ArevaEPRDCPEm Resource

From: Pederson Ronda M (AREVA NP INC) [Ronda.Pederson@areva.com]
Sent: Friday, November 13, 2009 3:34 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 286, FSAR Ch. 7
Attachments: RAI 286 Response US EPR DC.pdf

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information RAI 286. The attached file, "RAI 286 Response US EPR DC" provides technically correct and complete responses to 8 of the 18 questions.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 286 Questions 07.08-8, 07.09-50, 07.09-55 and 07.09-58.

The following table indicates the respective page(s) in the response document, "RAI 286 Response US EPR DC," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 286 — 07.06-3	2	2
RAI 286 — 07.07-18	3	4
RAI 286 — 07.07-19	5	5
RAI 286 — 07.08-7	6	6
RAI 286 — 07.08-8	7	7
RAI 286 — 07.08-9	8	8
RAI 286 — 07.09-46	9	9
RAI 286 — 07.09-47	10	10
RAI 286 — 07.09-49	11	11
RAI 286 — 07.09-50	12	12
RAI 286 — 07.09-51	13	13
RAI 286 — 07.09-52	14	14
RAI 286 — 07.09-53	15	15
RAI 286 — 07.09-54	16	17
RAI 286 — 07.09-55	18	18
RAI 286 — 07.09-56	19	20
RAI 286 — 07.09-57	21	21
RAI 286 — 07.09-58	22	22

A complete answer is not provided for 10 of the 18 questions. The schedule for a technically correct and complete response to these questions is provided below.

Question #	Response Date
RAI 286 — 07.06-3	December 18, 2009
RAI 286 — 07.07-19	December 18, 2009
RAI 286 — 07.08-7	January 22, 2010
RAI 286 — 07.08-9	January 22, 2010
RAI 286 — 07.09-46	January 22, 2010
RAI 286 — 07.09-47	February 26, 2010
RAI 286 — 07.09-49	January 22, 2010

RAI 286 — 07.09-52	January 22, 2010
RAI 286 — 07.09-53	December 18, 2009
RAI 286 — 07.09-57	December 18, 2009

Sincerely,

Ronda Pederson

ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Wednesday, October 14, 2009 8:06 PM
To: ZZ-DL-A-USEPR-DL
Cc: Cheung, Calvin; Mott, Kenneth; Zhang, Deanna; Spaulding, Deirdre; Jackson, Terry; Canova, Michael; Guardiola, Maria; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 286(3567,3561,3562,3563), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 27, 2009, and discussed with your staff on September 3, 2009. Drat RAI Question 07.09-48 was deleted and Draft RAI Questions 07.09-47, 07.09-51, and 07-09-52 were modified as a result of that discussion. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 952

Mail Envelope Properties (5CEC4184E98FFE49A383961FAD402D310165D9AF)

Subject: Response to U.S. EPR Design Certification Application RAI No. 286, FSAR Ch. 7
Sent Date: 11/13/2009 3:33:50 PM
Received Date: 11/13/2009 3:33:52 PM
From: Pederson Ronda M (AREVA NP INC)

Created By: Ronda.Pederson@areva.com

Recipients:
"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen V (AREVA NP INC)" <Karen.Delano@areva.com>
Tracking Status: None
"PANNELL George L (AREVA NP INC)" <George.Pannell@areva.com>
Tracking Status: None
"Tesfaye, Getachew" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

Post Office: AUSLYNCMX02.adom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	3456	11/13/2009 3:33:52 PM
RAI 286 Response US EPR DC.pdf	151598	

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

Response to

Request for Additional Information No. 286 (3567, 3561, 3562, 3563), Revision 1

10/14/2009

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.06 - Interlock Systems Important to Safety
SRP Section: 07.07 - Control Systems
SRP Section: 07.08 - Diverse Instrumentation and Control 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)

Question 07.06-3:

Follow-up to RAI Question No. 07.06-1

Where is the information below provided in the FSAR?

AREVA NP's response to RAI Question 07.06-1 states:

> "During a pressure increase due to the failed closed large miniflow valve of one of the MHSI pumps, by the time RCS pressure reaches the RHR safety valve opening setpoint, the three MHSI pumps with open large miniflow lines are no longer able to inject due to the higher RCS pressure caused by the single MHSI pump with its large miniflow valve closed."

10 CFR 52.47(a)(2) requires, in part, that a description of structures, systems, and components be sufficient to permit understanding of the systems design and their relationship to the safety evaluation. If this information does not reside in the U.S. EPR FSAR, please include this information.

Response to Question 07.06-3:

A response to this question will be provided by December 18, 2009.

Question 07.07-18:

Follow-up to RAI Question No. 07.07-16

Describe further why Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation," Revision 3, does not apply to the incore and excore instrumentation systems for the U.S. EPR.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 6.8 of IEEE Std. 603-1991 requires allowance for instrument uncertainties between the process analytical limit and the device setpoint. Regulatory Guide 1.105 provides an acceptable method for addressing Clause 6.8. In the response to RAI 07.07-16, AREVA NP stated that the regulatory guide was only applicable to the Protection System since the setpoints resided in the software of that system and not to the incore and excore instrumentation system. While the staff acknowledges that the setpoints reside in the Protection System, the uncertainties that influence the setpoint methodology and calcuations are associated with the safety-related instruments. Therefore, the regulatory guide would not only be applicable to the system where the setpoint resides, but to all I&C systems that could contribute to the uncertainties factored into the the setpoint methodology and calculations. Provide further description as to why the incore and excore instrumentation systems should not address the guidance in Regulatory Guide 1.105 and update the U.S. EPR DC-FSAR accordingly.

Response to Question 07.07-18:

Regulatory Guide 1.105, "Setpoints for Safety-Related Instrumentation," Revision 3, does not apply to the incore and excore instrumentation systems for the U.S. EPR because these systems do not develop or use setpoints for actuation. The setpoints associated with the protection system (PS) are maintained within the PS software only.

Applying RG 1.105 to the PS suggests that the uncertainties introduced by incore and excore instruments (as well as other plant process measurement sensors) are factored into the relevant PS setpoints. Applying RG 1.105 guidance to the incore and excore instrumentation systems will result in no design or engineering actions beyond what is already required by applying RG 1.105 to the PS, and it is unnecessary to apply RG 1.105 to the instruments.

Uncertainties associated with safety-related instruments are compensated for in the PS software. The uncertainty methodology is described in detail in the following topical reports:

1. The setpoint methodology for the incore instrumentation system is described in ANP-10287P, Revision 0, “Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report,” Section 2.2, Section 2.3, Section 2.4, Section 3.1-13, Section 3.1-14, and Section 3.1-15. A draft safety evaluation report was issued for this topical report on August 20, 2009.
2. The setpoint methodology for the excore instrumentation system is described in ANP-10275P-A, Revision 0, “U.S. EPR Instrument Setpoint Methodology Topical Report,” Section 5.2, Section 5.3, Section 5.3.4, Section 5.3.7 through Section 5.3.11, and Appendix E.

The setpoint methodology described in Topical Report ANP-10287P, Revision 0 and Topical Report ANP-10275P-A, Revision 0 will be used to develop setpoints associated with the PS for the U.S. EPR.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.07-19:

Follow-up to RAI Question No. 07.07-12

In accordance with 10 CFR 52.47(a), the NRC staff requests that the applicant update the U.S EPR FSAR with Figure 07.07-12-1, "Signal Flow from PS through CU" that was provided in the response to RAI No. 57, Question 07.07-12.

10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components to permit understanding of the system design and its relation to the safety evaluation. The NRC staff reviewed Chapter 7 of the U.S. EPR DC-FSAR, Revision 1, and the U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Technical Report, ANP-10304, Revision 0, and the response to RAI No. 57, Question 07.07-12. The staff found the figure provided in the response to Question 07.07-12 to be adequate, but should be included in the DC-FSAR. Without this type of figure, the RCSL design descriptions are not sufficient to permit understanding of the system designs and their relationship to the safety evaluation(s). The staff requests that the figure associated with Question 07.07-12 be included in the DC-FSAR, or an equivalent figure that contains at a minimum:

3. A properly labeled figure
4. Signal and Logic flow that will show process flow from the PS isolation devices through the Control Rod Drive Control System
5. Input and output signals of the RCSL system and the RCSL system components
6. Properly labeled boundaries of the RCSL system and the RCSL system components
7. RCSL system component functions and processes (i.e., algorithms, signal selection, summation)
8. Description of signal media paths used (i.e., plant data network, internal RCSL signal path, hardwired, fiber)
9. Channel and/or division boundaries

Response to Question 07.07-19:

A response to this question will be provided by December 18, 2009.

Question 07.08-7:

Follow-up to RAI Question No. 07.08-2

Describe the Diverse Actuation System (DAS) on-line self-test features that address the testing and surveillance criteria of Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related." Specifically, identify the self-test features and their coverage of possible failures that might occur with the DAS. Also, identify any other testing that may be applied to the DAS for system testing and surveillance.

10 CFR 50.62 requires, in part, that equipment used to mitigate an Anticipated Transient Without Scram should perform it in a reliable manner. Generic Letter 85-06 and its enclosure titled "QA Guidance for Non-Safety-Related ATWS Equipment", provide guidance on quality and reliability criteria for such systems. The staff acknowledges that DAS self-tests will be used, at least in part, to address the testing criteria for the DAS. However, the staff requests the following information regarding the self tests:

a. Identify the types of self tests and their coverage for potential failures in the DAS.
b. How the DAS online self-test will indicate DAS operational status (i.e., proper and correct operation, failure of DAS functionality).
c. Identification of any other testing outside of the self tests for the DAS.

The staff also request that information used to address this RAI request be inserted within the applicable Chapter 7 FSAR sections.

Response to Question 07.08-7:

A response to this question will be provided by January 22, 2010.

Question 07.08-8:

Follow-up to RAI Question No. 07.08-3

Provide a clear commitment to Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That is Not Safety-Related," and its enclosure in Section 7.8 of the U.S. EPR DC-FSAR.

10 CFR 52.47(a)(2) requires, in part, a description of strucutres, systems, and components. In RAI 07.08-3, the staff requested an information as to whether AREVA NP commits to Generic Letter 85-06 for the Diverse Actuation System. The response pointed to Section 7.1, which in turn pointed to Chapter 17, which in turn pointed to a quality assurance program topical report. For clarity in the DC-FSAR, the staff requests AREVA NP to also make the commitment statement in Chapter 7 as it is the area where compliance against 10 CFR 50.62 is evaluated and the commitment statement is credited for addressing the quality aspects of that particular regulation.

Response to Question 07.08-8:

Because the diverse actuation system (DAS) performs anticipated transient without scram (ATWS) functions, it is designed in accordance with the quality requirements of Generic Letter 85-06. U.S. EPR FSAR Tier 2, Section 7.8 will be revised to include compliance with Generic Letter 85-06.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.8.2 will be revised as described in the response and indicated on the enclosed markup.

Question 07.08-9:

Follow-up to RAI Question No. 07.08-4

Further justify why the Process Information and Control System (PICS) does not need to meet 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 1.

GDC 1 requires, in part, that structures, systems and components important to safety shall be design, fabricated, erected, and tested to quality standards commensurate with the importance of the safety functions to be performed. The staff identified throughout Chapter 7 of the U.S. EPR DC-FSAR that PICS is the system that the operators will normally use to monitor and control plant safety systems during all conditions of plant operation, "including normal operation, anticipated operational occurrences, postulated accidents, and beyond design basis events. Additionally, PICS provides functions that address the requirements of GDC 13 and 19 (e.g., post-accident monitoring), as well as diverse actuation functions provided there is a software common-cause failure. As such, the staff sees that PICS is an important to safety system and is required to meet GDC1. The staff requests that information be provided as to the quality standards that PICS will designed and tested. As one example, if PICS is credited for diverse actuation, AREVA NP should address the applicability of Generic Letter 85-06 and its enclosure as one potential standard/guidance. AREVA NP should also describe compliance to GDC 1 for systems that support PICS and enable its proper operation, such as the plant data network.

Response to Question 07.08-9:

A response to this question will be provided by January 22, 2010.

Question 07.09-46:

Follow-up to RAI Question Nos. 07.09-3, 07.09-5, 07.09-8, 07.09-10, 07.09-12, 07.09-15, 07.09-23, 07.09-25, 07.09-27, 07.09-28, and 07.09-35

Identify all data communication interfaces between safety and non-safety systems, and between redundant safety divisions within the U.S. EPR Instrumentation and Control (I&C) Systems architecture. Demonstrate how these interfaces meet the physical, electrical, communications, and functional independence requirements of 10 CFR 50.55a(h) and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.1 requires redundant portions of the safety system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. In addition, IEEE Std. 603-1991, Clause 5.6.3, and GDC 24 require safety systems to be independent from non-safety systems such that credible failures in and consequential actions by non-safety systems do not prevent the safety system from performing its required functions. Digital Instrumentation and Controls Interim Staff Guidance (ISG) on Highly-Integrated Control Rooms-Communications Issues (HICRc) (ISG #4-HICRc) Section 1, "Interdivisional Communications" provides design criteria for communications independence between redundant divisions of safety systems and between safety and non-safety systems. In addition, NUREG-0800, Standard Review Plan (SRP) Branch Technical Position (BTP) 7-11, "Guidance on Application and Qualification of Isolation Devices," provides design criteria for electrical isolation devices.

The staff reviewed U.S. EPR DC-FSAR, Section 7.1, which describes the I&C systems within the U.S. EPR architecture, and finds that additional clarification is required to verify how interfaces between redundant portions of safety systems and between safety and non-safety systems meet the physical, electrical, communications, and functional independence requirements of IEEE Std. 603-1991, Clause 5.6. Specifically, the staff requests the applicant to 1) provide a table listing all the data communication interfaces between safety divisions and between safety and non-safety systems; 2) describe how physical separation is met in each of the interfaces; 3) describe how electrical isolation is met in accordance with IEEE Std. 384-1981 and BTP 7-11 for each of the interfaces; 4) describe how communications independence is maintained for each of the interfaces by addressing the twenty criteria provided in Section 1 of ISG #4-HICRc; 5) describe how functional independence is maintained by identifying the information transmitted and demonstrating that no failures (i.e. functional misbehavior) by the non-safety system can degrade, or exceed, any safety function within the safety system. In addition, the staff requests the applicant update the FSAR to include the information requested above.

Response to Question 07.09-46:

A response to this question will be provided by January 22, 2010.

Question 07.09-47:

Follow-up to RAI Question Nos. 07.09-6, 07.09-14, and 07.09-18

Demonstrate the estimated response time of the computerized portion of the Protection System (PS) is within the bounding time limits established for the PS within the U.S. EPR DC-FSAR, Table 15.0-7 and Table 15.0-8. In addition, identify the Inspection, Test, Analysis, and Acceptance Criteria (ITAAC) that verifies the protection system meets the response times assumed in the accident analyses.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. IEEE Standard 603-1991, Clause 4.10 requires identification of the critical points in time or plant conditions for which the protective actions must be initiated and the point in time or plant conditions that define the proper completion of the safety function. The critical points in time are determined by the reactor protection system response time modeled in the accident analyses. The protection system should be designed and tested to meet the response times assumed in the accident analyses.

In response to the NRC staff's request for additional information (RAI) 4 for ANP-10281, "U.S. EPR Digital Protection System Report," the applicant stated:

"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 functios 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."

U.S. EPR FSAR Tier 2, Table 15.0-7—Reactor Trip Setpoints and Delays Used in the Accident Analysis and Table 15.0-8—Engineered Safety Features Functions Used in the Accident Analysis list the time delay assumed for each protective function performed by the Protection System (PS). Verify that the estimated response times provided in the Attachment B of the Second Request For Additional Information for the U.S. Digital Protection Topical Report are consistent with the timing delays assumed in U.S. EPR DC-FSAR, Table 15.0-7 and Table 15.0-8. Identify the ITAAC that verifies the as-installed PS response time, from sensor output to final actuation device, is bounded by the PS response time used in the U.S. EPR DC-FSAR, Tables 15.0-7 and 15.0-8 accident analysis. In addition, describe how the time delay of the PACS module is incorporated into the PS response time analysis in ANP-10281P.

Response to Question 07.09-47:

A response to this question will be provided by February 26, 2010.

Question 07.09-49:

Follow-up to RAI Question Nos. 07.09-29, 07.09-34, 07.09-36, and 07.09-37

Demonstrate how operating experience regarding the effects of data storms on non-safety data communication networks will be addressed for the plant data network.

10 CFR 52.47(a)(22) requires applicants for design certifications include information necessary to demonstrate how operating experience insights have been incorporated into the plant design. U.S. EPR FSAR Tier 2, Section 7.1 describes the interconnections of non-safety I&C systems via the plant data network. This section has not addressed the design of the plant data network to preclude the susceptibility of this network to data storms. 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," (ML071510428, dated April 17, 2007), describing operational experience on the effects of a data storm on non-safety control networks.

Response to Question 07.09-49:

A response to this question will be provided by January 22, 2010.

Question 07.09-50:

Follow-up to RAI Question No. 07.09-7

Clarify whether the service unit used to service the SICS is safety related or non-safety related.

U.S. EPR DC-FSAR, Revision 0, Section 7.1.1.3.1 states that the safety-related portion of the SICS consists of service units. Response to RAI 56 Supplement 1, Question 7.9-7 states:

"The three data communication systems (DCS) referred to in this question (severe accident (SA) instrumentation and controls (I&C)-safety information and control system (SICS); GW-plant data network; SU-QDS) are non-safety-related. (Note: The SU is designated as safety-related in the U.S. EPR FSAR. This will be corrected to classify the SU as non-safety-related.) None of these communication paths are relied upon to perform safety-related plant functions."

The applicant proposed to modify the FSAR to correct the classification of the SU as safety-related. The staff reviewed U.S. EPR DC-FSAR, Revision 1, Section 7.1.1.3.1 (pg. 7.1-8) and finds that the service unit is still classified as safety-related.

Response to Question 07.09-50:

U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 will be revised to clarify that service units (SUs) are classified as non-safety-related.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 will be revised as described in the response and indicated on the enclosed markup.

Question 07.09-51:

Clarify the usage of the term “segmentation” in Section 6.1.4.4 of ANP-10281, “U.S. EPR Digital Protection System Topical Report.”

Section 6.1.4.4 of the U.S. EPR Digital Protection System Topical Report uses the word “segmentation” for declaration of failure of a network segment within the PS network architecture. However, this section has not clearly defined “segmentation” in this context. Typically, segmentation is used to segregate networks, packets, or memory, and not used for declaration of inoperability. The staff requests the applicant revise Section 6.1.4.4 of the U.S. EPR Digital Protection System Topical Report to clearly define “segmentation” in the context of the U.S. EPR digital protection system architecture.

Response to Question 07.09-51:

The term “operability” is used in the U.S. EPR FSAR Tier 2, Chapter 16 Technical Specifications and has a very specific meaning. Inoperability of a component is declared by an operator, not automatically by a function of the protection system (PS). System, device, and component operability is defined and described in U.S. EPR FSAR Tier 2, Chapter 16, Section 1.1.

The term “segmentation” in Topical Report ANP-10281 is not used for declaration of inoperability of a network segment within the PS network architecture. Topical Report ANP-10281, Section 6.1.4.4 provides an accurate definition of the segmentation function. The segmentation function in the optical link module (OLM) is provided to enhance system reliability, not to declare inoperability. Additionally, no credit is taken for the segmentation functionality in the PS failure modes and effects analysis (FMEA).

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.09-52:

Follow-up to RAI Question Nos. 07.09-29 and 07.09-30

Demonstrate that plant data network is of sufficient quality and capacity to support PICS functions to meet the control room capabilities required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 19, and the D3 requirements to meet Staff Requirements Memorandum (SRM) for SECY-93-87.

GDC 19, “Control Room,” requires a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Additionally, the SRM for SECY-093-87 provides the four point position on Diversity and Defense in Depth (D3) for ALWRs. Point 4 requires a set of displays and controls located in the main control room to be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems.

U.S. EPR DC-FSAR, Section 7.1.1.3.2, describes the capabilities of the Process Information and Control System (PICS) with regards to the capability for safe operation of the plant from the main control room during normal and accident conditions. In addition, the PICS is credited to meet Point 4 of the D3 requirements specified in the SRM for SECY-093-87. The capabilities of the PICS to achieve both hot and cold shut down conditions from the remote shutdown system are described in Section 7.1.1.3.2. Equipment such as network switches and electrical and fiber optic cables are provided (as part of the plant data network) to support the required data communications between the PICS and other instrumentation and control systems. Provide an ITAAC that verifies the plant data network is of sufficient quality and capacity to support PICS functions.

Response to Question 07.09-52:

A response to this question will be provided by January 22, 2010.

Question 07.09-53:

Follow-up to RAI Question No. 07.09-30

Identify the Inspection, Test, Analysis, and Acceptance Criteria (ITAAC) that verifies the PICS is designed and built to quality standards commensurate with control room functions this system performs, as required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 19, and the D3 requirements to meet Staff Requirements Memorandum (SRM) for SECY-93-87.

GDC 19, "Control Room," requires a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Additionally, the SRM for SECY-093-87 provides the four point position on Diversity and Defense in Depth (D3) for ALWRs. Point 4 requires a set of displays and controls located in the main control room to be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems.

In response to Request for Additional Information (RAI) 56, Question 07.09-30, the applicant stated:

"Even though the PICS is classified as a non-safety-related system and is not required to meet the standards of safety-classified class 1E systems, the PICS is designed to high quality standards and will employ redundancy to provide fault tolerance. The PICS design will be implemented with equipment, such as network switches and electrical and fiber optic cables, that is typical of modern digital distributed control systems used for power plant control. To provide sufficient quality, industrial standards for electromagnetic interference (EMI) and radio frequency interferences (RFI) will be included on this equipment.

Additionally, the PICS will be implemented with physical and functional redundancy of components. In the event of a single component failure, sufficient redundancy will still exist to permit a redistribution of the working area and tasks to continue utilization of the PICS to control and monitor the plant. Physical separation of redundant components into different rooms and different fire zones provides independence of redundant structures of PICS."

Provide the ITAAC that verifies the PICS is designed to quality standards and will employ redundancy to provide fault tolerance.

Response to Question 07.09-53:

A response to this question will be provided by December 18, 2009.

Question 07.09-54:

Follow-up to RAI Question No. 07.09-11

Confirm that the data communications between CUs are point-to-point as stated in the response for Request for Additional Information (RAI) 56, Question 7.09-11.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.1, requires the 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 safety functions. In RAI 56, Question 7.09-11, the staff requested the applicant to demonstrate how the data communications components and interconnecting cables between divisions of the SAS meet the single failure criterion defined in IEEE Std. 603-1991, Clause 5.1. In response, the applicant stated:

> "As described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.2,"Data Communications," the control unit (CU)-CU networks are point-to-point between divisions, and separate networks are provided for the A and B redundancies. This results in six individual point-to-point connections for redundancy A."

The staff reviewed Figure 7.1-7, "Safety Automation System Architecture," and found 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 1) confirm that the response provided is accurate, 2) incorporate the response into the FSAR, and 3) modify Figure 7.1-7 to be consistent.

Response to Question 07.09-54:

The safety automation system (SAS) CU-CU networks are point-to-point, consistent with U.S. EPR FSAR Tier 2, Figure 7.1-7.

U.S. EPR FSAR Tier 2, Figure 7.1-1—Symbol Legend defines the symbology used to represent the SAS networks (see Figure 07.09-54-1). The definition in U.S EPR FSAR Tier 2, Figure 7.1-1 indicates that this symbol is a functional data connection that does not imply a specific network topology and that the text description of the system identifies the specific network implementation used for that system.

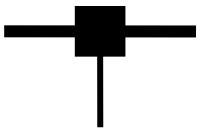
This symbolic representation is used throughout U.S. EPR FSAR Tier 2, Section 7.1. For example, U.S. EPR FSAR Tier 2, Figure 7.1-6—Protection System Architecture uses the "functional data connection" symbol to represent both point-to-point and redundant ring topology networks.

See U.S. EPR FSAR Tier 2, Section 7.1 for more detailed information.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Figure 07.09-54-1—Symbol Legend

	Functional data connection. May be implemented with point-to-point or networked data connections. Refer to text description for the specific implementation.

Question 07.09-55:

Follow-up to RAI Question No. 07.09-21

Incorporate the response in Request for Additional Information (RAI) 56, Question 07.09-21 regarding the PS compliance with GDC 4 into the U.S. EPR Final Safety Analysis Report (FSAR).

In response to RAI 56, Question 07.09-21, the applicant stated:

> "U.S. EPR FSAR Tier 2, Section 7.1.2.2.3 addresses PS compliance with GDC 4. The cables used to interconnect functional units within the PS are considered part of the PS. Data communication cables will be routed throughout the plant and may be placed in the same raceway as low-level analog cables. When possible, routing of communication cables is limited to non-hazard and limited-hazard areas. If any safety-related communication cables are routed through a hazard area, acceptable means of physical protection will be provided. When passing through another divisional building, IEEE Class 1E communication cables will be in a fire protected enclosure to prevent a fire in one division from damaging communication cables of another division. Damage to fiber optic communication cables will not result in spurious actuations of equipment, but may result in loss of component function. However, divisional redundancy allows supported safety functions to be maintained.
>
> The data communication modules (e.g., communication processors, optical link modules) that are part of the PS are located within the PS cabinets. These cabinets are located in mild environment areas within the four Safeguard Buildings (SBs)."

The staff requests the applicant incorporate this response into the U.S. EPR FSAR.

Response to Question 07.09-55:

The Response to RAI 56, Supplement 3, Question 07.09-21 is described in detail in U.S. EPR FSAR Tier 2, Section 8.3.1.1.9.

U.S. EPR FSAR Tier 2, Section 7.1.1.4.1 will be revised to include the following:

> "The data communication modules (e.g., communication processors, optical link modules) that are part of the PS are located within the PS cabinets. These cabinets are located in mild environment areas within the four Safeguard Buildings (SBs). The cables used to interconnect functional units within the PS are considered part of the PS. Cabling independence and separation are described in Section 8.3.1.1.9."

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.1.1.4.1 will be revised as described in the response and indicated on the enclosed markup.

Question 07.09-56:

Follow-up to RAI Question No. 07.09-38

Clarify whether the non-safety related MSI within the RCSL is connected to the safety-related MSI within the SAS.

10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components to permit an understanding of the system design and its relation to the safety evaluation. U.S. EPR DC-FSAR, Figure 7.1-7 and Figure 7.1-10 depict connections (e.g. M1-G1, M1-G2) from the safety-related MSI of the SAS to the non-safety related MSI of the RCSL. In addition, the non-safety related MSI of the RCSL is depicted as connected to the GW (e.g. GW1 via M1-G1) through the same connection as the one used for the safety-related MSI. Verify this depiction is accurate. In addition, describe why the non-safety related MSI needs to be connected to the safety related MSI from the SAS. Incorporate this information into the U.S. EPR DC-FSAR.

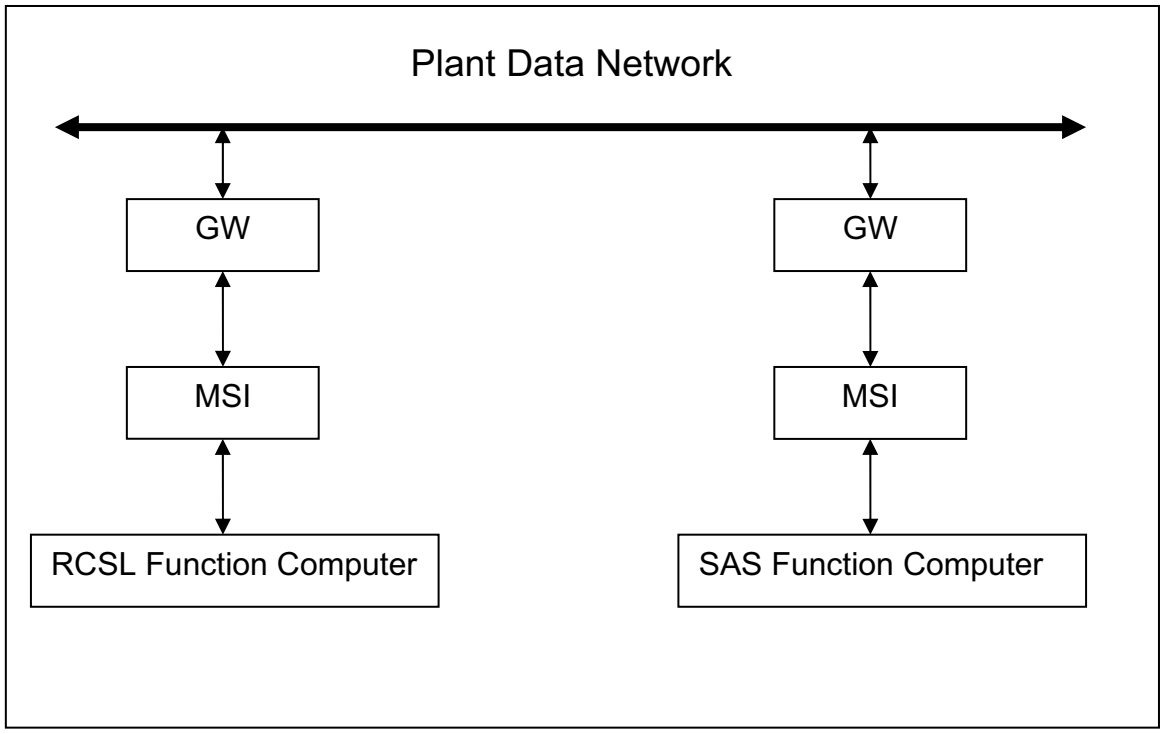
Response to Question 07.09-56:

The gateways (GW) shown in U.S. EPR FSAR Tier 2, Figure 7.1-7 are physically different computers than the GWs shown in U.S. EPR FSAR Tier 2, Figure 7.1-10 (i.e., each Teleperm XS (TXS)-based system has its own GWs). The GWs are provided to interface the TXS system to the plant data network. There is not a connection between the reactor control, surveillance, and limitation (RCSL) monitoring service interface (MSI) and the safety automation system (SAS) MSI. Figure 07.09-56-1 illustrates this concept.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Figure 07.09-56-1—Example of the MSIs and GW connection to the Plant Data Network



Question 07.09-57:

Follow-up to RAI Question No. RAI 07.09-44

Verify that the overspeed control of the Turbine Generator Instrumentation and Control System does not use the plant data network.

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. This section states that the data communications systems (DCS) should have sufficient excess capacity margins to accommodate likely future increases in DCS or software or hardware changes to equipment attached to the DCS. U.S. EPR DC-FSAR, Figure 7.1-12, “Process Automation System Architecture (Turbine Island and Balance of Plant Subsystem,” depicts the Control Units of the Turbine Island and Balance of Plant Subsystems are connected to the plant data network. Clarify whether the turbine overspeed control within the Turbine Instrumentation and Controls subsystem requires input from the plant data network, and if so, describe how diversity of the turbine overspeed trip devices is accomplished.

Response to Question 07.09-57:

A response to this question will be provided by December 18, 2009.

Question 07.09-58:

Follow-up to RAI Question No. 07.09-33

Incorporate the response in Request for Additional Information (RAI) 56, Question 07.09-33 regarding additional data connections that may be implemented in the Process Automation System (PAS) into the U.S. EPR DC-FSAR.

In response to RAI 56, Question 07.09-33, the applicant stated:

> "U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 specifies point-to-point data communications between divisions, within two PAS subsystems (nuclear island subsystem (NIS) and diverse actuation system (DAS)). Other types of data communications may be implemented within the same division in the NIS and DAS. Additionally, the turbine island subsystem (TIS) and balance of plant subsystem (BPS) are not divisionalized in the same way as the NIS and DAS. Other types of data communications may be implemented within the TIS and BPS."

The staff requests the applicant incorporate this response into the U.S. EPR FSAR.

Response to Question 07.09-58:

U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 will be revised to incorporate the Response to RAI 56, Supplement 1, Question 07.09-33.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.1.1.4.6 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

- Monitoring and control of essential non-safety-related systems to achieve and maintain hot-standby on a loss of PICS (MCR).
- Monitoring and control of systems to mitigate severe accidents (MCR).
- Backup safety parameter display system (SPDS) functions (MCR).
- Display high priority alarms (MCR).

Architecture

The SICS consists of a safety-related portion and a non-safety-related portion to perform its functions.

Safety-Related Portion of SICS

Figure 7.1-3—Safety Information and Control System Architecture (Safety-Related Portion) provides a functional representation of the safety-related portion of the SICS.

The safety-related portion of the SICS is organized into four independent divisions located in separate Safeguards Buildings. HMI equipment is located in the MCR and RSS, and is physically separated.

The safety-related portion of the SICS consists of these functional units:

- Panel interfaces (PI)
- Qualified display systems (QDS).
- ~~Service units (SU).~~ ← 07.09-50

PIs perform data processing functions and are provided to interface between the various Level 1 systems and the HMI devices in the MCR or RSS. Control PIs process manual commands initiated from the HMI devices and information related to actuator status for display. Monitoring PIs only transfer information to the HMI devices for display to the operator. Hardwired connections to non-safety-related I&C systems may be used as required by the SICS human factors design and are isolated as described in Section 7.1.1.6.4.

Control QDSs provide the capability to initiate manual commands and display actuator-related information. Monitoring QDSs only provide information to the operator. The number and physical arrangement of QDSs provided in the MCR and RSS are determined based on functional and human factors requirements.

Hardwired I&C is used to provide information to the operator and provide the ability to actuate and control plant equipment. Hardwired I&C is connected to the PIs, various Level 1 I&C systems, and the reactor trip devices.

The PS is organized into four redundant, independent divisions located in separate Safeguards Buildings. Each division contains two functionally independent subsystems (A and B). These subsystems are used to implement functional diversity for reactor trip functions.

The PS consists of these functional units:

- Remote Acquisition Units (RAU).
- Rod Control Cluster Assembly Units (RCCAU).
- Acquisition and Processing Units (APU).
- Actuation Logic Units (ALU).
- MSIs.
- GWs.
- SUs.

Details on these functional units, along with details of the PS architecture, are described in Digital Protection System Topical Report (ANP-10281) (Reference 6).

Equipment

The PS is implemented with the TXS digital I&C platform.

The RAUs, RCCAUs, APUs, ALUs, and MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable are used for the various data and hardwired connections.

07.09-55

The data communication modules (e.g., communication modules, optical link modules) that are part of the PS are located within the PS cabinets. These cabinets are located in mild environment areas within the four Safeguard Buildings. The cables used to interconnect functional units within the PS are considered part of the PS. Cabling independence and separation are described in Section 8.3.1.1.9.

Qualification Requirements

The equipment used in the PS is qualified for environmental, seismic, electromagnetic interference, and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

– System Validation Phase.

- A criticality analysis is performed for the DAS software in accordance with accepted industrial practice.
- Verification and validation (V&V) of the DAS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- DAS system requirements are documented in a traceable form that is under configuration management, providing traceability of every software requirement to one or more system requirements.
- The DAS system design is validated through acceptance test in the System Validation (or equivalent) phase.

Diversity Requirements

The PAS is credited by the defense-in-depth and diversity analysis described in Section 7.8.2. These diversity requirements apply to the PAS equipment:

- The system hardware in the PAS is diverse from the TXS system hardware.
- The system software in the PAS is diverse from the TXS system software.
- Application software for PAS shall be developed by different personnel than those who develop application software for the TXS systems.
- Application software for PAS shall be developed using a different design tool than that used to develop application software for the TXS systems.
- Application software for PAS shall be tested using a different testing tool than those used for testing application software for the TXS systems.

Data Communications

The functional units in the PAS interface to the PICS via the plant data network.

The NIS implements point-to-point data connections between the CUs in each division to share signals to implement signal selection algorithms.

The DAS implements point-to-point data connections between the DAUs for voting purposes.

07.09-58

Other types of data connections may be implemented within the same division of the NIS and the DAS.~~Other data connections may be implemented as required.~~

The TIS and BPS are not divisionalized. Other types of data connections may be implemented within the TIS and BPS.

7.8.2.1.8 Generic Letter 85-06 - Quality Assurance Guidance for ATWS Equipment that is not Safety Related

07.08-8

AREVA NP Inc. implements quality requirements to ATWS equipment in accordance with Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is not Safety Related."

7.8.2.2 Evaluation of NUREG/CR-6303 Guidelines

7.8.2.2.1 Identifying System Blocks (Guidelines 1 and 5)

The blocks are identified at the system level within the I&C architecture described in Section 7.1. Within the PS, subsystems A and B provide for functional diversity.

7.8.2.2.2 Determining Degree of Diversity (Guideline 2)

The PICS and PAS are implemented with digital I&C equipment that is diverse from the TXS platform. The PACS is implemented using non-computerized technology that is diverse from the TXS digital platform. The hardwired portions of the SICS are diverse from TXS. The equipment for the PICS, PAS, PACS and SICS is described in Section 7.1.

7.8.2.2.3 System Failure Types (Guideline 3)

Type 1 Failures

Type 1 failures are caused by a failure of the I&C that induces a plant transient requiring a protective action.

These failures are mitigated in the U.S. EPR I&C design through the use of signal selection algorithms in control systems, and redundancy, fault detection and voting in the PS.

Chapter 15 identifies control system malfunctions that result in initiating events. The DAS is provided as a diverse means of actuating RT and ESF to mitigate these events concurrent with a CCF of the PS.

Type 2 Failures

Type 2 failures are undetected failures that prevent the safety I&C systems from executing safety functions, when required.

These failures are mitigated in the U.S. EPR design through two primary methods. Functional diversity within the PS is provided to mitigate an error due to a requirement specification. Equipment diversity is provided so that the PICS, PAS, PACS and hardwired portions of the SICS are not affected by a CCF of the TXS platform.

2. NUREG/CR-6303, “Method for Performing Diversity and Defense-in-Depth Analysis of Reactor Protection Systems,” U.S. Nuclear Regulatory Commission, December 1994.

3. SECY-93-087, “Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs,” U.S. Nuclear Regulatory Commission, April 1993.

07.08-8

4. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related," U.S. Nuclear Regulatory Commission, April 16, 1986.

Next File