ArevaEPRDCPEm Resource

From: Tesfaye, Getachew
Sent: Friday, September 10, 2010 7:33 PM
To: 'usepr@areva.com'
Cc: Zhao, Jack; Morton, Wendell; Mott, Kenneth; Spaulding, Deirdre; Truong, Tung; Zhang, Deanna; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: Draft - U.S. EPR Design Certification Application RAI No. 442 (4295,5076,5068,5067), FSAR Ch. 7
Attachments: Draft RAI_442_ICE1_4295_5076_5068_5067.doc

Attached please find draft RAI No. 442 regarding your application for standard design certification of the U.S. EPR. If you have any question or need clarifications regarding this RAI, please let me know as soon as possible, I will have our technical Staff available to discuss them with you.

Please also review the RAI to ensure that we have not inadvertently included proprietary information. If there are any proprietary information, please let me know within the next ten days. If I do not hear from you within the next ten days, I will assume there are none and will make the draft RAI publicly available.

Thanks,
Getachew Tesfaye
Sr. Project Manager
NRO/DNRL/NARP
(301) 415-3361

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 1983

Mail Envelope Properties (0A64B42AAA8FD4418CE1EB5240A6FED11E222CF709)

Subject: Draft - U.S. EPR Design Certification Application RAI No. 442 (4295,5076,5068,5067), FSAR Ch. 7
Sent Date: 9/10/2010 7:33:19 PM
Received Date: 9/10/2010 7:33:20 PM
From: Tesfaye, Getachew

Created By: Getachew.Tesfaye@nrc.gov

Recipients:
"Zhao, Jack" <Jack.Zhao@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Mott, Kenneth" <Kenneth.Mott@nrc.gov>
Tracking Status: None
"Spaulding, Deirdre" <Deirdre.Spaulding@nrc.gov>
Tracking Status: None
"Truong, Tung" <Tung.Truong@nrc.gov>
Tracking Status: None
"Zhang, Deanna" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Jackson, Terry" <Terry.Jackson@nrc.gov>
Tracking Status: None
"Canova, Michael" <Michael.Canova@nrc.gov>
Tracking Status: None
"Colaccino, Joseph" <Joseph.Colaccino@nrc.gov>
Tracking Status: None
"ArevaEPRDCPEm Resource" <ArevaEPRDCPEm.Resource@nrc.gov>
Tracking Status: None
"'usepr@areva.com'" <usepr@areva.com>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	727	9/10/2010 7:33:20 PM
Draft RAI_442_ICE1_4295_5076_5068_5067.doc	74234	

Options
Priority: Standard
Return Notification: No
Reply Requested: No
Sensitivity: Normal
Expiration Date:
Recipients Received:

Draft

Request for Additional Information No. 442(4295, 5076, 5068, 5067), Revision 1

9/10/2010

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.01 - Instrumentation and Controls - Introduction
SRP Section: 07.03 - Engineered Safety Features Systems
SRP Section: 07.09 - Data Communication Systems

Application Section: FSAR Ch 7

QUESTIONS for Instrumentation, Controls and Electrical Engineering 1 (AP1000/EPR Projects) (ICE1)

07.01-26

Provide sufficient information for the staff to conclude that the safety-related standalone or packaged systems provide sufficient independence between other safety divisions or non-safety systems.

10 CFR 50.55a(h) (IEEE Std. 603-1991) requires addressing the independence between safety systems and other systems. U.S. EPR FSAR Subsection 7.1.1.5 states that Level 0 interface level includes components such as sensors, actuators, and switchgear. However, in this subsection there are also a few safety standalone or packaged systems. The staff requests the applicant to include sufficient design information to address all aspects of independence for those standalone I&C systems. In addition, clarify how those standalone I&C systems are connected in Figure 7.1-2 of the FSAR and what kind of platforms will be used for the safety-related standalone systems.

07.01-27

a. Address identifiable, but non-detectable failures. Clause 5.1 of IEEE Std. 603-1991 states, in part, that safety systems shall perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures. IEEE Std. 603-1991 states identifiable, but non-detectable failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication. Sections 7.2.2.2 and 7.3.2.2 of U.S. EPR FSAR did not address identifiable, but non-detectable failures. If there are no identifiable, but non-detectable failures, then state so. Also, clearly define what the IEEE Std. 603-1991 detectable failures (i.e. U.S. EPR FMEA undetected failures).

b. During an audit in February 2010, the NRC staff found the comments column in the U.S. EPR Failure Modes and Effects Analysis (FMEA) helpful to understand the analysis. WE request that the information in the comments column be incorporated into the respective FMEA summary tables in the U.S. EPR FSAR, Table 7.2-2 for Reactor Trip and Table 7.3-2 for ESF Actuations.

07.01-28

Clarify the actuation path for system and component level control of safety systems from the Process Information and Control System (PICS).

10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components sufficient to permit understanding of the system designs. During the review of Technical Report ANP-10309, "U.S. EPR Digital Protection System", Revision 0, the staff observed that in Section 8.5, the applicant states that, " While the US EPR design includes the ability to manually manipulate these actuators at the individual component level from the non-safety-related PICS (the component level manipulations are not processed through the PS), the system level actuations addressed in this section are implemented through Class 1E actuation paths and are single failure tolerant." The applicant did not state where in the ESF logic chain that the system level manual actuation originates from the PICS. In a teleconference the staff had with the applicant, the applicant states that the manual actuation signal goes through the PACS. During this teleconference, the applicant committed to clarifying this Section 8.5 of Technical Report ANP-10309, U.S. EPR Digital Protection System, Revision 0, in order to make it clearer that the system level manual actuation from the PICS goes through the PACS.

07.01-29

Clarify FSAR and technical report figures associated with manual engineered safety feature actuation.

10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components sufficient to permit understanding of the system designs. The staff, noticed there are some differences between the logic drawings that depict a "typical ESFAS actuation sequence" in Figure 8-1 ANP-10281P, "US EPR Digital Protection System Technical Report, Revision 0, and Figure 7.3-1 of US EPR FSAR Tier 2, Section 7.3. The staff also observed that there is no manual actuation signal line depicted in either figure for ESF, whereas a manual actuation is shown for RT functions shown in Figures 7-4 and 7.2-3 of ANP-10281P, "US EPR Digital Protection System Technical Report, Revision 0, and US EPR FSAR Tier 2, Section 7.2, respectively. The staff presented its observations to the applicant in a teleconference and the applicant agreed to modify Figure 8-1 ANP-10281P, "US EPR Digital Protection System Technical Report, Revision 0, and Figure 7.3-1 of US EPR FSAR Tier 2, Section 7.3 to bring them in line with each other. The applicant also verbally committed to adding detail for manual actuation for each ESF figure to accurately reflect that this functionality does exist in the typical ESF actuation sequence.

07.01-30

Provide details on how the U.S. EPR design will verify functionality of the self testing features based on guidance from BTP 7-17.

For the U.S. EPR design, the applicant has committed to meeting BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions." BTP 7-17 (which cites GDC

21 and 10 CFR 50.55a(h) as a regulatory bases) states that: "(a) Self-test functions should be verified during periodic functional tests, and (b) If automatic test features are credited with performing surveillance test functions, provisions should be made to confirm the execution of the automatic test during plant operation. The capability to periodically test and calibrate the automatic test equipment should also be provided. The balance of surveillance and test functions that are not performed by the automatic test feature should be performed manually to meet the intent of Regulatory Guide 1.118. In addition, the automatic test feature function should conform to the same requirements and considerations (e.g., test interval) as the manual function."

a. The staff requests that the applicant provide details on the method by which the U.S. EPR Protection System self testing features will be periodically verified and how the operation will be confirmed during plant operation.

b. How does the applicant propose to meet item (b), as quoted above?

07.01-31

Follow-up RAI 321, Question 07.01-19.

The staff requests that the following additional information be provided:

a. Information which adequately describes your commercial grade dedication program.

b. Information which adequately identifies the specific critical characteristics.

In the original question, the staff RAI requested the following:

> Describe the software development process (SDP) used for the video display that will be used in the safety information and control systems (SICS), particularly with respect to identification of aspects that differ from the SDP used for the TELEPERM XS. The applicant needs to provide a description of the differences in the SDP for the safety-related video display. The staff needs to be able to determine acceptability with regards to the quality requirements of 10 CFR 50.55a(a)(1); 10 CFR Part 50, Appendix A, General Design Criteria 1; 10 CFR Part 50, Appendix B; and 10 CFR 50.55a(h) are met.

In its response, AREVA NP indicated that: "QDS system software is commercial software. … qualify the QDS … through a commercial dedication process that conforms to the guidance of EPRI TR-106439, 'Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications.' … The QDS specific [development] tools [used to create the QDS application software] will be qualified as part of the commercial grade dedication process. …"

The NRC staff safety evaluation (SE) of TR-106439 stated that applicants referencing TR-106439 need to provide details regarding the dedication process. AREVA NP listed the following four (4) items as the process they would follow for commercial dedication.

1. Identification of the critical characteristics the system software must exhibit.
2. Definition of a combination of supplemental testing, supplier surveys, source verifications, or performance reviews, which demonstrate that the system software exhibits the critical characteristics.

3. Performance of the defined combination of supplemental testing, supplier surveys, source verifications, or performance reviews.
4. Creation of a dedication acceptance package that documents the results of activity 3 and provides evidence that the QDS system software exhibits the required critical characteristics.

The staff has determined that the four (4) items do not provide a detailed description of their dedication process. Additional information is requested which describes the detailed commercial dedication process that AREVA NP will follow, in conformance with EPRI TR-106439. Additionally, in its response, AREVA NP did not provide the specific critical characteristics. The NRC staff SE of TR-106439 stated that applicants referencing TR-106439 need to provide specific critical characteristics. Additional information is requested which provides the specific critical characteristics.

07.01-32

Follow-up RAI to 321, Question 07.01-19.

The staff requests that the following additional information be provided:

AREVA NP addressed the issue concerning the language “without further NRC review” in its Software Program Manual (SPM). How will AREVA NP address this language in the EPR FSAR, Tier 2?

In the Question 07.01-19, the staff requested the following:

> Describe the software development process (SDP) used for the video display that will be used in the safety information and control systems (SICS), particularly with respect to identification of aspects that differ from the SDP used for the TELEPERM XS.
> The applicant needs to provide a description of the differences in the SDP for the safety-related video display. The staff needs to be able to determine acceptability with regards to the quality requirements of 10 CFR 50.55a(a)(1); 10 CFR Part 50, Appendix A, General Design Criteria 1; 10 CFR Part 50, Appendix B; and 10 CFR 50.55a(h) are met.

The staff reviewed the AREVA NP response to RAI 321, Question 07.01-19, and found that the proposed FSAR markup (Tier 2, Revision 2 Interim, Page 7.1-5) contains language which is problematic. The problematic phase is “without further NRC review.” AREVA NP addressed this issue in its Software Program Manual (SPM). How will AREVA NP address this language in the EPR FSAR, Tier 2?

07.03-32

Follow-up to RAI 285, Question 07.03-27

After reviewing the applicant's response to RAI 285, Question 07.03-27, the staff requests the applicant to explicitly identify in Chapter 7 which Protection System (PS) manual functions are credited in the safety analysis.

U.S. EPR DC-FSAR, Section 15.0.0.3.7 identifies operator actions that are credited for isolating an affected SG during a steam generator tube rupture (SGTR) event. U.S. EPR DC-FSAR

Chapter 7 does not address the crediting of manual actions for a SGTR event. Nor did Chapter 7 address component level control in Section 7.3. The staff generated an RAI requesting the applicant to clarify the issue. Although the applicant provided a response with good information that addressed some of the staff's concerns, there are issues that still require resolution before this question can be closed. This RAI question is intended to address compliance of the PS design with IEEE 603-1998, Clauses 4.e, 5.8.1 and 6.2.b. The staff used Standard Review Plan Section 7.1-C and 7.3 as guidance.

1. For Section 7.3....for each ESF function section, explicitly state in that section there are safety-related, component level manual controls available on both PICS and SICS in the Main Control Room. This is consistent with how manual system-level control is discussed in Section 7.3
2. For Section 7.3....state explicitly, in each applicable ESF system section, that it's safety-related manual actuation is credited in the safety analysis. This is consistent with how manual system-level control is discussed in Section 7.3.
3. For Chapter 7....for other manual actions credited in the safety analysis, state explicitly in the applicable section. For example Section 15.0.0.3.7 states that there is a manual action to perform a reactor trip if the chemical and volume control system (CVCS) is running during an SGTR. This should be called out in Section 7.2.

07.03-33

Incorporate the response to the 4th RAI to Topical Report ANP-12081P, "U.S. EPR Digital Protection System Topical Report" and Attachment B to the 2nd RAI into the U.S. EPR, Tier 2, FSAR or Technical Report ANP-10309P, "U.S. EPR Digital Protection System Technical Report" to demonstrate conformance to IEEE Std. 603-1998, Clause 4.10.

Clause 4.10 of IEEE Std. 603-1998 requires, as a part of the design basis, identification of the critical points in time or the plant conditions, after the onset of a design basis event. In Section 4.3 of the SER for Topical Report EMF-2110(NP)(A), the staff stated that the TXS system architecture and the system response time test methodology, as discussed in the topical report, demonstrated that the TXS system design is consistent with BTP HICB-21 (Note: BTP-21 provides updated guidance to BTP HICB-21). It is, therefore, acceptable. However, the staff included plant-specific action item (PSAI) 11 in the SER for licensees who reference this topical report to perform protection system response time tests in accordance with plant technical specification requirements. PSAI 11 required licensees to evaluate plant-specific accident analysis to confirm that a TXS reactor trip system includes the provision to detect accident conditions and anticipated operational occurrences in order to initiate reactor shutdown (safety analysis confirmation for accuracy and time response) consistent with accident analysis presented in Chapter 15 of the plant safety analysis report. To address this PSAI, the staff requested the applicant to demonstrate how the guidance of BTP 7-21 is addressed in the design of the protection system to meet IEEE Std. 603-1998, Clause 4.10. This request was documented in the 4th RAI for Topical Report ANP-10281P, “U.S. EPR Digital Protection System Topical Report.” In response to the RAI, the applicant stated that the methodology used to estimate the response time of the computerized portion of the PS establishes a theoretical bounding response time for the typical types of functions performed by the PS. The final response time of the PS will be verified to be within the bounding time limits established for the PS. The applicant provided an analysis of the allocation of time delays to the computerized portion of the PS in Attachment B of the 2nd RAI for the U.S. Digital Protection Topical Report.

07.03-34

Provide more information on the self-diagnostic features of the PACS. U.S. EPR FSAR, Tier 2, Revision 1, Section 7.1.2.6.21 states the following: "The PACS contains self-diagnostic test features to alert plant personnel of a fault within one of the PACS components.

Currently, Chapter 7 of the U.S. EPR FSAR does not provide any specific details on the PACS modules self-testing abilities. There is also no information in Chapter 7 where status indication, especially in terms of alarms, is displayed in the Main Control Room. ANP-10310P, "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report" provides details on the PACS. However it does not provide enough detail for the staff to make a finding. The applicant does not consider the PACS a part of the Protection System (PS), so the inherent self-testing features will be evaluated individually by the staff as well. The staff created this RAI question in order the get further information on the PACS self-diagnostic/monitoring abilities in order to gain a greater understanding of all self-testing features of the entire platform. Standard Review Plan Section 7.1-C and BTP 7-17 were used as guidance.

1. Provide more detailed information on the PACS self-testing features, in terms of coverage capabilities, types of failures they can detect, and how they meet IEEE Std. 603 -1998, Clauses 5.7 and 5.8.
2. Where do alarms and any other equipment status details from the PACS display? PICS or SICS, both or another display entirely
3. Provide more detail on how the PACS self diagnostic features addresses guidance from BTP 7-17, "Guidance on Self-test and Surveillance Test Provisions". Section 3 of BTP 7-17 states that, "Self-test functions should be verified during periodic functional tests."
4. Does the applicant intend to provide an ITAAC to verify the self-testing functions of the PACS and what will be the acceptance criteria for this ITAAC?

07.09-61

Demonstrate how the use of SINEC H1 protocol which operates over Ethernet meets the reliability requirements of IEEE Std. 603-1998, Clause 5.15.

Clause 5.15 of IEEE Std. 603-1998 requires appropriate analysis be performed on the system design for which either quantitative or qualitative reliability goals have been established to determine that such goals have been achieved. To meet the requirements of IEEE Std. 603-1998, Clause 5.15, data communications systems in support of safety functions should demonstrate sufficient reliability in accordance with the acceptance criteria described in SRP Section 7.9. SRP Section 7.9 states that protocols proposed for use, whether standard or proprietary, should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

Topical Report EMF-2110(NP) states that two communications protocols are used in the TXS system, the SINEC L2 Profibus protocol and the SINEC H1 Ethernet protocol. In addition, Section 7.1.1.3.1 of the U.S. EPR, Tier 2, FSAR states that the TXS Ethernet protocol is also used between the Panel Interfaces (PI)s of the SICS and the Safety Qualified Display System (QDS) within the SICS. The staff finds that the applicant has not demonstrated how these

protocols communicate deterministically for safety applications to meet the requirements of IEEE Std. 603-1998, Clause 5.15. Specifically, the applicant has not provided an analysis of hazards and performance of these two protocols to demonstrate that data communications using these protocols are deterministic. This is of special concern for SINEC H1 protocol since it is Ethernet-based, which typically has been shown to be non-deterministic. As such, the staff requests the applicant to provide additional information to demonstrate how data communications using these protocols are deterministic and to incorporate the response into the U.S. EPR, Tier 2, FSAR.

07.09-62

Follow-up to RAI 286, Question 7.09-49.

Incorporate the response to RAI 286, Question 7.09-49 into the U.S. EPR, Tier 2 FSAR.

10 CFR Part 50, Appendix A, General Design Criteria 13, requires, in part, instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety. The NRC issued Information Notice: 2007-15, “Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations,” (ADAMS Accession No. ML071510428), describing operational experience on the effects of a data storm on non-safety control networks. The staff issued RAI 286, Question 7.09-49 to request the applicant to demonstrate how operating experience insights regarding the effects of data storms on non-safety data communications networks are addressed for the plant data network, which provides important to safety functions such as alarms, indications, and controls for all operational conditions. In response, the applicant states that sound engineering and design practices will be applied to development of the U.S. EPR plant data network and the instrumentation and controls (I&C) systems connected to the network. The plant data network will be designed to withstand data traffic, and the interfacing I&C systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the network. Specific design details regarding preclusion of data storm events on a non-safety-related network will be developed later in the design process, and are thus not planned for inclusion in the application for design certification. However, the design features of the safety-related I&C systems that protect the safety-related functions will protect against loss of safety functions in case of data storm events on the non-safety-related plant data network. The staff finds this response acceptable. However, the staff requests the applicant to incorporate this response into the U.S. EPR, Tier 2, FSAR.

07.09-63

Clarify statements made in Technical Report ANP-10309P regarding the potential modification to the general network concepts and diagrams described in this technical report.

10 CFR 52.47(a)(2) requires that the design certification application must include a description and analysis of the structures, systems, and components (SSCs) of the facility, with emphasis upon performance requirements, the bases, with technical justification therefore, upon which these requirements have been established, and the evaluations required to show that safety functions will be accomplished. Section 6 of Technical Report ANP-10309P provides a description of the communications network topology within the U.S. EPR PS. Figure 6-3 through Figure 6-19 of this technical report depicts the network architecture within the PS architecture,

implemented using individual point-to-point and ring networks. These figures are designated proprietary. The technical report states that these represent the intended PS network design. These figures are provided to assist in understanding general network concepts described in this technical report, but are subject to modification during the U.S. EPR detailed design process. The staff requested the applicant to clarify how the general network concepts described in this technical report may be modified.

07.09-64

Follow-up to RAI 56, Questions 7.9-11

Clarify U.S. EPR, Tier 2, FSAR, Figure 7.1-7 to demonstrate compliance with IEEE Std. 603-1998, Clause 5.1.

IEEE Std. 603-1998, Clause 5.1 requires safety systems to perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. In the case of SAS, U.S. EPR, Tier 2, FSAR, Figure 7.1-7 shows that the Control Units (CU)s of redundant Safety Automation System (SAS) divisions are interconnected in a bus network. As such, the staff finds that the applicant has not demonstrated how a failure within the CUs of one division will not propagate to another division. As a result, the staff requested the applicant to demonstrate how the SAS design meets the requirements of IEEE Std. 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21, in RAI 56, Question 7.9-11. In response, the applicant provided in “Response to Request for Additional Information No. 56, Supplement 1: U.S. EPR Design Certification Application,” a description of how the data communications within the SAS meet IEEE Std. 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21. This response states that, as described in U.S. EPR, Tier 2, FSAR, Section 7.1.1.4.2, “Data Communications,” the CU-CU networks within the SAS are point-to-point between divisions, and separate networks are provided for the A and B redundancies. This result in six individual point-to-point connections for redundancy A, and another six interdivisional connections exist for redundancy B. A single failure that impairs any one of these connections only affects communications between two CUs. For example, if the Division 1 CU(A) to Division 2 CU(A) connection fails, Division 1 CU(A) and Division 2 CU(A) both still communicate with the CU(A)s in Divisions 3 and 4. The staff finds this response is inconsistent with Figure 7.1-7 within the U.S. EPR, Tier 2, FSAR, as documented in RAI 07.09-54. Specifically, the staff reviewed Figure 7.1-7, “Safety Automation System Architecture,” and finds that these CU-CU networks are connected in a bus topology and not point-to-point connections as specified in the RAI response. The staff requests the applicant to clarify the representation of the SAS network architecture to clearly demonstrate the point to point connection between CUs to show how the design meets IEEE Std. 603-1998, Clause 5.1.

07.09-65

Incorporate the response to RAI 24 and 38 for Topical Report ANP-10281P into the U.S. EPR, Tier 2, FSAR or its referenced documents, to demonstrate independence when the ring network topology is used in the Protection System.

10 CFR Part 50, Appendix A, GDC 23, “Protection System Failure Modes,” requires the protection system to be designed to fail into a safe state or into a state demonstrated to be

acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced. NUREG/CR-6082, “Data Communications,” provides additional discussion of independence and failure modes. In response to RAI 24, the applicant described the network failure modes and how these failures are bounded. In RAI 38 of the “Third Request for Additional for Information” for Topical Report ANP-10281P, the staff requested the applicant to describe the failure modes of the ring network employed in the U.S. EPR digital PS used to provide SPND measurements to the RAU and certain APUs, as required by GDC 23 of Appendix A to 10 CFR Part 50. The applicant provided in “Response to Third Request for Additional Information” for the Topical Report ANP-10281P, a description of how data messages are interpreted for validity and different types of message failures. The response also described how the APU will process each type of failure mode. In addition, the applicant provided in “U.S. EPR Digital Protection System Topical Report, Supplemental Information” a table detailing postulated communications failures within the TXS communications system. The staff requests the applicant to incorporate these responses from RAI 24 and RAI 38 for Topical Report ANP-10281P and the information in “U.S. EPR Digital Protection System Topical Report, Supplemental Information” into the U.S. EPR, Tier 2 FSAR or Technical Report ANP-10309P to demonstrate compliance to GDC 23.

07.09-66

Follow-up to RAI 286, Question 7.9-52.

Incorporate the response to RAI 286, Question 7.9-52 regarding the quality of the plant data network to demonstrate compliance to 10 CFR Part 50 General Design Criterion (GDC) 1.

GDC 1 requires structures, systems, and components important to safety to be designed, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. Where generally recognized codes and standards are used, they shall be identified and evaluated to determine their applicability, adequacy, and sufficiency and shall be supplemented or modified as necessary to assure a quality product in keeping with the required safety function. The Processing Information and Control System (PICS) is used to operate the plant during normal and accident conditions. This operation is achieved using the plant data network. In RAI 286, Question 7.9-52, the staff requested the applicant to demonstrate the quality and network capacity of the plant data network to support PICS functions. In response, the applicant stated that the normal control systems that will be utilized in the U.S. EPR must have adequate bandwidth to reliably operate and maneuver all the other systems in the reactor plant needed for plant operation and also to keep the plant reliably online. These I&C systems will be specified and procured consistent with the application of digital control technology currently in use in other power generation facilities. The staff requests the applicant to include the commitment to have adequate bandwidth to reliably operate and maneuver all systems in the reactor plant needed for plant operation and to keep the plant reliably online in the U.S. EPR, Tier 2, FSAR to demonstrate compliance to GDC 1. In addition, clarify whether the plant data network and terminal data network are classified as part of the PICS.

07.09-67

Describe the communication pathway used to initiate a turbine trip upon an automatic or manual reactor trip to meet 10 CFR Part 50, General Design Criterion (GDC) 20.

GDC 20 requires, in part, that the protection system is designed to initiate automatically the operation of the appropriate systems and to sense accident conditions and to initiate the operation of systems and components important to safety. Section 7.1.1.4.7 of the U.S. EPR, Tier 2, FSAR states that the TG I&C system regulates the operation of the turbine-generator for power generation. Demonstrate that upon a reactor trip, initiated either manually by the operator or automatically by the PS or the DAS, reliable communication pathways between the PS and the TG I&C system, and between the DAS and the TG I&C system, exist to ensure that the TG I&C system receives the reactor trip signal to meet the requirements of GDC 20.