop into the core by gravity.

b) CEA Operation

DCD Subsection 7.7.1.1 describes how CEAs are operated. The digital rod control system (DRCS) uses automatic CEA motion demand signals from the reactor regulating system (RRS) or manual motion signals from the DRCS soft control display on the information flat panel display (IFPD) to convert these signals to direct current pulses that are transmitted to the control element drive mechanism (CEDM) coils to cause CEA motion.

There are five modes of control: sequential group movement in manual and automatic control, manual group movement, manual individual CEA movement, and standby. Sequential group movement functions such that, when the moving group reaches a programmed low (or high) position, the next group begins inserting (or withdrawing), thus providing for overlapping motion of the regulating groups. Refer to Figures 1 and 2 for sequential group movement in manual and automatic control.

The shutdown CEAs are moved in the manual control mode only, with either individual or group movement. The DRCS soft control permits withdrawal of no more than one shutdown group at any time. The part-strength CEAs (PSCEAs) are normally moved manually, with either individual or group movement.

TS

Figure 1 Sequential Group Withdrawal Movement of Regulating Groups

Figure 2 Sequential Group Insertion Movement of Regulating Groups

c) CEA control limit and interlock

The DRCS includes normal CEA control limits and CEA interlocks for all full-strength CEAs and part-strength CEAs (PSCEAs). The CEA control limits include both the upper group stop (UGS) and the lower group stop (LGS) to prohibits the withdrawal or insertion in automatic and manual sequential, and manual group control modes. Control limits are provided to automatically terminate CEA motion upon reaching the CEA limits of travel. Whenever the DRCS receives an upper electrical limit (UEL) or lower electrical limit (LEL) interlock signals from the reed switch position transmitters (RSPTs), it prohibits the withdrawal or the insertion of the appropriate CEA in all DRCS control mode. These UEL and LEL interlock signals are provided to automatically terminate CEA motion upon reaching the CEA upper and lower limits of travel.

The DRCS receives automatic withdrawal prohibit (AWP) signals from RRS and steam bypass control system (SBCS), which prohibits the CEA withdrawal in automatic sequential DRCS control mode. The DRCS also receives CEA withdrawal prohibit (CWP) signal from PPS which prohibits the CEA withdrawal in all DRCS control modes.

The DRCS includes pulse counting to infer each CEA position by electronically monitoring the mechanical actions within each CEDM to determine when a CEDM has raised or lowered the CEA. The pulse counting CEA position signal associated with each CEA is reset to zero whenever the rod drop contact (located within the RSPT housing) is closed. Refer to Figure 3.

TS

Figure 3 CEA Limit and Interlock for CEA Operation

d) CEA related Penalty Factors

There are three kinds of CEA related penalty factor in CPCS. Each CPC knows the subgroup positions from its target CEAs. So, CPC determines subgroup deviation penalty factor and out of sequence penalty factor. And, each CEAC knows the position of all CEAs in the core. So, each CEAC determines CEAC deviation penalty factors due to single CEA misaligned from their subgroup.

Subgroup Deviation Penalty Factor

Each CEA subgroup position is compared to its respective group position to determine whether the subgroup deviates excessively from the group position. If a subgroup position and the corresponding group position are not within the deadbands at the top or bottom of the core, and if a subgroup deviation is greater than the subgroup deviation threshold, subgroup deviation penalty factor is applied.

Out of sequence penalty factor

If the regulating groups are not within the upper and lower deadband, and if the higher regulating group is more inserted than the lower regulating group, out of sequence penalty factor is applied.

CEAC Deviation penalty factor

If any subgroup of CEAs is not aligned within a limited threshold, CEAC will determine the CEAC deviation penalty factor for deviation type (withdrawal type, insertion type, multiple type). These penalty factors are sent to the CPC, and used for DNBR and LPD calculations.

e) Diagram for CPCS FMEA

All failure mode and effect analysis are provided in DCD Tier 2 table 7.2-7 FMEA table. The diagram to show the CPCS system operation according to failure mode is provided in Figure 4. The numbers in figure 4 are corresponded with the numbers in DCD Tier 2 table 7.2-7 FMEA table with prefix ‘2-‘.

TS

Figure 4 CPCS Block Diagram for FMEA

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 Technical/Topical/Environmental Reports.

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.:	**50-7911**
SRP Section:	**BTP 7-17 Guidance on Self-Test and Surveillance Test Provisions**
Application Section:	**Technical Report APR1400-Z-J-NR-14001-P, Rev.0, Section 4.3.2.3**
Date of RAI Issued:	**06/23/2015**

Question No. 07.02-4

a) How the validity of each CPCS program’s execution interval and dynamic adjustments to the parameters is determined and

b) The actions that occur if the CPCS determines that the execution interval or programs’ dynamic adjustments to the parameters are not valid.

10 CFR 50.55a(h)(3) requires compliance with IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.10, "Repair," requires safety systems to be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment. SRP Branch Technical Position 7-17, "Guidance on Self-Test and Surveillance Test Provisions" provides guidance regarding the use of fault detection and self-diagnostics. Section 4.3.2.3, “Program Structure,” of the Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states the CPCS will group detailed calculations of departure from nucleate boiling ratio (DNBR) and peak linear heat rate into different programs and will determine if the execution interval over which the dynamic adjustments to the parameters, calculated in each program, are valid. The NRC staff was not able to identify design descriptions that would explain how the execution interval and dynamic adjustments to parameters are determined to be valid and what protective actions would occur if the execution interval or dynamic changes of the programs were found to be invalid. Explain how the validity of the execution interval and dynamic changes of CPCS programs is determined and the actions performed if the execution interval of the programs or dynamic changes were found to be invalid. Update the application accordingly.

Response

The core protection calculator system (CPCS) calculates departure from nucleate boiling ratio (DNBR) and high local power density (LPD) values to generate low DNBR and high LPD trip signals. The CPC processor performs algorithms of DNBR and LPD based on the core average power, reactor coolant pressure, reactor inlet/outlet temperatures, reactor coolant flow, and the core power distribution. According to DCD Tier 2, Table 7.2-5, "Reactor Protective Instrumentation Response Time", the DNBR and LPD trips should be generated within 450 msec.

TS

Figure 1. Task interface for dynamic adjustments

TS

DNBR and LPD trips of integration and system test (IST) in testing phase do not successfully pass the acceptance criteria in DCD Tier 2, Table 7.2-5.

Data communication among tasks with different execution cycle times is described in Section 4.3.2.3 of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Technical Report APR1400-Z-J-NR-14001-NP, Rev. 0, Section 4.3.2.3 will be revised as indicated on the attached markup.

- The CPCS software is protected against unauthorized alterations (this includes setpoints and code) by control of access to software media and CRC authentication.

TS

Figure 4-8a Dynamic adjustments to the parameters

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**07.02**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-5

Explain why the Local Coincidence Logic (LCL) processor schematic boxes are different in Figure 4-5 of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, and Figure 7.2-10 of APR1400 FSAR, Tier 2, Rev. 0.

10 CFR 52.47(a)(2) requires, in part, the FSAR design descriptions be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the information provided for the design basis items should be technically accurate and should have one and only one interpretation. Figure 4-5 of Technical Report APR1400-Z-J-NR-14001-P displays “OR” gates for all LCL processors while Figure 7.2-10 in the FSAR displays several empty LCL processor schematic boxes (i.e., LCL processor’s A4 and A3). Discuss the differences between the two figures and update the application as necessary.

Response

Figure 4-5 of Safety I&C System Technical Report will be revised to be identical to Figure 7.2-10 of DCD Tier 2.

Each LCL processor is capable of receiving only two bistable processor logic outputs via SDL, and each LCL rack receives eight bistable processor logic outputs in total, which come from four safety channels (each safety channel generates two bistable processor outputs from two redundant bistable processors).

As indicated in Figure 7.2-10 of DCD Tier 2, LCL A4 processor in LCL rack 1 and LCL A3 processor in LCL rack 2 are included in each LCL rack to receive the bistable processor outputs only, with no coincidence logic implemented.

Currently, Figure 4-5 of Safety I&C System Technical Report is missing 'A4', 'A2', 'A3', and 'A1' in the LCL rack 1 portion and 'A2', 'A4', 'A1', and 'A3' in the LCL rack 2 portion. These will be added as indicated on the attached mark-up.

Accordingly, the logic drawn with 'OR' gates in the LCL processor schematic boxes (i.e., the leftmost LCL processor in LCL rack 1 and the rightmost LCL processor in LCL rack 2) in Figure 4-5 of Safety I&C System Technical Report will be removed as indicated on the attached mark-up.

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

Figure 4-5 in Safety I&C System Technical Report will be revised as indicated on the attached markup.

TS

Figure 4-5 PPS Division A Trip Path Diagram

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

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

Docket No. 52-046

RAI No.:	**50-7911**
SRP Section: Section	**SRP 7.2 Reactor Trip System**
Application Section:	**Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, Section 4.1.1.3**
Date of RAI Issued:	**06/23/2015**

Question No. 07.02-6

Explain why the CPCS would allow a safety limit to be exceeded before transmitting a trip signal.

10 CFR 50.36(c)(1)(ii)(A) requires, in part, where a limiting safety system setting is specified for a variable on which a safety limit has been placed, the setting must be so chosen that automatic protective action will correct the abnormal situation before a safety limit is exceeded. Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, Section 4.1.1.3, “Core Protection Calculator System,” states:

The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed a safety limit, a trip signal is transmitted to the PPS using hardwired cables.

Initiating a protective action after a safety limit is exceeded does not comply with the requirements of 10 CFR 50.36. Modify the application to describe how the CPCS and other APR1400 safety-related instrumentation and control (I&C) systems will initiate an automatic reactor trip prior to exceeding a safety limit.

Response

The CPCS is designed to generate the DNBR and LPD trip signals when the calculated DNBR and LPD values exceed the DNBR and LPD trip setpoints. The DNBR and LPD trips shall be generated based on the trip setpoints before the DNBR and LPD values exceed a safety limit.

Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, Section 4.1.1.3 will be revised as indicated on the attached markup.

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Technical Report APR1400-Z-J-NR-14001-NP, Rev.0, Section 4.1.1.3 will be revised as indicated on the attached markup.

communication via the serial data link (SDL, i.e., HSL) from safety systems to non-safety systems (i.e., QIAS-N) and buffering circuit using dual-ported memory are commonly used to prevent endangering the safety function. The other means from safety to non-safety data communication is via the plant computer datalink using the unidirectional protocol from the MTP.

- The DPS is diverse from the safety I&C system in aspects of trip mechanism, hardware and software.
- In addition to the DPS, the hardwired DMA switches and the DIS are provided on the MCR SC to cope with CCF of the safety I&C system.

4.1.1 Safety I&C Systems

4.1.1.1 Plant Protection System

The PPS consists of four redundant divisions that perform the necessary bistable, coincidence, initiation logic, maintenance and test function.

The PPS initiates reactor trip and system-level ESF actuation functions when a safety limit is exceeded by the plant conditions. To detect such conditions, the system utilizes measurements of the reactor core, reactor coolant system, main steam supply system, and containment building parameters.

Each PPS redundant division receives the process and discrete signals directly from field sensors or via the APC-S, ENFMS, and CPCS. The PPS provides the reactor trip signals to the RTSS using hardwired cables and ESFAS initiation signals to the ESF-CCS via fiber optic SDLs.

4.1.1.2 Engineered Safety Features - Component Control System

The ESF-CCS consists of four independent divisions that perform additional 2-out-of-4 voting logic, component control logic, and priority logic function.

The group controller (GC) of each ESF-CCS division receives four division ESFAS initiation signals derived from the ESFAS portion of the PPS and performs additional selective 2-out-of-4 coincidence logic to generate the ESF actuation signal. The GC also receives two division ESFAS initiation signals derived from the radiation monitoring system (RMS) and performs 1-out-of-2 logic to generate the ESF actuation signal. The ESF actuation signals are transmitted to the loop controller (LC) of the ESF-CCS. The LC executes the component control logic and outputs the component control signal to the CIM. The component control logic includes the priority logic for the operator's manual control signal and ESF actuation signal. The ESF-CCS soft control module (ESCM) on the operator console generates a component control signal of safety components by manual operator actions.

4.1.1.3 Core Protection Calculator System

Insert 'setpoints'

The CPCS has four redundant channels that compute the DNBR and LPD values using process values, reactor coolant pump (RCP) speed, CEA position and ex-core neutron flux.

The CPCS compares the DNBR and LPD values against setpoints to determine if fuel design limits are exceeded. When these values exceed ~~a safety limit~~, a trip signal is transmitted to the PPS using hardwired cables.

4.1.1.4 Qualified Indication and Alarm System - P

The QIAS-P, which has two independent divisions A and B, is implemented on the common PLC platform for the safety system. The QIAS-P processes the plant parameters that are input from the safety I&C

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**Technical Report APR1400-Z-J-NR-14001-P, Rev.0 Appendix C.**
Date of RAI Issued:	**06/23/2015**

Question No. 07.02-7

a) Define and explain the differences and similarities between the following terms used in Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, describing the CEAs:
I. CEA number 1
II. CEA 1 (referred to as the center CEA)
III. CEA01 (as listed in Table C.5.1-1)

b) Explain why the design descriptions state the center CEA is assigned to only CPCS Channel B (i.e., 70 CEA's to Channel B versus 69), yet, figures and tables of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, demonstrate that the center CEA is going to both CPCS Channels B and C (for a total of 70 CEAs to both channels).

10 CFR 50.55a(h)(3) requires compliance to IEEE Std 603-1991. IEEE-603-1991, Clause 5.6.1, requires redundant portions of a safety system provided for a safety function to 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. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 5.6, "Independence," states that the safety system design precludes the use of components that are common to redundant portions of the safety system or any other features that could compromise the independence of redundant portions of the safety system.

Section C.5.1.3.2, "Divisional Independence," in Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states that the twenty-third subgroup consists of 4 CEAs distributed to the four quadrants of the reactor core with CEA number 1 being located at the center of the core and that the center CEA is assigned to Channel B (thus, 70 CEA's to Channel B versus 69). However, Table C.5.1-1, "RSPT1 and RSPT2 Channel Assignment" and Figure 4-8, "CPCS Block Diagram," of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, show the center CEA is going to both CPCS Channels B and C (for a total of 70 CEAs to both channels - 3 quadrants times 23 CEAs equals 69, plus the center CEA would equal 70). Correctly define the acronym for the center CEA and consistently apply center CEA terminology. Also, clarify the assignment of the center CEA to the CPCS channels that would demonstrate compliance to the applicable safety system independence requirements of IEEE-603-1991. Update the application as necessary.

Response

There are no differences among CEA number 1, CEA 1 and CEA01. To keep consistency in the Technical Report APR1400-Z-J-NR-14001-P, CEA01 will be used for CEA 1 and CEA number 1. The CEA number 1 and CEA 1 in Technical Report APR1400-Z-J-NR-14001-P will be revised as CEA01.

The center CEA is assigned to channel B and C. Therefore, the sentence in Section C.5.1.3.2 will be revised as follows:

“The RSPT monitored by CPCS B and C for CEA01 (the center CEA) is assigned to channels B and C.”

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Technical Report APR1400-Z-J-NR-14001-NP, Rev. 0, C.5.1.3.2 and C.5.1.3.7 will be revised as indicated on the attached markup.

TS

TS

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**DCD Tier 2, Section 7.2**
Date of RAI Issued:	**06/23/2015**

Question No. 07.02-8

Provide design information that would:

a) Define the conditions resulting in unavailable CEA position data.

b) What are the failures that cause CEA position data to become unavailable?

c) Describe what system, component, and/or processor senses and makes the determination that CEA position data is unavailable?

d) Explain all system actions and the component(s) and/or device(s) that control those actions that are performed when switching from using the preferred CEA position data to the alternate source.

e) Include failure mode entries into APR1400 FSAR, Tier 2, Revision 0, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” describing safety system actions performed after CEA position data becomes unavailable.

10 CFR Part 50, Appendix A, General Design Criteria (GDC) 21, "Protection System Reliability and Testability," requires, in part, that redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function, and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 5.5, “System Integrity,’ states, in part, that the review of system integrity should confirm that the design provides for safety systems to fail in a safe state, or into a state that has been demonstrated to be Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the

design basis information provided for each design basis item should be complete and sufficient to enable the detailed design of the I&C system to be carried out.

Section 4.3.3.2, “CEA Calculator Rack,” of Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, states that, should the preferred source of CEA position data become unavailable, the alternate source will be used. However, the staff was not able to find information that describes: (a) The conditions resulting in unavailable CEA position data; (b) what failures would cause CEA position to become unavailable; (c) what portion of the I&C system determines CEA position is unavailable; (d) what actions would occur to transfer CEA position data to the alternate source; and (e) identification of CEA position unavailability in the Plant Protection System failure modes and effects analysis. Explain and describe the complete safety system actions performed to detect and mitigate against the unavailability of preferred CEA position data. Update the application accordingly.

Response

a), b), c) The conditions resulting in unavailable CEA position data and the failures that cause CEA position data to become unavailable are defined as follows;

- RSPT sensor failures : open circuit, short circuit, spike noise
- Failures detected by AI diagnostic (e.g., open loop detection, out of range, calibration error, configuration error)
- Failures detected by CEA position processor (CPP) (e.g., out of range, AI module error)
- Failures detected by CEA calculator (CEAC) (e.g., rate of change increase, rate of change decrease)
- Failures detected by an SDL diagnostic (e.g., CRC error, live signal exchange error, receive monitoring of SDL telegrams, SDL disturbed, SDL overload)

d) In the core protection calculation system (CPCS) channel, there are two selection logics as shown in Figure 1. One is the primary/back-up selection logic for the non-target CEAs in the CEAC processor. The other is primary/alternative selection logic for the target CEAs and PF in the CPC processor.

If the primary source of CEA position data becomes unavailable, the back-up source is used in the CEAC processor. To determine the quality of the primary source of CEA position, the CEAC monitors the following information.

- Heartbeat from the CPP
- CPP failure flag
- Safety data link error flag

If the primary source of target rod CEA position data and penalty factor become unavailable, the alternative source is used in the CPC processor. To determine the quality of primary source of the target rod and the penalty factor, the CPC processor monitors the following information.

- Heartbeat from the CEAC

- CEAC failure flag
- Safety data link error flag

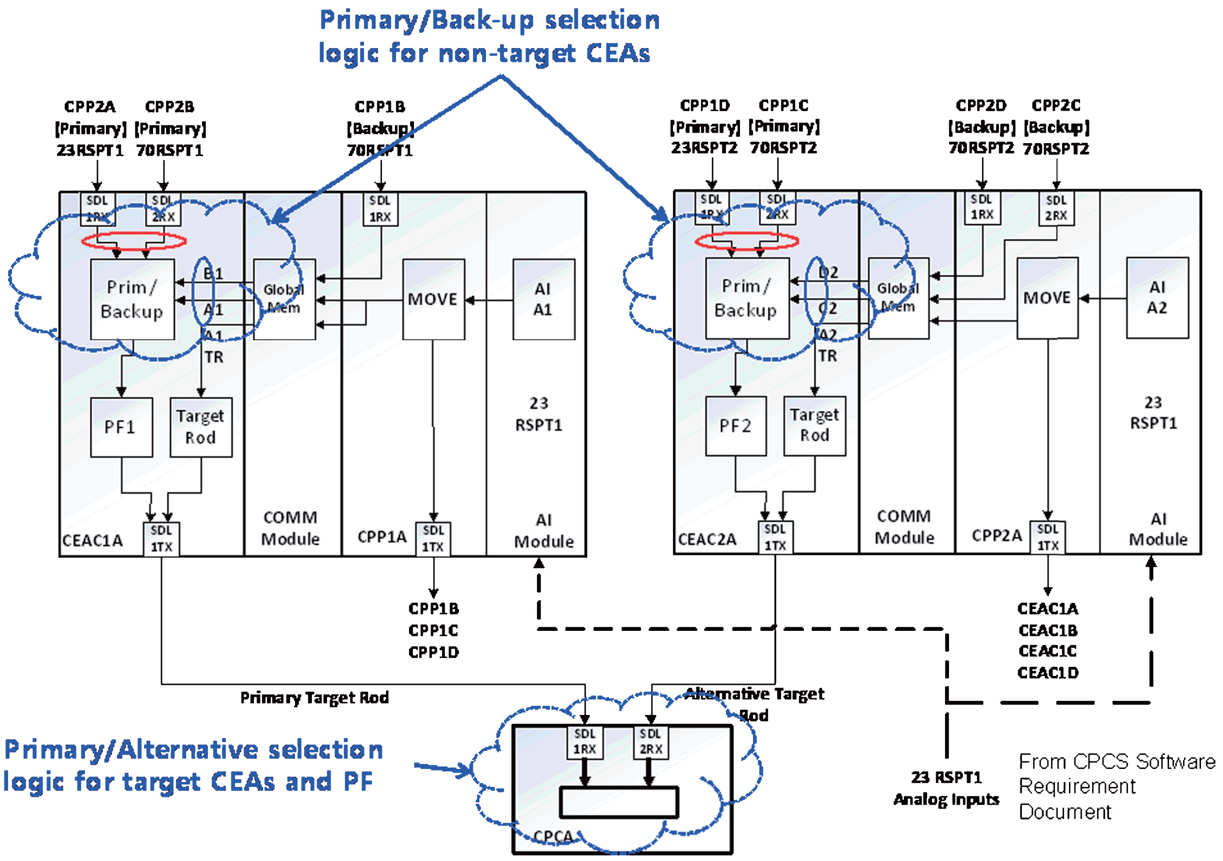

Figure 1 Redundancy in CPCS

e) APR1400 FSAR, Tier 2, Revision 0, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System” provides the safety system actions performed after CEA position data becomes unavailable in items 2-4 and 2-5.

New table entries describing the CPP1 failures in channels C and D, and the CPP2 failures in channels A and B will be added into APR1400 DCD, Tier 2, Revision 0, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System.”

Impact on DCD

APR1400 DCD, Tier 2, Revision 0, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System” will be revised as indicated on the attached markup.

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 Technical/Topical/Environmental Reports.

Table 7.2-7 (28 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-14	CEA position processor 1 in channels A or B. Processor and/ or communication section.	a) OFF; processor off	Loss of module power; software execution stops.	• CPP1 watchdog timer timeout, CPP trouble OM/MTP indication, channel Trouble annunciation. • Loss of alternate source of RSPT 1 CEA position transmission to CEAC 1 in all four channels. • Loss of preferred source of target CEA position in channel of origin. • Loss of receive ports for alternate CEA position to CEAC 1.	• CPP trouble OM/MTP indication, channel trouble annunciation in all four channels and channel trouble indication on OM/MTP in all 4 channels due to loss of 1 of 2 redundant sources of CEA position input • Run lamp out on affected CPP • Diagnostics identify loss of SDL input to CPC. • WDT in the affected CPP provide failure to CPC	• CPPs 1 and 2 are redundant in each channel. • CPP 2 in channels A and B is preferred source of CEAC 1 CEA position in all channels, and alternate source of target CEA position.	None. CEAC 1 in all channels normally receives CEA position from CPP2. Target CEA position input in affected channel is switched from the CEAC 1 to CPC SDL to the CEAC 2 to CPC SDL. Loss of CPP 1 receives ports in channels A and B disables the alternate source of SDL input to CEAC 1. This has no effect on CEAC 1 since the preferred SDL input is directly to the CEAC processor receive port.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; Erroneous CEA position transmitted	Unrecognized hardware or software malfunction	• Failure to provide proper alternate source of CEA position in CEAC 1 in all channels. • Possible failure of preferred source of target CEA position transmission in channel of origin	• Possible erroneous target CEA position indication • If problem is due to processor failure, this is detected by on line diagnostics and a CPP trouble/CPP WDT time out.	• CPP1 is alternate source for CEAC 1 position indication, and is normally not selected. • CPP1 is preferred source of target CEA position, and target CEA position may be improper in one CPC channel. • 3-channel redundancy.	None. If target CEA position is improper, one CPC channel is inoperable, and RPS logic is in 2-out-of-2 coincidence logic.	To restore the PPS logic to 2-out-of-3 coincidence logic, the bypassed channel is returned to operation and the failed channels are bypassed

Insert the new item 2–14a.

This new items will be added after item no. 2−14

Table 7.2-7

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-14a	CEA Position Processor 2 in Channels A or B. Processor and/ or communication section.	a) OFF; processor off	Loss of module power; software execution stops.	CPP2 Watchdog timer timeout, CPP Trouble OM/MTP indication, Channel Trouble annunciation Loss of primary source of RSPT 1 CEA position transmission to CEAC 1 in all four channels Loss of alternative source of Target CEA position in channel of origin Loss of receive ports for primary CEA position to CEAC 1	CPP Trouble OM/MTP indication, Channel Trouble annunciation in all four channels and Channel Trouble indication on OM/MTP in all 4 channels due to loss of 1 of 2 redundant sources of CEA position input Run lamp out on affected CPP Diagnostics identify loss of SDL input to CPC. WDT in the affected CPP	CPPs 1 and 2 are redundant in each channel. CPP 1 in channels A and B is alternative source of CEAC 1 CEA position in all channels. CPP 1 in channels A and B is primary source of Target CEA position.	None. CEAC 1 in all channels is switched from CEA positions from CPP2 to CPP1. CPC in all channels normally receives Target CEA position input from the CEAC 1 to CPC SDL Loss of CPP 2 ports in channels C and D disables the primary source of SDL input to CEAC 1.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; Erroneous CEA position transmitted	Un-recognized hardware or software malfunction	Failure to provide proper primary source of CEA position in CEAC 1 in all channels. Possible failure of alternative source of target CEA position transmission in channel of origin	Possible erroneous target CEA position indication	CPP2 is proper alternative source for Target CEA position indication, and is normally not selected. CPP2 is preferred source of CEA position, and CEAC1 receiving CEA positions from CPP2 may be improper in all channels. 2 CEAC redundancy	None. If CEA position in CEAC1 is improper, CEAC1 in all channels is inoperable, and CEAC2 in all channels are operable. RPS remains in 2-out-of-3 coincidence logic.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect Upon PPS	Remarks and Other Effects
2-14b	CEA Position Processor 1 in Channels C or D. Processor and/ or communication section.	a) OFF; processor off	Loss of module power; software execution stops.	CPP1 Watchdog timer timeout, CPP Trouble OM/MTP indication, Channel Trouble annunciation Loss of primary source of RSPT 1 CEA position transmission to CEAC 2 in all four channels Loss of primary source of Target CEA position in channel of origin Loss of receive ports for primary CEA position to CEAC 2	CPP Trouble OM/MTP indication, Channel Trouble annunciation in all four channels and Channel Trouble indication on OM/MTP in all 4 channels due to loss of 1 of 2 redundant sources of CEA position input Run lamp out on affected CPP Diagnostics identify loss of SDL input to CPC. WDT in the affected CPP	CPPs 1 and 2 are redundant in each channel. CPP 2 in channels C and D is alternative source of CEAC 2 CEA position in all channels, and alternate source of Target CEA position.	None. CEAC 2 in all channels is switched for CEA positions from CPP1 to CPP2. Target CEA position input in affected channel is switched from the CEAC 1 to CPC SDL to the CEAC 2 to CPC SDL. Loss of CPP 1 ports in channels C and D disables the alternative source of SDL input to CEAC 1.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.
		b) ON; Erroneous CEA position transmitted	Un-recognized hardware or software malfunction	Failure to provide proper primary source of CEA position in CEAC 2 in all channels. Possible failure of primary source of target CEA position transmission in channel of origin	Possible erroneous target CEA position indication	CPP2 is alternative source for Target CEA position indication, and is normally not selected. CPP1 is primary source of CEA position, and CEAC2 receiving CEA positions from CPP1 may be improper in all channels. 2 CEAC redundancy	None. If CEA position in CEAC2 is improper, CEAC2 in all channels is inoperable, and CEAC1 in all channels are operable. RPS remains in 2-out-of-3 coincidence logic.	Operation with a single failed CEAC in one or more channels addressed in LCO 3.3.3.

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**07.02**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-10

Describe what happens to the Reactor Protection System (RPS) channel status when the RPS detects a high steam generator sensor failure.

10 CFR Part 50, Appendix A, GDC 23, "Protection system failure modes," requires protection systems to be designed to fail into a safe state or into state demonstrated to be acceptable on some other defined basis. SRP Appendix 7.1-C, Section 5.5, “System Integrity,” states that computer-based safety systems should, upon detection of inoperable input instruments, automatically place the protective functions associated with the failed instrument(s) into a safe state (e.g., automatically place the affected channel(s) in trip), unless the operator has already placed the affected channel in a bypass mode.

APR1400 FSAR, Tier 2, Rev. 0, Table 7.2-7, single failure entry Item# 1-6, b), states that once the reactor protection system (RPS) detects and activates an alarm for a detected “sensor failure,” the RPS trip logic would be changed to a 2-out-of-2 (as listed in the “Effect on PPS” column). The alarm would result from the RPS feature of “comparison of three channels” for the failed steam generator high pressure sensor signal. However, since the logic of the RPS is not designed to provide a trip for a high steam generator pressure, it is not clear why the RPS trip logic would change for a failed high steam generator pressure sensor. Describe other actions initiated by the RPS resulting from an RPS detected high steam generator pressure sensor failure and the basis for the actions described in Table 7.2-7.

Response

Upon a high steam generator pressure signal resulting from the sensor failure (DCD Tier 2, Table 7.2-7, single failure entry Item# 1-6, b)), the channel trip in that channel will not occur, even when the affected steam generator experiences a low-pressure state which is sufficient to generate the trip condition. This results in 2-out-of-2 coincidence logic, because the channel with sensor failure (high) cannot generate steam generator low pressure trip signal due to the sensor failure.

Item #1-6 b) discusses the sensor failure (high), which is different from an over-range error (analyzed as Item #3 of Table 7.2-7 in DCD Tier 2, which discusses the "out of range high or low" failure that is detected at the analog input stage of the PPS). The "comparison of three channels" alarm and periodic test will be the only way to be aware of the sensor failure (high), and prompts an operator to place the failed channel in trip channel bypass.

For this particular case, the sensor failure signal would not be detected as a failed signal at the input stage of the PPS.

In summary, there is no other action initiated by the RPS resulting from an RPS detected high steam generator pressure sensor failure.

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 Reports.

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**7.2**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-11

Define and explain the meaning of the term "quality margin" as it relates to APR1400 FSAR, Tier 2, Rev. 0, Table 7.2-7, "Failure Mode and Effects Analysis for the Plant Protection System," Item# 2-1, b).

10 CFR 52.47(a)(2) requires the FSAR design descriptions be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. SRP Appendix 7.1-C, "Guidance for Evaluation of Conformance to IEEE Std. 603," Section 4, "Safety System Designation," states that the information provided for the design basis items, taken alone and in combination, should have one and only one interpretation.

Section 4.5.2, "DNBR/Quality Trip," in Technical Report APR1400-F-C-NR-14003-P, Rev. 0, "Functional Design Requirement for a CPCS for APR1400," states that if "Quality Margin Trip" is violated, a DNBR Trip or Pre-trip signal is issued. However, the NRC staff was not able to identify a definition or design description of the term "quality margin" to understand its usage in the technical report and in Table 7.2-7, ″Failure Mode and Effects Analysis for the Plant Protection System," single failure entry Item # 2-1, b), of APR1400 FSAR, Tier 2, Chapter 7, Rev. 0. Define and describe the term "quality margin" and update the FSAR and technical reports accordingly.

Response

Section 4.2.7, "Update of DNBR and Quality Margin," in Technical Report APR1400-F-C-NR-14003-P, Rev. 0, "Functional Design Requirement for a CPCS for APR1400," states that the quality at the node of minimum DNBR is calculated based on the core inlet enthalpy, the saturated liquid enthalpy, and the latent heat of vaporization. Quality margin is defined in equation 4.2-49 of the technical report as the difference between the quality limit and the calculated value of quality discussed above.

The following definition for quality margin will be added in Table 7.2-7, Item # 2-1, b) of the DCD.

“Quality: the mass fraction of vapor in the mixture.”
“Quality margin: the difference between the quality limit and the calculated quality.”

Impact on DCD

DCD Table 7.2-7 will be revised as indicated on the attached markup.

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 Report

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

Non-Proprietary

Table 7.2-7 (13 of 68)

No.	Name	Failure Mode	Cause	Symptoms and Local Effects Including Dependent Failures	Method of Detection	Inherent Compensating Provision	Effect on PPS	Remarks and Other Effects
2-1	Analog input hot leg temperature	a) High level signal (out of range)	Sensor failure	For failures beyond input module range limits: DNBR/LPD channel auxiliary trip on sensor out of range failure; CPC failed sensor indication and channel trouble OM and MTP indication, channel trouble annunciation. *	• For out of range failures: DNBR/LPD channel auxiliary trip, CPC sensor failure indication / annunciation, CPC trouble indication / annunciation. • Sensor input cross channel comparison.	Three-channel redundancy	DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	To restore the system logic to 2-out-of-3 coincidence, the bypassed channel is returned to operation and the failed channel is bypassed.
		b) High level signal (in range)	Sensor failure	• For in range failures, possible DNBR/LPD channel trip on quality margin. • Likely Auxiliary trip on VOPT for rapid changes. • CPC software generated sensor failure alarm if process exceeds high range limits.	For in range failures: Increase in delta T power, Sensor input cross channel comparison possible sensor failure alarm.	Three-channel redundancy	When trip occurs, DNBR/LPD logic of RPS are converted to 1-out-of-2 coincidence logic.	
		c) Low level signal (out of range)	Sensor failure	For failures beyond input module range limits: DNBR/LPD channel auxiliary trip on sensor out of range failure; CPC sensor failure indication and channel trouble OM and MTP indication, channel trouble annunciation.	[illegible] trouble indication/ annunciation • Sensor input cross channel comparison	Three-channel [illegible]	DNBR/LPD logic of [illegible]	

*Quality: the mass fraction of vapor in the mixture.
Quality margin: the difference between the quality limit and the calculated quality.

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.:	**50-7911**
SRP Section:	**07.02 – Reactor Trip System**
Application Section:	**DCD Tier 2, Section 7.2**
Date of RAI Issue:	**06/23/2015**

Question No. 07.02-12

For the single failure entry items 2-4a), 2-4b), and 2-4c), of APR1400 FSAR, Tier 2, Chapter 7, Rev. 0, Table 7.2-7, “Failure Mode and Effects Analysis for the Plant Protection System,” explain:

a) The difference between a sensor and a finger;

b) Why the plant would shut down due to an in-range 12 finger CEA single failure;

c) Why the plant would not shut down due to an in-range 4 finger CEA single failure; and

d) Why an excessive number of failures, as postulated in single failure entries 2-4b) and 2-4c), do not result in the same reactor protection system (RPS) protective actions.

10 CFR Part 50, Appendix A, GDC 21, requires, in part, redundancy and independence to be designed into the reactor protection system to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy. SRP Appendix 7.1-C, “Guidance for Evaluation of Conformance to IEEE Std. 603,” Section 4, “Safety System Designation,” states that the information provided for the design basis items should be technically accurate.

Response

a) The APR1400 has control element assemblies (CEAs) which have 4 or 12 fingers. The term "finger" is used to describe a control rod within an assembly. The term "sensor" is used to describe the reed switch position transmitters, which sense movement of a CEA.

b) The COLSS is a reactor core monitoring system and the CPCS is a core protection system. The COLSS and CPCS complement each other. COLSS limiting conditions for operation (LCOs) are limited, or the CPCS can be adequately manipulated to prevent violation of the DNBR SAFDL in case of event.

As analyzed in DCD 15.4.3, during 4-finger CEA drop event, thermal margin decrement triggered by integrated radial peak (Fr) distortion change and xenon redistribution is preserved as initial thermal margin through the technical specifications LCOs, and hence it negates the application of CEA drop penalty factor and reactor shut down.

However, in case of a 12-finger CEA drop, the thermal margin decrement caused by Fr distortion change and xenon redistribution is significant. So LCOs should be excessively limited if this thermal margin decrement was preserved in LCOs. Therefore instead of a preservation of the initial thermal margin in LCOs, CPCS may trip the reactor by applying a penalty factor to DNBR and the DNBR SAFDL is not exceeded.

Even though a 12-finger CEA drop is caused by any false signal, CPCS recognizes it as a real drop. Therefore the same penalty factor for a 12-finger CEA drop is applied to DNBR calculation.

c) During 4-finger CEA drop event, thermal margin decrement triggered by Fr distortion change and xenon redistribution is preserved as initial thermal margin through the technical specifications LCOs, and neither the application of CEA drop penalty factor nor reactor shut down is required.

d) An excessive number of failures will set the pertinent CEAC ‘inoperable’. However, if the other CEAC is operable, the plant remains operable without a need to apply of a penalty. If both CEACs are inoperable, a big penalty factor will be applied to trip the reactor.

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 Technical/Topical/Environmental Reports.