REVISED 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.: **45-7883**

SRP Section: **07.09 - Data Communication Systems**

Application Section:

Date of RAI Issue: **06/23/2015**

Question No. 07.09-7

Clarify what is meant by "any errors", and describe potential data communication faults and mitigating measures.

10 CFR 50.55a(h) requires compliance to IEEE Std 603-1991. IEEE Std 603-1991, Clause 5.6.1, states, in part, “Redundant portions of a safety system provided for a safety function shall 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,” and Clause 5.6.3, states, in part, “The safety system design shall be such that credible failures in and consequential actions by other systems, as documented in 4.8 of the design basis, shall not prevent the safety systems from meeting the requirements of this standard.” RG 1.75 provides guidance on the physical separation requirements of IEEE Std. 603-1991, Clause 5.6. BTP 7-11 provides guidance on application and qualification of isolation devices to meet the electrical isolation requirements of IEEE Std. 603-1991 Clause 5.6. DI&C-ISG-04 provides guidance for meeting the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.

DI&C ISG-04, Section 1, Position 12, states, in part, "Communication faults should not adversely affect the performance of required safety functions in any way...", and lists examples of credible communication faults. APR1400 FSAR, Tier 2, Section 7.1, Page 7.1-3, states, in part, “Data communications within or between I&C systems are designed to provide reasonable assurance that any error in data communication will not cause inadvertent actuations or prevent the safety functions from being performed.” Clarify whether the applicant really meant "any" errors as this goal is typically difficult to achieve except on simple communication schemes. Also, per DI&C ISG-04, Section 1, Position 12, describe the potential data communication faults between IFPD and ESCM and the mitigating measures for each fault.

Response - (Rev. 1)

The use of “any error” in APR1400 DCD, Tier 2, Section 7.1 means the malfunctions that lead to detectable and undetectable failures of data communications. APR1400 FSAR, Tier 2, Section 7.1, Page 7.1-3, sub-part, “Data Communication” will be updated as follows: “Data communications within or between I&C systems is provided with the communication independence to ensure that there will be no adverse impact on the safety systems. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, a qualified serial data link, and Ethernet network. Communication independence is provided among safety divisions and between safety and non-safety data communication systems. The safety and non-safety data communication systems are diverse.”

TS

TS

TS

TS

TS

Impact on DCD

APR1400 DCD Tier 2, Section 7.1, Page 7.1-3 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-14001-NP, Rev. 0, “Safety I&C System”, Subsection C.5.1.5 will be revised as indicated in Attachment 2.

Some I&C functions are not installed on a common PLC and DCS platform. These functions are implemented in independent systems to fulfill system design requirements. Non-standard systems include the diverse protection system (DPS), diverse indication system (DIS), NSSS integrity monitoring system (NIMS), radiation monitoring system (RMS), and seismic monitoring system (SMS).

Data Communications

~~Data communications within or between I&C systems are designed to provide reasonable assurance that any error in data communication will not cause inadvertent actuations or prevent the safety functions from being performed. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, and a network between qualified PLC and non-qualified DCS. The qualified PLC data communications network is independent and diverse from the non-qualified DCS data network.~~

Replace with "A" on the next page.

Human-System Interface

The APR1400 HSI is designed based on a compact workstation using the soft control and digital DCS. The compact workstation, which is based on HSI, provides a convenient operating environment to facilitate the display of plant status information to the operator so that operability is enhanced by using advanced display, alarm, and procedure systems. The HSI has sufficient diversity to demonstrate defense-in-depth protection against common-cause failure of the safety system.

7.1.1 Identification of Safety Systems and Non-Safety Systems

Safety and non-safety I&C systems, including supporting systems, are identified in the following subsections.

7.1.1.1 Plant Protection System

The PPS is a safety system that includes electrical, electronic, network, mechanical devices, and circuits and performs the following protective functions:

a. Reactor protection system (RPS)

"A"

Data communications within or between I&C systems is provided with the communication independence to ensure that there will be no adverse impact on the safety systems. Data communication systems are composed of a qualified PLC data communication network, a non-qualified DCS data communication network, a qualified serial data link, and Ethernet network. Communication independence is provided among safety divisions and between safety and non-safety data communication systems. The safety and non-safety data communication systems are diverse.

TS

Page intentionally blank

TS

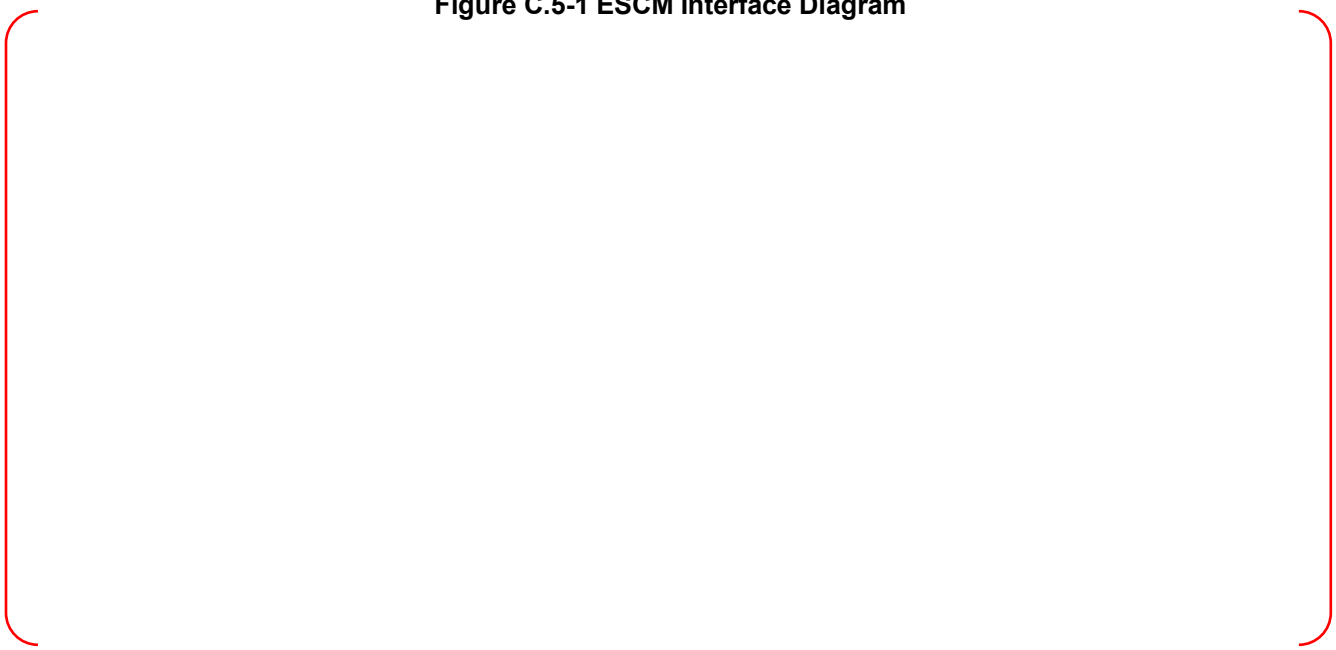
TS

TS

TS

TS

Figure C.5-1 ESCM Interface Diagram



TS

TS

TS

TS

TS

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

Page intentionally blank

TS

TS

TS