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.:	**68-7892**
SRP Section:	**07.07 - Control Systems Not Required for Safety**
Application Section:	**7.7**
Date of RAI Issue:	**07/10/2015**

Question No. 07.07-1

Clarify whether the intent of APR1400 Final Safety Analysis Report (FSAR), Tier 1, Table 2.5.5-2, Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) Item No. 2, is to verify diversity between safety and non-safety-related instrumentation and control (I&C) equipment and software.

10 CFR 52.47(b)(1) states in part that if the inspections, tests and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. In ITAAC Item No. 2, the design commitment states, "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)." Independence is a safety attribute established by such requirements as General Design Criteria 24 and IEEE Std. 603-1991, Clause 5.6, as incorporated by reference in 10 CFR 50.55a(a)(2). The manner in which this ITAAC item is written would imply the PCS and P-CCS are diverse from the PPS and ESF-CCS because it states the equipment and software are independent between systems rather than simply stating the systems are independent.

Verify the intent of this ITAAC is actually to establish and verify diversity between the subject systems or to verify independence between safety and non-safety I&C systems.

Response

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.

Impact on DCD

APR1400 DCD, Tier 1, Subsection 2.5.5 and Table 2.5.5-2 will be revised as shown in the Attachment associated with this response.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

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

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: • 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.
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: • Controls at the RSR are disabled when controls are active in the MCR for the as-built PCS and P-CCS. • 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

different

.

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

RESPONSE TO REQUEST FOR ADDITIONAL INFORMATION

APR1400 Design Certification

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

Docket No. 52-046

RAI No.: **68-7892**

SRP Section: **7.7 – Control Systems**

Application Section: **07.07**

Date of RAI Issue: **07/10/2015**

Question No. 07.07-5

Clarify the network architectural arrangements and interfaces for the individual non-safety I&C systems, with specific attention to those cited in the failure boundary portion of Figure 4.1-1 in Technical Report APR1400-Z-J-NR-14012-P, Rev.0, "Control System CCF Analysis Technical Report."

10 CFR 52.47(a)(2) requires, in part, that the description of structures, systems and components shall be sufficient to permit understanding of the system designs. Section 4.4.2 of the Control System CCF Analysis Technical Report states, in part, that, "The non-safety system incorporates network communication configurations that have dual or redundant communications paths." and Section 4.4.6, "Design Features to Cope with Broadcast Storms on the IFPD/ESCM Ethernet Networks," discusses the potential for a broadcast storm on the Ethernet networks. Figure 4.1-1, "Credible Failure Boundary of Control System CCF," of Technical Report APR1400-Z-J-NR-14012-P, Rev. 0, is a general network diagram illustrating the baseline communications paths but does not convey the level of detail mentioned in the above quotes, thereby making it difficult to understand the non-safety I&C architecture.

1. Are there figures illustrating the internal network architectural layout of specific non-safety I&C systems such as the power control system (PCS), as it is described in APR1400 FSAR, Tier 2, Section 7.7? This is critical as the PCS system contains multiple subsystems such as the reactor regulating system (RRS) and the digital rod control system (DRCS).

2. Describe the interface, along with communication type and logic, facilitating the turbine trip function from a reactor trip signal. APR1400 FSAR, Tier 2, Section 10.2.2.3.3, describes the Turbine Generator Control system as a 2-out-of-3 logic system but the Plant Protection System is a 2-out-of-4 logic system.

3. In Figure 4.1-2, "Control System Overview," of Technical Report APR1400-Z-J-NR-14012-P, the acronym, “RRS” (Reactor Regulating System?) is not defined in the drawing key.

Response

1. Figure 4.1-1 in Technical Report APR1400-Z-J-NR-14012-P, Rev 0, “Control System CCF Analysis Technical Report” shows the overview architecture of APR1400 I&C systems. The non-safety I&C system in Figure 4.1-1 represents sets of equipment (such as the IPS server cabinet, the P-CCS group controller cabinet, and the P-CCS loop controller cabinet), depending on their dedicated functions.

   In the case of the information processing system (IPS) and the process-component control system (P-CCS), including the NSSS process control system (NPCS), there are no internal dedicated networks for each non-safety I&C system. The data communication network-information (DCN-I) network provides non-safety data communication for these non-safety I&C systems. Refer to APR1400 DCD Subsection 7.9.1.3 and Figure 7.9-1 for additional information about the DCN-I network.

   The non-safety standalone systems such as the fixed in-core detector amplification system (FIDAS), the NSSS integrity monitoring system (NIMS), the BOP monitoring system and the auto synchronizers for the turbine/generator are generally connected to the datalink server. The datalink server provides datalink connections for non-safety standalone systems to interface with the DCN-I network. The turbine/generator control system (T/GCS) is connected to the P-CCS controller to perform the T/G control function.

   The non-safety DRCS controller receives signals from the PPS Channel D and RSPTs via the DRCS Remote I/O cabinets, which use the remote digital input devices of the non-safety common platform. The hardwired signals from the safety system are input to the DRCS Remote I/O cabinets and transmitted to the DRCS controller via a fiber optic isolation data link. DRCS Remote I/O cabinets are designed as associated circuits according to IEEE Std. 384. DCD Tier 2, Subsection 7.7.1.1 will be revised as shown in Attachment 1 to explain the isolation of interface signals from the RSPTs.

   The internal network architecture of the PCS and other communication architecture mentioned in the above description are shown in Figure 7.7-5-1 for information. The PCS MTP can use the common platform for non-safety I&C or dedicated equipment. If dedicated equipment is used, a dedicated gateway will be applied to interface with the DCN-I network. The Control groups of the PCS and the P-CCS are described in Table 4.5-2 in Technical Report APR1400-Z-J-NR-14012-P. Each control group function of the P-CCS in Table 4.5-2 is assigned to at least one group controller or one loop controller.

   The IFPD/ESCM Ethernet network architecture is shown in Figure C.5-1 in Technical Report APR1400-Z-J-NR-14001-P, Rev 0, “Safety I&C System Technical Report”

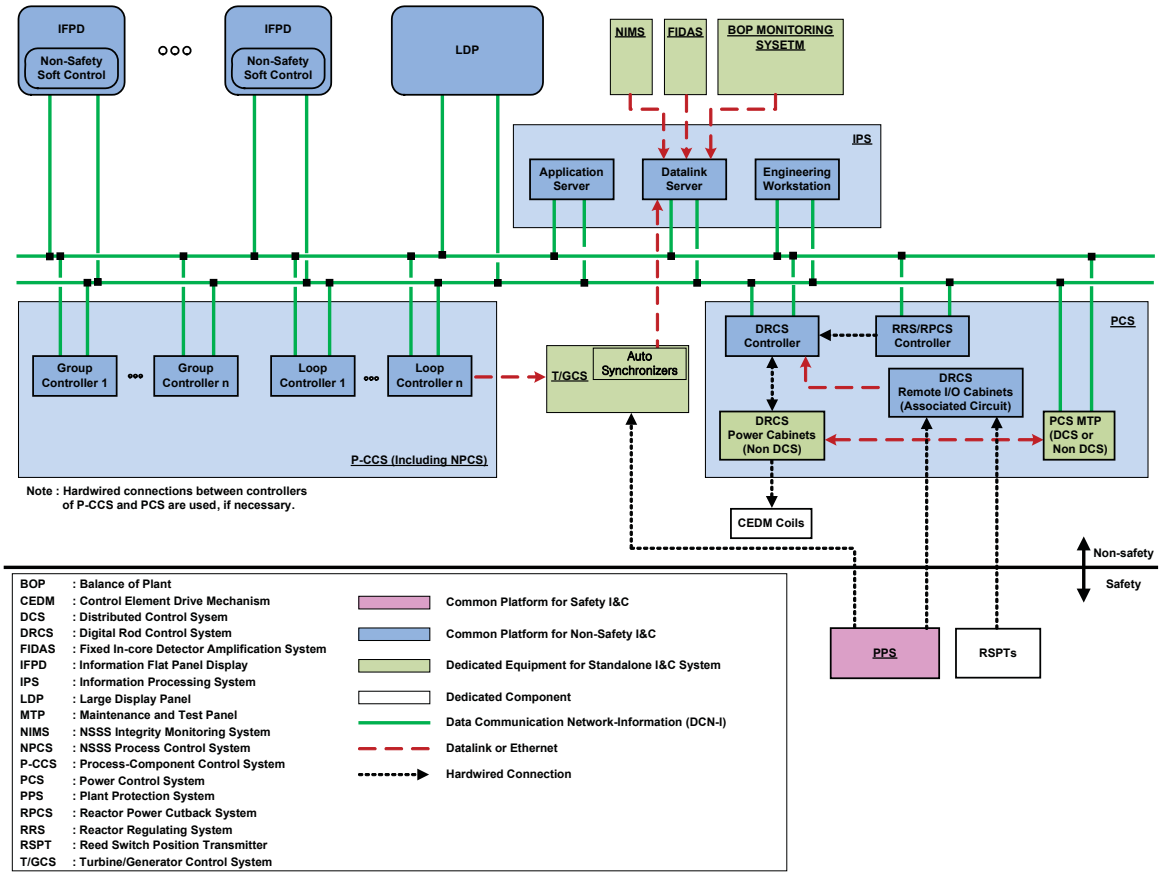

Figure 7.7-5-1 Internal network architectural layout of PCS and other non-safety I&C systems

2. The "2-out-of-3 majority voting" logic stated in APR1400 FSAR, Tier 2, Section 10.2.2.3.3 is dedicated logic within the turbine protection system to prevent spurious turbine trips and enhance protection system operation. This 2-out-of 3 voting logic is independent and different from the 2-out-of-4 voting logic implemented in the plant protection system (PPS).

   Turbine generator control system (T/GCS) interfaces with the divisionalized PPS in order to receive the turbine trip initiation signal upon a reactor trip. This interface is implemented via hardwired connection unidirectionally from the PPS to the T/GCS. Refer to right side of APR1400 FSAR, Tier 2, Figure 7.2-14 for the PPS Interface Logic Diagram. The independence between safety systems and other systems is described in Section A.5.6 of the Safety I&C System Technical Report.

3. Figure 4.1-2 in Technical Report APR1400-Z-J-NR-14012-P will be revised to define the acronym “RRS”.

Impact on DCD

DCD Tier2, Subsection 7.7.1.1 will be revised as indicated in Attachment 1.

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-14012-NP, Rev.0 will be revised as indicated in Attachment 2.

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 PSCEAs are normally moved manually, with either individual or group movement.

During plant startup and shutdown, and all cases where power is below a preset value, manual control is used. Automatic control of the regulating CEAs by the RRS can be selected by the operator only when power exceeds the preset value. Manual control can be used to override automatic control at any time.

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. This permits the pulse counting system to automatically reset the position to zero, whenever a reactor trip occurs or whenever a CEA is dropped into the core. This CEA position information is used in MCR displays. The displays provide CEA group information and individual CEA position information.

The DRCS also provides the IPS with each CEA position from the pulse counting system for use in the CEA monitoring displays and alarms and the core operating limit supervisory system (COLSS) as described in Subsection 7.7.1.4.

The DRCS receives a CEA withdrawal prohibit (CWP) signal from the PPS. This signal stops withdrawal motion of all CEAs. It can be overridden by the operator with the DRCS soft control display on the IFPD in the MCR.

The CWP interlock is interfaced to the protection systems via optical isolation to provide ~~reasonable assurance of~~ separation and independence.

b. Pressurizer pressure and level control systems

1) Pressurizer pressure control system

The UEL, LEL and rod drop contact signals from RSPTs are interfaced to the DRCS via optical isolation to provide separation and independence.

TS

Figure 4.1-2 Control System Overview