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.:	**356-7881**
SRP Section:	**07 – Instrumentation and Controls – Overview of Review Process**
Application Section:	**7.0**
Date of RAI Issue:	**01/04/2016**

Question No. 07-20

Provide the unavailability analysis as described in Technical Report APR1400-Z-J-NR-14001-P, Rev.0, “Safety I&C System.”

10 CFR 50.55a(h)(3) requires compliance with IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.15, requires, in part, systems for which either quantitative or qualitative reliability goals have been established, appropriate analysis of the design shall be performed in order to confirm that such goals have been achieved. Technical Report APR1400-Z-J-NR-14001-P, Rev.0, Section 7.2, "Unavailability Analysis," describes analysis that assesses the availability of the safety I&C systems that, along with the individual system FMEAs, addresses reliability requirements for the APR1400 design. The applicant does not present the analysis within this report, nor does the applicant provide information on where this analysis may reside within the application.

1. Provide the unavailability analysis, as described in Section 7.2 of Technical Report APR1400-Z-J-NR-14001-P, Rev.0.

2. Is this analysis applicable to all safety I&C systems?

Response

1. As stated, 10 CFR 50.55a(h)(3) requires compliance with IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.15 requires an appropriate analysis for systems for which either quantitative or qualitative reliability goals have been established to confirm that such goals have been achieved.

   The Standard Review Plan (SRP) points to SRP Appendix 7.1-B Subsection 4.1 and SRP Appendix 7.1-C Subsection 5.15 to address reliability in GDC 21 compliance.

SRP Appendix 7.1-B Subsection 4.1 discusses protection system reliability, specifically in the second two paragraphs which state: “Staff acceptance of system reliability is based on the deterministic criteria described in IEEE Std. 279-1971 rather than on quantitative reliability goals. The NRC staff does not endorse the concept of quantitative reliability goals as the sole means of meeting the requirements for reliability of protection systems. Quantitative reliability determination, using a combination of analysis, testing, and operating experience can provide an added level of confidence in the reliable performance of the I&C system. The applicant/licensee should justify that the degree of redundancy, diversity, testability, and quality provided in the protection system design is adequate to achieve functional reliability commensurate with the safety functions to be performed.”

SRP Appendix 7.1-C Subsection 5.15 discusses reliability as it applies to IEEE Std. 603-1991 clause 5.15. This section states that for computer systems, both hardware and software reliability should be analyzed and points to SRP Appendix 7.1-D for software reliability determination and SRP BTP 7-14 for software development processes that are expected to produce reliable software. This section also states “the assessment of reliability should consider the effect of possible hardware and software failures and the design features to prevent or limit the effects of these failures. SRP Appendix 7.1-D indicates that the concept of quantitative reliability goals is not sufficient as a sole means of meeting the NRC’s regulations for the reliability of digital computers used in safety systems. This is discussed in more detail as part of subsection 4 above. SRP Appendix 7.1-C Subsection 4 discusses reliability stating “Clause 4.9 of IEEE Std. 603-1991 requires the identification of the methods used to determine that the reliability of the safety system design is appropriate for each such design, and the identification of the methods used to verify that any qualitative or quantitative reliability goals imposed on the system design have been met. Staff acceptance of system reliability is based on deterministic criteria described in IEEE 603-1991, and IEEE Std. 7-4.3.2-2003, rather than on quantitative reliability goals. Therefore, the system design basis should discuss the methods used to confirm that these deterministic criteria have been met.

The APR1400 addresses the reliability requirements of IEEE Std. 603-1991 through the FMEA as indicated in Technical Report APR1400-Z-J-NR-14001-P, Rev. 0, Section 7.1. The FMEA was performed IAW ANSI/IEEE-352-1987 and included in the DCD as Table 7.2-7 & 7.3-8.

The Unavailability Analysis described in APR1400-Z-J-NR-14001-P, Section 7.2 is not intended to address the reliability requirements of IEEE Std. 603-1991 and Section 7.2 will be removed from APR1400-Z-J-NR-14001-P.

2. The Unavailability Analysis described in APR1400-Z-J-NR-14001-P, Section 7.2 is not intended to address the reliability requirements of IEEE Std. 603-1991 and Section 7.2 will be removed from APR1400-Z-J-NR-14001-P.

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 7.2 will be deleted from APR1400-Z-NR-14001-P/NP, Rev. 0, “Safety I&C System” as shown in the Attachment.

- Software (fails off/stalls/spurious data)
- Fiber optic receiver/transmitter modules (off/open/shorted)
- Relay coils/contact (open/shorted)
- Manual switches (open/shorted)

Symptoms and local effects: Identifies the immediate consequence of each failure mode and any secondary side effects.

Method of detection: Identifies method by which failure is detected, e.g.: self- annunciating, automatic or manual test, etc.

Inherent compensating provisions: Any compensating features within the design are addressed such as:

- Redundant divisions of the PPS and ESF-CCS
- Auctioneered AC/DC power supplies
- Fail-safe design. For example, outputs go to appropriate trip, initiation or actuation state upon loss of electrical power. Fail-safe design upon loss of data communications. For example, SDN failures (due to a CI failure, or break in an interconnecting coaxial or fiber optic cable, etc.) that result in loss of data communications to the receiving PM. Upon detection of the loss of communications, the effected PM will force its safety-related trip output signals to their “fail-safe” state.

Effect upon system: Describes the ultimate effect of the failure mode on the overall system, e.g.: logic is changed from 2-out-of-4 to 2-out-of-3 coincidence or ESFAS function is actuated.

Remarks and other effects: Identifies the effects of the failure on overall plant operations or interfacing systems.

The FMEA considers the effects of these types of failures on the system and any other impacts on interfacing plant systems or components.

The system-level FMEA results for the PPS and ESF-CCS are included in the DCD.

~~7.2 Unavailability Analysis~~

~~An unavailability analysis is performed on both the PPS and the ESF-CCS to assess their unavailability when they are requested to perform their functions. The analysis quantifies the probability that the PPS would fail to trip the reactor upon demand. The analysis also quantifies the probability that ESF-CCS would fail to actuate safe guard equipment when demanded.~~

~~The fault tree model for the PPS and ESF-CCS design is developed to perform this analysis. The PPS and ESF-CCS fault tree contains failures or faults which could render the affected system unavailable given a demand for the system to perform its intended function.~~