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

Question No. 07.07-6

Clarify the information given with regards to network data storms in Sections 4.4.5, "Design Features to Prevent CCF Due to Broadcast Storms on the DCN-I Network," and 4.4.6 of Technical Report APR1400-Z-J-NR-14012P, "Control System CCF Analysis Technical Report," Rev. 0.

IEEE Std. 603-1991, Clause 5.6.3, as incorporated by reference in 10 CFR 50.55a(a)(2), states, in part, that the safety system design shall be such that credible failures in and consequential actions by other systems, as documented in the design basis per Clause 4.8, shall not prevent the safety systems from meeting the requirements of this standard.

Sections 4.4.5 and 4.4.6 of Technical Report APR1400-Z-J-NR-14012P state, in part, that, "A broadcast storm could occur on the DCN-I network..." The sections go on to discuss how a broadcast storm is handled and its event type classification, including classification justification. However Section 4.4.5 does not provide an adequate technical basis to substantiate the event classification assigned to broadcast data storms.

NRC Information Notice 2007-15, "EFFECTS OF ETHERNET-BASED, NON-SAFETY RELATED CONTROLS ON THE SAFE AND CONTINUED OPERATION OF NUCLEAR POWER STATIONS," documents a network data storm event that resulted in a loss of multiple reactor recirculation pumps at Brown's Ferry Unit 3. The root cause of the data storm even was determined to be excessive network traffic and not a failure in the software or hardware of any specific component. It is not apparent that in this report that excessive network traffic was considered as a potential failure mode in the DCN-I network or other non-safety networks within this design.

1. Was excessive network traffic considered a potential failure mode in the APR1400 design? If so, where is this information described?

2. What are the design features in place to cope with excessive network traffic and the potential effects on safety and non-safety I&C components?

3. Provide more information on the technical basis/justification for the data storm event classification for the DCN-I and IFPD/ESCM Ethernet networks described in sections 4.4.5 and 4.4.6.

4. Does the applicant intend to verify the adequacy of operator actions to cope with a data storm event through an ITAAC?

5. Has the applicant verified the adequacy of operator actions through human factors engineering or analysis?

Response – (Rev. 1)

TS

TS

Impact on DCD

There is no impact on the DCD.

Impact on PRA

There is no impact on the PRA.

Impact on Technical Specifications

There is no impact on the Technical Specifications.

Impact on Technical/Topical/Environmental Reports

Subsections 4.4.5 and 4.4.6 of technical report APR1400-Z-J-NR-14012-NP, Rev. 0, “Control System CCF Analysis” will be revised as indicated in Attachment 1 associated with this response.

Subsection 4.6.1.3 of technical report APR1400-Z-J-NR-14001-NP, Rev. 0, “Safety I&C System” will be revised as indicated in Attachment 2 associated with this response.

TS

TS

4.4.5. Design Features to Prevent CCF Due to Broadcast Storms on the DCN-I Network

TS

Page intentionally blank

4.4.6. Design Features to Cope with Broadcast Storms on the IFPD/ESCM Ethernet Networks

TS

[ ]

RAI 68-7892 - Question 07.07-6_Rev.1

There is no difference in data transfer rate, data bandwidth, data accuracy and error performance during normal and abnormal operations (i.e., whether the nuclear power plant is in a steady state or undergoing a transient or accident condition).

The SDN has a deterministic network protocol that is used for non-node communication within a division. The controllers of PPS and ESF-CCS and FPDs will be nodes on the SDN.

There are two modes of data transmission of the SDN:

- Process data transfer - deterministic
- Message transfer - non-deterministic

Process data transfer is the mode of communications between the nodes in the same division. It is also the mode in which the FPDs receive data from the SDN network.

Insert "B" on the next page.

Message transfer is received for on-demand data that is initiated from the FPDs.

Details for deterministic communication are described in Reference 12.

4.6.1.4 Reliability

Error checking techniques for data integrity such as CRC are incorporated into the communication protocol to assure the integrity of the transmitted data.

Upon detection of the communication loss within a safety system, the system is designed such that communication failures shall not prevent safety systems from performing their intended safety function as analyzed in Appendix C.

Refer to Appendix C and Section 5.6 of Reference 12 for a detailed description on the SDL compliance to the criteria in DI&C-ISG-04 Section 1.

4.6.1.5 Control of Access

Security provisions are provided for the data communication system associated with the system to which it is connected such as key locked door and protection against unauthorized software alteration.

4.6.1.6 Single Failure Criterion

The configuration of the data communication system is designed so that the requirements of the SFC are satisfied. The FMEA shows that no single failure will defeat more than one of the four redundant safety I&C system divisions as applicable.

The FMEA for the safety I&C system in the DCD Chapter 7 describes and provides a detailed evaluation; including network cable and equipment failures, failure to transmit and receive data or transmission of erroneous data. The data communication system is designed with redundancy and multiple data paths, if necessary.

4.6.1.7 Independence

The data communication system is designed to maintain the independence between the safety divisions (A, B, C, D), and the independence between the safety and non-safety systems.

Communication between safety I&C systems is performed via SDL fiber optic cables only.

Page intentionally blank