

## ArevaEPRDCPEm Resource

---

**From:** Pederson Ronda M (AREVA NP INC) [Ronda.Pederson@areva.com]  
**Sent:** Wednesday, January 14, 2009 1:26 PM  
**To:** Getachew Tesfaye  
**Cc:** PANNELL George L (AREVA NP INC); DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 56, Supplement 1  
**Attachments:** RAI 56 Supplement 1 Response US EPR DC.pdf

Getachew,

The attached file, "RAI 56 Supplement 1 Response US EPR DC.pdf," provides technically correct and complete responses to 14 of the 45 questions, as committed.

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 56 Question 07.09-7.

The following table indicates the respective page(s) in the response document, "RAI 56 Supplement 1 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

<b>Question #</b>	<b>Start Page</b>	<b>End Page</b>
RAI 56 - 07.09-1	2	3
RAI 56 - 07.09-5	4	4
RAI 56 - 07.09-7	5	7
RAI 56 - 07.09-11	7	8
RAI 56 - 07.09-12	9	9
RAI 56 - 07.09-17	10	13
RAI 56 - 07.09-19	14	14
RAI 56 - 07.09-25	15	16
RAI 56 - 07.09-28	17	18
RAI 56 - 07.09-30	19	19
RAI 56 - 07.09-32	20	20
RAI 56 - 07.09-33	21	22
RAI 56 - 07.09-35	23	23
RAI 56 - 07.09-45	24	24

The schedule for technically correct and complete responses to the remaining 31 questions is unchanged and provided below:

<b>Question #</b>	<b>Response Date</b>
RAI 56 - 07.09-2	March 31, 2009
RAI 56 - 07.09-3	March 31, 2009
RAI 56 - 07.09-4	March 31, 2009
RAI 56 - 07.09-6	March 31, 2009
RAI 56 - 07.09-8	March 3, 2009
RAI 56 - 07.09-9	March 31, 2009
RAI 56 - 07.09-10	March 31, 2009
RAI 56 - 07.09-13	March 3, 2009
RAI 56 - 07.09-14	March 31, 2009
RAI 56 - 07.09-15	March 3, 2009
RAI 56 - 07.09-16	March 3, 2009

RAI 56 - 07.09-18	March 3, 2009
RAI 56 - 07.09-20	March 3, 2009
RAI 56 - 07.09-21	March 3, 2009
RAI 56 - 07.09-22	March 3, 2009
RAI 56 - 07.09-23	March 31, 2009
RAI 56 - 07.09-24	March 3, 2009
RAI 56 - 07.09-26	March 31, 2009
RAI 56 - 07.09-27	March 31, 2009
RAI 56 - 07.09-29	March 3, 2009
RAI 56 - 07.09-31	March 31, 2009
RAI 56 - 07.09-34	March 3, 2009
RAI 56 - 07.09-36	March 3, 2009
RAI 56 - 07.09-37	March 3, 2009
RAI 56 - 07.09-38	March 3, 2009
RAI 56 - 07.09-39	March 31, 2009
RAI 56 - 07.09-40	March 31, 2009
RAI 56 - 07.09-41	March 31, 2009
RAI 56 - 07.09-42	March 31, 2009
RAI 56 - 07.09-43	March 31, 2009
RAI 56 - 07.09-44	March 3, 2009

Sincerely,

*Ronda Pederson*

[ronda.pederson@areva.com](mailto: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:** Pederson Ronda M (AREVA NP INC)

**Sent:** Wednesday, November 26, 2008 3:18 PM

**To:** 'Getachew Tesfaye'

**Cc:** PANNELL George L (AREVA NP INC); DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC)

**Subject:** Response to U.S. EPR Design Certification Application RAI No. 56, FSAR Ch 7, Revised Schedule

Getachew,

On October 10, 2008, AREVA NP provided a schedule for responding to the 45 questions in NRC's RAI No. 56. On October 22, 2008, a public meeting was held between AREVA NP Inc. and the NRC to discuss the U.S. EPR FSAR Chapter 7 and RAI No.'s 56 through 61.

A revised schedule for a technically correct and complete response to each of the 45 questions of RAI No. 56 is provided below.

Question #	Response Date
RAI 56 - 07.09-1	January 15, 2009

RAI 56 - 07.09-2	March 31, 2009
RAI 56 - 07.09-3	March 31, 2009
RAI 56 - 07.09-4	March 31, 2009
RAI 56 - 07.09-5	January 15, 2009
RAI 56 - 07.09-6	March 31, 2009
RAI 56 - 07.09-7	January 15, 2009
RAI 56 - 07.09-8	March 3, 2009
RAI 56 - 07.09-9	March 31, 2009
RAI 56 - 07.09-10	March 31, 2009
RAI 56 - 07.09-11	January 15, 2009
RAI 56 - 07.09-12	January 15, 2009
RAI 56 - 07.09-13	March 3, 2009
RAI 56 - 07.09-14	March 31, 2009
RAI 56 - 07.09-15	March 3, 2009
RAI 56 - 07.09-16	March 3, 2009
RAI 56 - 07.09-17	January 15, 2009
RAI 56 - 07.09-18	March 3, 2009
RAI 56 - 07.09-19	January 15, 2009
RAI 56 - 07.09-20	March 3, 2009
RAI 56 - 07.09-21	March 3, 2009
RAI 56 - 07.09-22	March 3, 2009
RAI 56 - 07.09-23	March 31, 2009
RAI 56 - 07.09-24	March 3, 2009
RAI 56 - 07.09-25	January 15, 2009
RAI 56 - 07.09-26	March 31, 2009
RAI 56 - 07.09-27	March 31, 2009
RAI 56 - 07.09-28	January 15, 2009
RAI 56 - 07.09-29	March 3, 2009
RAI 56 - 07.09-30	January 15, 2009
RAI 56 - 07.09-31	March 31, 2009
RAI 56 - 07.09-32	January 15, 2009
RAI 56 - 07.09-33	January 15, 2009
RAI 56 - 07.09-34	March 3, 2009
RAI 56 - 07.09-35	January 15, 2009
RAI 56 - 07.09-36	March 3, 2009
RAI 56 - 07.09-37	March 3, 2009
RAI 56 - 07.09-38	March 3, 2009
RAI 56 - 07.09-39	March 31, 2009
RAI 56 - 07.09-40	March 31, 2009
RAI 56 - 07.09-41	March 31, 2009
RAI 56 - 07.09-42	March 31, 2009
RAI 56 - 07.09-43	March 31, 2009
RAI 56 - 07.09-44	March 3, 2009
RAI 56 - 07.09-45	January 15, 2009

Sincerely,

*Ronda Pederson*

[ronda.pederson@areva.com](mailto:ronda.pederson@areva.com)

Licensing Manager, U.S. EPR(TM) 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:** Pederson Ronda M (AREVA NP INC)

**Sent:** Friday, October 10, 2008 6:50 PM

**To:** 'Getachew Tesfaye'

**Cc:** DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); PANNELL George L (AREVA NP INC); DUNCAN Leslie E (AREVA NP INC); WELLS Russell D (AREVA NP INC)

**Subject:** Response to U.S. EPR Design Certification Application RAI No. 56 (942), FSAR Ch7

Getachew,

The attached file, "RAI 56 Response US EPR DC.pdf" provides an interim response to each of the 45 questions.

A complete answer is not provided for 45 of the 45 questions.

A complete response to each of the questions will be provided by December 1, 2008.

Sincerely,

*Ronda Pederson*

[ronda.pederson@areva.com](mailto:ronda.pederson@areva.com)

Licensing Manager, U.S. EPR Design Certification  
New Plants Deployment

**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:** Getachew Tesfaye [mailto:Getachew.Tesfaye@nrc.gov]

**Sent:** Friday, September 12, 2008 5:44 PM

**To:** ZZ-DL-A-USEPR-DL

**Cc:** Deanna Zhang; Terry Jackson; Michael Canova; Joseph Colaccino; John Rycyna; Mario Gareri

**Subject:** U.S. EPR Design Certification Application RAI No. 56 (942), FSAR Ch7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 26, 2008, and on September 5, 2008, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. 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:** 115

**Mail Envelope Properties** (5CEC4184E98FFE49A383961FAD402D3197A938)

**Subject:** Response to U.S. EPR Design Certification Application RAI No. 56, Supplement 1  
**Sent Date:** 1/14/2009 1:25:45 PM  
**Received Date:** 1/14/2009 1:25:52 PM  
**From:** Pederson Ronda M (AREVA NP INC)

**Created By:** Ronda.Pederson@areva.com

**Recipients:**

"PANNELL George L (AREVA NP INC)" <George.Pannell@areva.com>

Tracking Status: None

"DELANO Karen V (AREVA NP INC)" <Karen.Delano@areva.com>

Tracking Status: None

"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>

Tracking Status: None

"Getachew Tesfaye" <Getachew.Tesfaye@nrc.gov>

Tracking Status: None

**Post Office:** AUSLYNCMX02.adom.ad.corp

<b>Files</b>	<b>Size</b>	<b>Date &amp; Time</b>
MESSAGE	7732	1/14/2009 1:25:52 PM
RAI 56 Supplement 1 Response US EPR DC.pdf		99745

**Options**

**Priority:** Standard

**Return Notification:** No

**Reply Requested:** No

**Sensitivity:** Normal

**Expiration Date:**

**Recipients Received:**

**Response to**

**Request for Additional Information No. 56, Supplement 1**

**9/12/2008**

**U. S. EPR Standard Design Certification**

**AREVA NP Inc.**

**Docket No. 52-020**

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

**Application Section: Section 7.1**

**ICE1 Branch**

**Question 07.09-1:**

Demonstrate how the optical link modules used for communications between redundant portions of the safety instrumentation and control systems are designed to meet IEEE Std. 603-1991, Clause 5.6.1, requirements.

Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System, [Adams Accession No. ML003732662] states that the communication protocols used for sending messages are not acknowledged by the receiver. Thus, the subrack receiving the message cannot influence the operation of the sending subrack. However, in Topical Report ANP-10281P, "U.S. EPR Digital Protection System Topical Report," the applicant states that echo and segmentation will be used to acknowledge the success of the message transfer at each communication path by the Optical Link Module (OLM). The OLM is the electrical/optical converter that also forwards received messages in one port to all other connected ports. The echo and segmentation function is completed by sending a copy of the original message as an echo back to the sending OLM to acknowledge the receipt of the message. This topical report is currently under review by the NRC and has yet to be approved. Clause 5.6.1 of IEEE Std. 603-1991 requires redundant portions of a safety system provided for a safety function be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. Demonstrate how TELEPERM XS communications principles are maintained in this case to meet IEEE Std. 603-1991, Clause 5.6.1, requirements for independence between redundant portions of safety systems. Specifically, describe where the echo functions terminate (i.e. at the OLM, or at the communications processor of the sending node).

**Response to Question 07.09-1:**

The Teleperm XS (TXS) function and communications processors are not involved in echo functionality. The receiving processors do not provide any acknowledgement of received messages, and the sending processors do not expect an acknowledgement.

The echo functions terminate at the OLM as described in the following ANP-10281P sections:

ANP-10281P, Section 6.1.3, "Network Topologies – Independence of PS Divisions" states:

"Communication independence is not a function of the network topology or the operation of the OLMs. Communication independence is achieved, regardless of the physical topology of the network, through the features designed into the TXS platform for interference-free communication."

ANP-10281P, Section 6.1.4, "Network Operation Concepts" states:

"The echo and segmentation functions are performed by the OLM independently of the operation and communication monitoring functions of any PS units."

ANP-10281P, Section 6.1.4.1, "Send Echo" states:

"The echo is terminated when received by the OLM and is not allowed to propagate to the connected PS function computers."

TXS product documentation that describes the operation of the OLMs, including echo functionality, was provided for NRC staff audit on October 8, 2008.

**FSAR Impact:**

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

**Question 07.09-5:**

Demonstrate how data communications systems within the SICS meet IEEE Std. 603-1991, Clause 5.1, "Single Failure Requirements."

The DC FSAR, Tier 2, Section 7.1.1.3.1 provides a summary of the data communications within the safety portion of the SICS, including the interconnections to other I&C systems and components. This summary does not indicate whether there is redundancy built within these connections (i.e. cables) to meet IEEE Std. 603-1991, Clause 5.1. 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 the safety functions. Provide additional information to demonstrate how the data communications links within the SICS and from the SICS to other I&C systems and components meet the requirements of Clause 5.1.

**Response to Question 07.09-5:**

Refer to U.S. EPR FSAR Tier 2, Figure 7.1-3—Safety Information and Control System Architecture (Safety-Related Portion) for the safety-related communication connections within the safety information and control system (SICS).

As shown on Figure 7.1-3, there are no redundant network connections within the divisions. Each qualified display system (QDS) is directly connected to a panel interface (PI). IEEE Std. 603-1991, Clause 5.1 requires demonstration of single failure tolerance for the functions of the system, not for the individual connections. The use of a four channel redundant design that aligns with the mechanical system redundancy provides protection for a single failure because the single failure does not prevent the system from performing its safety functions. The remaining three divisions are able to perform the safety functions of the system.

The data communication paths between divisions within the SICS for the monitoring QDS (see U.S. EPR FSAR Tier 2, Figure 7.1-3) are via PI-PI connections, which are discussed in U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 and Section 7.1.1.6.4. These sections describe the independence of the connections that support the single failure tolerance of the system.

**FSAR Impact:**

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

**Question 07.09-7:**

Address the acceptance criteria of NUREG-0800, the Standard Review Plan (SRP), Section 7.9, "Data Communications Systems."

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 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. SRP, Section 7.9, "Data Communications Systems," provides the performance design considerations. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems. The real-time performance should be reviewed with SRP Branch Technical Position 7-21.

Section 7.1.1.3.1 of the U.S. EPR DC-FSAR states that the communication between the service unit (SU) and the qualified display system (QDS) uses bi-directional, networked data connections; communication between the gateway (GW) and Plant Data Network also uses bi-directional, networked data connections. Provide additional information regarding the protocol used in the communication between the SA I&C and the SICS, between the SU and QDS, and between the GW and the Plant Data Network. Demonstrate that the real-time performance of these communications have been considered in the design.

**Response to Question 07.09-7:**

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.

As defined in SRP 7.0-A, Section C.3.B and SRP Figure 7.0-A-1, non-safety-related control systems and non-safety-related data communications systems should receive:

“...a limited review as necessary to confirm that control system failures cannot have an adverse effect on safety system functions and will not pose frequent challenges to the safety systems. An area of special emphasis for control systems is to assure that the control system design is consistent with the commitments for control system/safety system independence. Isolation of safety systems from control system failures should be addressed.”

The U.S. EPR does not rely on specific protocol or real-time performance characteristics of the non-safety-related communications to achieve independence of the safety systems from non-safety systems or from the effects of non-safety system failures.

U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 describes the QDS-SU (safety to non-safety) connection and the isolation measures taken for protecting the safety functions.

Branch Technical Position (BTP) 7-21 real-time performance requirements are a result of safety-related considerations, such as setpoint calculations and protection system (PS) response times, which are not impacted by the non-safety-related DCS described in this question.

RAI 57, Response to Question 07.07-13 describes non-safety system failures considered in U.S. EPR FSAR Tier 2, Chapter 15 plant safety analyses.

RAI 57, Response to Question 07.07-17 describes how the functional descriptions in U.S. EPR FSAR Tier 2, Section 7.7 and the system descriptions in U.S. EPR FSAR Tier 2, Section 7.1 support a reasonable assurance finding for GDC 13 concerning non-safety control systems that DCS supports.

The four SRP 7.9 acceptance criteria applicable to DCS are:

- 10 CFR 50.55a(a)(1), "Quality Standards for Systems Important to Safety."
- 10 CFR 50.55a(h), "Protection and Safety Systems" (IEEE Std 603-1991, Clause 5.6.3, independence Between Safety Systems and Other Systems).
- GDC 1, "Quality Standards and Records."
- GDC 24, "Separation of Protection and Control Systems."

U.S. EPR FSAR Tier 2, Section 7.1.2.1 addresses U.S. EPR compliance with these four SRP 7.9 acceptance criteria.

U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 will be revised to correct the designation of the SU as non-safety-related. The SU-QDS communication description will also be moved to the non-safety data communication section.

**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 07.09-11:**

Demonstrate how data communications systems within the SAS meet IEEE Std. 603-1991, Clause 5.1, "Single Failure Criterion."

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 the safety functions.

DC FSAR, Tier 2, Section 7.1.1.4.2, provides a summary of the design of the SAS, including the data communications within the SAS. This section states that the SAS consists of four divisions located in four separate safeguards buildings to provide redundancy in case of single failures of one division. A description of the data communications interfaces between the components within the SAS and other systems and components is provided in this section. This section states that copper and fiber optic cable is used for the various data and hardwired connections. This section does not indicate whether there is redundancy built within the data communications components and interconnecting cables to meet IEEE Std. 603-1991, Clause 5.1. Provide additional information to demonstrate how the data communications components and interconnecting cables within the SAS meet the requirements of Clause 5.1. In addition, for each of the communications interfaces described in this section, state whether data communications is achieved through fiber-optic cabling or copper cabling.

**Response to Question 07.09-11:**

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:

- Division 1 CU(A) to Division 2 CU(A).
- Division 1 CU(A) to Division 3 CU(A).
- Division 1 CU(A) to Division 4 CU(A).
- Division 2 CU(A) to Division 3 CU(A).
- Division 2 CU(A) to Division 4 CU(A).
- Division 3 CU(A) to Division 4 CU(A).

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 signal selection algorithms described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.2 accommodate and disposition the missing signal from the failed connection.

Additionally, the CU(B)s will not be affected by the single failure. The B redundancy of the safety automation system (SAS) will still operate with communications between all four divisions.

The following networks described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.2 use fiber optical cabling:

- CU–CU.
- CU–monitoring service interface (MSI).
- SAS–safety information and control system (SICS) (both control and monitoring).

The other networks described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.2 may use either fiber optical cabling or copper cabling, depending on the technology available.

**FSAR Impact:**

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

**Question 07.09-12:**

Demonstrate how the interface between the Monitoring and Service Interface (MSI) and the Service Unit (SU) meets IEEE Std. 603-1991, Clause 5.6.1.

IEEE Std. 603-1991, Clause 5.6.1, requires redundant portions of a safety system provided for a safety function to be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function.

DC FSAR, Tier 2, Section 7.1.1.4.2, states that the communications between the MSI and the SU uses non-safety-related, inter-divisional, bi-directional, point to point data connections implemented with the TXS Ethernet protocol. This network is provided for the servicing of the SAS. The staff finds that additional information is required to understand how this communication is inter-divisional. If there is interdivisional communication involved, what measures are taken to meet IEEE Std. 603-1991, Clause 5.6.1, for the proposed communication?

**Response to Question 07.09-12:**

The use of the term “interdivisional” regarding the SU–MSI interface is based on the definition found in DI&C-ISG-04, “Task Working Group #4: Highly-Integrated Control Rooms – Communications Issues.” ISG-04 defines interdivisional communications as “communications among different safety divisions or between a safety division and a non-safety entity”. The SU is a non-safety-related entity, and each MSI is part of a safety division.

Because the interface is between non-safety and safety, and not between safety divisions, IEEE 603, Clause 5.6.1 is not applicable. Instead, the SU interface to SAS satisfies IEEE 603, Clause 5.6.3.

Topical Report ANP-10281P, "U.S. EPR Digital Protection System," Section 13.2 describes how independence is achieved for the Teleperm XS (TXS) SU maintenance interface.

The TXS SU maintenance interface was reviewed and approved in the SER for Siemens Topical Report EMF 2110-NP, “TELEPERM XS: A Digital Reactor Protection System.”

**FSAR Impact:**

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

**Question 07.09-17:**

Demonstrate how the communications within the protection system meets IEEE Std. 603-1991, Clause 5.6.1, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 22 requirements. In addition, provide information to describe the failure modes of the data communications systems used to support protection system functions, as required by GDC 23.

IEEE Std. 603-1991, Clause 5.6.1, requires redundant portions of a safety system provided for a safety function to be independent of and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function during and following any design basis event requiring that safety function. GDC 22, "Protection System Independence," requires the protection system to be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis. Section 6 of the AREVA NP Topical Report ANP-10281, "U.S. EPR Digital Protection System Topical Report," provides a description of the network topologies implemented within the protection system. This topical report is currently under NRC review and has not yet been approved. This topical report states that remote acquisition unit - acquisition and processing unit (RAU-APU) network is implemented using a redundant ring topology across all four redundant divisions of the PS. Optical Link Modules (OLMs) are used to interconnect this ring network with the functional units of each redundant division. Due to the design of the OLM, every signal received in one port of the OLM will be forwarded out all other ports of the OLM. This topical report states that the individual functional computer within each division will be responsible for ensuring IEEE Std. 603-1991, Clause 5.6.1, requirements for independence between redundant portions of the safety system are met. The staff requests the applicant to clarify how the implementation of the RAU-APU network will meet IEEE Std. 603-1991, Clause 5.6.1, and GDC 22 requirements if there is a failure within the functional computer such that communications independence is not maintained. Additionally, demonstrate how the design of the RAU-APU ring topology addresses the guidance provided in the Interim Staff Guidance (ISG) for Highly Integrated Control Room (HICR)-Communications (Digital I&C ISG #4). This ISG states that only point-to-point communication should be implemented for vital communications between redundant divisions. Demonstrate how the same level of independence will be achieved through a ring network such that an error within the network or within one division will not propagate to multiple other divisions. Provide information regarding the hardware and software design, all possible failures within the hardware and software and their effects, as well as any testing that have been completed to demonstrate that IEEE Std. 603-1991, Clause 5.6.1, requirements are met. 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. Describe all failure modes that can exist within the data communications systems used within the protection system and demonstrate how they fail into a safe or acceptable state to meet the requirements of GDC 23.

**Response to Question 07.09-17:**

This question contains four separate requests. Each request is identified and addressed individually below.

**Request 1:**

“The staff requests the applicant to clarify how the implementation of the RAU-APU network will meet IEEE Std. 603-1991, Clause 5.6.1, and GDC 22 requirements if there is a failure within the functional computer such that communications independence is not maintained.”

**Response 1:**

The protection system (PS) design is subject to and satisfies the single failure criterion. The use of Class 1E qualified equipment, along with design processes and testing carried out under 10 CFR 50 Appendix B quality assurance program, dictate that no more than one safety-related failure at a time is considered.

A safety-related design function of each function processor in a RAU-APU ring topology network is to correctly construct and transmit valid data messages. Another safety-related design function of each function processor is to detect and disposition invalid received messages. Application of the single failure criterion dictates that a postulated failure of a sending unit resulting in an invalid message sent, concurrent with a failure of a receiving unit to detect the message as being invalid, is beyond the design basis of the system.

If this concept of a safety-related transmit function separate from a safety-related receive function is ignored, then a point-to-point data connection between two redundant divisions is unacceptable. The application of this concept to the RAU-APU redundant ring topology networks is no different than application to a point-to-point network.

Communications independence can only be compromised through a failure of both the sending processor and a receiving processor. This type of multiple-failure scenario is beyond the design basis of the PS, similar to a postulated software common cause failure affecting more than one redundant division. A diverse actuation system is provided to cope with these beyond design basis events.

The methods used to establish communication independence between redundant portions of the PS are described in Topical Report ANP-10281P, “U.S. EPR Digital Protection System.”

**Request 2:**

“Demonstrate how the same level of independence will be achieved through a ring network such that an error within the network or within one division will not propagate to multiple other divisions.”

**Response 2:**

In a point-to-point network, an error in the sending division (single failure) will propagate to the receiving division. If the receiving entity does not recognize and accommodate the error (additional single failure), then communication independence has been compromised, which is an unacceptable result.

Similarly, in a Teleperm XS (TXS) ring topology, an error in the sending division (single failure) will propagate to the other divisions on the ring. If the other function processors on the ring do

not detect and accommodate the error (additional single failures), then communication independence has been compromised, which is an unacceptable result.

The use of a point-to-point network is not a means to establish communication independence; communication independence must be demonstrated in spite of such a connection. The existence of a point-to-point connection between two redundant divisions results in the need for the establishment of communication independence.

The methods used to establish communication independence between redundant portions of the PS are described in Topical Report ANP-10281P, "U.S. EPR Digital Protection System."

**Request 3:**

"Provide information regarding the hardware and software design, all possible failures within the hardware and software and their effects, as well as any testing that have been completed to demonstrate that IEEE Std. 603-1991, Clause 5.6.1 requirements are met."

**Response 3:**

Possible failures within the hardware and software and results of qualification or system testing are identified later in the design process, when specific versions of hardware are selected and the detailed software design is complete.

The system-level failure modes and effects analysis (FMEA) is summarized in U.S. EPR FSAR Tier 2, Section 7.2 and Section 7.3. These sections describe the bounding network failures that the FMEA includes.

**Request 4:**

"Describe all failure modes that can exist within the data communications systems used within the protection system and demonstrate how they fail into a safe or acceptable state to meet the requirements of GDC 23."

**Response 4:**

Failure modes that can exist within the data communications systems are identified later in the design process, when specific versions of hardware are selected and the detailed software design is complete.

AREVA NP has addressed each of the postulated communication failures found in Interim Staff Guidance (ISG) for Highly Integrated Control Room (HICR)-Communications (Digital I&C ISG #4) by identifying the TXS platform and PS system architecture characteristics that mitigate each failure type. This information was provided to the NRC staff on August 8, 2008 as Topical Report ANP-10281P, "Supplemental Information for the Digital Protection System."

The system-level FMEA is summarized in U.S. EPR FSAR Tier 2, Section 7.2 and Section 7.3. These sections describe the bounding network failures that the FMEA includes.

**FSAR Impact:**

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

**Question 07.09-19:**

Address the acceptance criteria of NUREG-0800, the Standard Review Plan (SRP), Section 7.9, "Data Communications Systems," for the data communications systems used in the protection system to support reactor trip system (RTS) and engineered safety features actuation system (ESFAS) functions.

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 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. SRP, Section 7.9, states that setpoint analyses should account for measurement inaccuracies attributable to the data communications systems in accordance with the guidance of Regulatory Guide 1.105, Revision 3. Show that the measurement inaccuracies attributable to the data communications systems are accounted for in the setpoint analyses.

Section 7 and 8 of the AREVA NP Topical Report ANP-10281 "U.S. EPR Digital Protection System Topical Report" provides a description of the system level RTS and ESFAS design. In addition, FSAR Tier 2, Sections 7.2 and 7.3, provide additional details on the RTS and ESFAS design. The staff finds that these descriptions do not provide sufficient information on the setpoint analyses to account for measurement inaccuracies attributable to the data communications system in accordance with the guidance of Regulatory Guide 1.105, Revision 3.

**Response to Question 07.09-19:**

In March 2007, AREVA NP submitted ANP-10275P, "U.S. EPR Instrument Setpoint Methodology Topical Report" for NRC review (ML070880719). This topical report was approved by SER on December 20, 2007.

ANP-10275P, Section 2.4, "Instrumentation and Controls Digital Protection System Uncertainties" describes the setpoint uncertainties considered for a digital system.

The networked data communications within the protection system (PS) do not introduce measurement inaccuracies beyond those described in ANP-10275P, Section 2.4.

**FSAR Impact:**

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

**Question 07.09-25:**

Demonstrate compliance with IEEE 603-1991, Clause 5.6 by addressing the guidance in Interim Staff Guidance (ISG) (Digital I&C ISG #4) Highly Integrated Control Room (HICR) – Communications.

Independence requirements of IEEE Std. 603-1991, Clause 5.6, are addressed by guidance in interim staff guidance (ISG) (Digital I&C ISG #4) on communications. Digital I&C ISG #4 HICR-Communications provide further clarification on acceptable methods of data communications between redundant divisions of the safety system and between safety and non-safety systems. This communications ISG states that vital communications among safety divisions should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. The staff requests that the applicant demonstrate that data communications between redundant divisions for each of the safety systems (Safety Information and Control System, Safety Automation System, Protection System, Priority Actuation and Control System) addresses the guidance of ISG #4- HICR-Communications with respect to point-to-point communication.

**Response to Question 07.09-25:**

Point #14 on page 7 in Digital I&C ISG #4 provides the following guidance on point-to-point communications:

“Vital communications should be point to point by means of a dedicated medium (copper or optical cable). In this context, “point to point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending and receiving node.”

Page 16 in Digital I&C ISG #4 provides the following definition of vital communications:

“Vital communications as used herein are communications that are needed to support a safety function. Failure of vital communications could inhibit the performance of the safety function. The most common implementation of vital communications is the distribution of channel trip information to other divisions for the purpose of voting.”

Vital communications between redundant divisions of the safety information and control systems (SICs) are provided through point-to-point connections. These point-to-point connections are shown in U.S. EPR FSAR Tier 2, Figure 7.1-3—Safety Information and Control System Architecture (Safety Related Portion) as functional data connections between the monitoring panel interfaces (PIs). U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 describes the PI-PI (Monitoring) data communications as bi-directional, point-to-point data connections. The vital communications sent between these point-to-point connections allow the display of redundant divisional information on a single qualified display system (QDS) for optimization of the human factors design.

Vital communications between redundant divisions of the safety automation system (SAS) are provided through point-to-point connections. The vital communications that are transmitted between the divisions are redundant sensor values which are used as inputs to signal selection

algorithms. The signal selection algorithms provide reliability in the control of safety-related processes. These point-to-point connections are shown between the control units (CUs) in U.S. EPR FSAR Tier 2, Figure 7.1-7—Safety Automation System Architecture of the U.S. EPR FSAR. Separate point-to-point connections are used for redundancies A and B as shown in the figure.

Topical Report ANP-10281P, “U.S. EPR Digital Protection System” describes the network topologies used for interdivisional communication connections in the protection systems (PSs). ANP-10281P Section 6.1.1 describes the redundant point-to-point network topology and Section 6.1.2 describes the ring network topology that is used to send vital communication between divisions. ANP-10281P Section 6.1.3 and Section 12 explain how these networks provide communication independence between the divisions of the PS.

The priority and actuator control system (PACS) does not require vital communications between divisions of the PACS. Safety-related signals sent to the PACS modules are hardwired from safety-related I&C systems (SICS, PS, and SAS) within the same division. This is illustrated in U.S. EPR FSAR Tier 2, Figure 7.1-8—Priority and Actuator Control System Architecture.

**FSAR Impact:**

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

**Question 07.09-28:**

Demonstrate how data communications between the Process Information and Control System (PICS) and the safety systems comply with IEEE Std. 603-1991, Clause 5.6.3, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24. Specifically, provide information that demonstrates how communications independence is achieved between the PICS and the safety systems.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from completing their intended safety functions. GDC 24, "Separation of Protection and Control Systems" requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

DC FSAR, Tier 2, Section 7.1.1.3.2 provides a description of the data communications within PICS. This section states that the PICS is used to control both safety-related and non-safety-related process systems. Demonstrate how data communications used by the PICS to perform control of safety-related process systems meet the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.3 and GDC 24.

**Response to Question 07.09-28:**

The PICS is classified as non-safety-related and is not credited for meeting IEEE Std. 603-1991, Clause 5.6.3, "Independence between Safety Systems and Other Systems," and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24.

IEEE Std. 603-1991, Clause 5.6.3.1 (1) states: "Equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system." The PICS does not perform any safety-related functions. Additionally, the methods and equipment that provide isolation between the PICS and the safety systems is classified as part of the safety systems and not the PICS. Therefore, IEEE Std. 603-1991, Clause 5.6.3 does not apply to the PICS.

Conformance to IEEE Std. 603-1991, Clause 5.6.3 is discussed in U.S EPR FSAR Tier 2, Section 7.4.2.2. Conformance to 10 CFR Part 50, Appendix A, GDC 24 is discussed in U.S EPR FSAR Tier 2, Section 7.1.2.2.13. U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 discusses the implementation of independence between safety-related and non-safety-related I&C systems.

Additionally, Topical Report ANP-10281P, "U.S. EPR Digital Protection System" discusses the interface between the PICS and the protection system (PS), including communication independence and isolation.

**FSAR Impact:**

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

**Question 07.09-30:**

Demonstrate that there is sufficient quality in the PICS data communications components to support the control room capabilities required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 19.

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.

DC FSAR, Tier 2, 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. The capabilities of the PICS to achieve both hot and cold shut down conditions from the remote shutdown system are also described in Section 7.1.1.3.2. Equipment such as network switches and electrical and fiber optic cables are provided to support the required data communications between the PICS and other instrumentation and control systems. The staff requires the applicant to provide information regarding the quality of the network switches and electrical and fiber optic cable to support PICS such that the capability for safe operation of the plant is maintained as required by GDC 19.

**Response to Question 07.09-30:**

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.

For those cases where the PICS will exchange information with safety-related I&C systems, communications independence is provided via the MSIs. Qualified isolation devices are used to provide electrical isolation between the PICS and the safety-related I&C systems for hardwired signals. The MSIs and the qualified isolation devices are part of the safety-related I&C system's scope.

**FSAR Impact:**

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

**Question 07.09-32:**

Demonstrate how the communications between the Protection System (PS) and Diverse Actuation System (DAS), and between the DAS and the Priority Actuation and Control System (PACS) meet IEEE Std. 603-1991, Clause 5.6.3, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety systems and other systems. This clause requires the safety system be designed such that credible failures in and consequential actions by other systems shall not prevent the safety systems from performing their intended safety functions. GDC 24, "Separation of Protection and Control Systems" requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

DC FSAR, Tier 2, Section 7.1.1.4.6, provides a description of the DAS. This section states that the DAS has four separate divisions, with each division containing a diverse actuation unit (DAU). Hardwired signals are acquired from the PS and compared to a setpoint. Fiber optic data point-to-point connections are provided to share trip requests, and two out of four voting is done in each DAU. Outputs are sent to the PACS via hardwired connections. Since the PS and PACS module are classified as safety-related, demonstrate how electrical and communications independence are maintained between the DAS and the PACS and between the DAS and the PS.

**Response to Question 07.09-32:**

U.S. EPR FSAR Tier 2, Section 7.1.1.6.4, "Independence" discusses measures applicable to I&C systems for establishing independence.

The sub-heading "Independence between the Safety I&C Systems and Non-Safety I&C Systems" states the following:

"Electrical isolation is provided for both hardwired and data communications between safety-related and non-safety-related I&C. For hardwired signals, qualified isolation devices are used with the safety-related I&C systems for signals to and from the non-safety-related I&C. Fiber optic cable is used for data connections between safety-related and non-safety-related I&C."

Because the connections between the DAS and PACS and between the DAS and PS are hardwired connections, electrical isolation is achieved with qualified isolation devices. Hardwired signals (as defined in U.S. EPR FSAR Tier 2, Section 7.1, "Definitions") do not require demonstration of communications independence.

**FSAR Impact:**

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

**Question 07.09-33:**

Clarify what additional data connections may be implemented in the Process Automation System (PAS) as stated in the DC FSAR, Tier 2, Section 7.1.1.4.6. Specifically, demonstrate how communications between the PAS and other non-safety systems meet IEEE Std. 603-1991, Clauses 5.6.3 and 5.9.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from completing their safety intended functions. IEEE Std. 603-1991, Clause 5.9, provides access control requirements for safety systems. This clause requires the design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

DC FSAR, Tier 2, Section 7.1.1.4.6, provides a description of data communications within the PAS. This section states that besides the data communications described within the subsystems of the PAS, other data connections may be implemented as required. Provide clarification on what other data connections may be required and whether it is bounded by any access control and independence requirements as required by IEEE Std. 603-1991, Clauses 5.6.3 and 5.9.

**Response to Question 07.09-33:**

This question contains two separate requests. Each request is identified and addressed individually below.

**Request 1:**

“What additional data connections, besides the data communications described within the subsystems of the PAS, may be implemented in the Process Automation System (PAS) as stated in the DC FSAR, Tier 2, Section 7.1.1.4.6?”

**Response 1:**

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.

**Request 2:**

“How do communications between the PAS and other non-safety systems meet IEEE Std. 603-1991, Clauses 5.6.3 and 5.9?”

**Response 2:**

IEEE Std. 603-1991, Clauses 5.6.3 and 5.9 specifically apply to safety-related equipment. The PAS is classified as non-safety-related and is not subject to the requirements of IEEE Std. 603-1991, Clauses 5.6.3 and 5.9, with respect to communication with other non-safety systems.

**FSAR Impact:**

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

**Question 07.09-35:**

Demonstrate how communications between the safety instrumentation and control (I&C) systems and the control unit (CU) and between the Process Automation System (PACS) and the Severe Accident I&C (SA I&C) systems system meet IEEE Std. 603-1991, Clause 5.6.3.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety systems and other systems. This clause requires the safety system be designed such that credible failures in and consequential actions by other systems shall not prevent the safety systems from performing their intended safety functions.

DC FSAR, Tier 2, Section 7.1.1.4.5, provides a description of data communications within the Severe Accident (SA) I&C system. This section states that hardwired inputs are acquired directly from field sensors or from isolated outputs of the safety I&C systems. Hardwired outputs are sent to the DCMs or PACS for component actuation. Provide information to demonstrate how the outputs from the safety I&C systems to the CUs are adequately isolated to meet IEEE Std. 603-1991, Clause 5.6.3. Are these outputs electrically isolated using Class 1E isolation devices? In addition, how is communications independence and electrical isolation maintained for the hardwired outputs from the SA I&C to the PACS to meet IEEE Std. 603-1991, Clause 5.6.3?

**Response to Question 07.09-35:**

The SA I&C system is not credited for meeting the requirements of IEEE Std. 603-1991, Clause 5.6.3. Where the SA I&C system interfaces with a safety I&C system, the safety I&C system is credited with satisfying the requirements of IEEE Std. 603-1998, Clause 5.6.3.

U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 describes how safety I&C systems interface with non-safety I&C systems. Safety systems of the U.S. EPR provide communication independence through the Class 1E qualified monitoring and service interface (MSI). Electrical isolation is provided through the Class 1E qualified isolation devices. Topical Report ANP-10273P, "AV42 Priority Actuation and Control Module," Section 4.8 describes how the PACS provides communication independence and electrical isolation between the PACS and non-safety I&C systems.

**FSAR Impact:**

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

**Question 07.09-45:**

Describe how the redundant communications paths between the Turbine Generator (TG) control room and the plant Process Automation System (PAS) is implemented.

DC FSAR, Tier 2, Section 10.2.2.5, provides a description of the design of the TC instrumentation and control system, including the data communications functions within this system. The applicant states in this section that two redundant communications paths are provided to connect the TG control system to the plant PAS. The staff requests the applicant to clarify how the redundant communications paths between the TG control room and the plant PAS is implemented. Specifically, state whether these direct communications paths are implemented via direct links or via the plant data network. If it is via direct links, are these links implemented with fiber-optic or copper cabling?

**Response to Question 07.09-45:**

As shown in U.S. EPR FSAR Tier 2, Figure 7.1.2—U.S. EPR I&C Architecture, the TG I&C is connected via the plant data network. Note that the as-built implementation of the network in question relies on the technologies (i.e., platform, manufacturer, vendor) selected for use.

**FSAR Impact:**

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

# U.S. EPR Final Safety Analysis Report Markups

Section 7.2 and Section 7.3 describe the methods used for manual actuation of reactor trip and engineered safety features. For other manual controls, the human factors principles described in Chapter 18 shall be used to select the type of HMI used.

07.09-7 →

~~SUs are provided for configuration and maintenance of the SICS. The PIs are serviced by the SUs of the SAS via the monitoring and service interface (MSI) of the SAS. The QDSs have dedicated SUs that are only connected to the QDS. The number and location of SUs is determined based on the number and layout of QDSs.~~

#### *Non-Safety-Related Portion of SICS*

Figure 7.1-4—Safety Information and Control System Architecture (Non-Safety-Related Portion) provides a functional representation of the non-safety-related portion of the SICS.

These functional units are implemented in the non-safety-related portion of the SICS:

- Gateways (GW).
- Qualified display systems ~~(QDS)~~.
- Service units.

GWs are provided to interface to the plant data network.

QDSs provided in divisions 2 and 3 to monitor and control other non-safety-related I&C systems via GWs on a loss of PICS.

QDSs are provided in divisions 1 and 4 to monitor and control equipment dedicated to mitigate severe accidents. These QDS utilize point-to-point data connections to transmit and receive information to the severe accident I&C (SA I&C).

The QDSs have dedicated SUs that are only connected to the QDS. The number and location of SUs is determined based on the number and layout of QDSs.

Hardwired I&C is also provided to monitor and control non-safety-related I&C systems. The human factors principles described in Chapter 18 are used to select the type of HMI used.

07.09-7 →

SUs are provided for configuration and maintenance of the SICS. The PIs are serviced by the SUs of the safety automation system (SAS) via the monitoring and service interface (MSI) of the SAS. The QDSs have dedicated SUs that are only connected to the QDS. The number and location of SUs is determined based on the number and layout of QDSs.

- SAS-SICS (Monitoring) – uni-directional (SAS to SICS), point-to-point data connections implemented with the TXS Profibus protocol.
- PI-QDS (Control) – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- PI-QDS (Monitoring) – uni-directional (PI to QDS), point-to-point data connections implemented with the TXS Ethernet protocol.
- PI-PI (Monitoring) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. This network is provided to allow the display of redundant divisional information on a single QDS for optimization of the human factors design. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4.

07.09-7 →

- ~~SU-QDS – bi-directional, networked data connections implemented with the TXS Ethernet protocol. The SU is an auxiliary feature, and this network is non-safety-related network provided for servicing of the QDSs. These data connections use dedicated ports on the QDS separate from the PI-QDS connections. The system software provides for isolation between the safety-related and non-safety-related data. Software modifications cannot be performed with the QDS in operation. Access is authorized only with appropriate administrative controls. Fiber optic cable is provided for electrical isolation.~~

~~These are a summary of the data~~ Data communications implemented in the non-safety-related portion of the SICS are:

07.09-7 →

- SU-QDS – bi-directional, networked data connections implemented with the TXS Ethernet protocol. The SU is an auxiliary feature, and this network is a non-safety-related network provided for servicing of the QDSs. These data connections use dedicated ports on the QDS separate from the PI-QDS connections. The system software provides for isolation between the safety-related and non-safety-related data. Software modifications cannot be performed with the QDS in operation. Access is authorized only with appropriate administrative controls. Fiber optic cable is provided for electrical isolation.

- SA I&C-SICS – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- GW-QDS – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data Network – bi-directional, networked communications.
- SU-QDS – bi-directional, networked data connections.

### Power Supply

The safety-related portion of the SICS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and