Response to

Request for Additional Information No. 286, Supplement 5

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 07.09-46:

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:

Key Definitions

The following key definitions provide background for this response and are referenced from the U.S. EPR FSAR and ISG04, as indicated:

Interdivisional communication	Communication among different safety divisions or between a safety division and a non-safety entity. (ISG04)
Safety division	The collection of safety channels that are powered by a single power division. Different channels perform different functions. Different divisions perform the same set of functions, and are redundant. Licensing credits redundancy among divisions. The voting logic that generates the final actuation signal to an item of plant equipment resides in one division and receives input from redundant channels in divisions. For this guidance, it is assumed that each of the actuation signals entering the voting logic that establishes the final actuation signal to an item of plant equipment is in a different division, regardless of the particular usage of the term “division” for a particular nuclear power plant. (ISG04)
Data communication	A method of sharing information between devices that involves a set of rules, formats, encodings, specifications, and conventions for transmitting data over a communication path, known as a protocol. (U.S. EPR FSAR)
Hardwired signal	An analog or discrete digital signal that does not use a data communications protocol. (U.S. EPR FSAR) U.S. EPR FSAR Tier 2, Section 7.1 will be revised to include “analog or discrete digital” to the existing hardwired signal definition.

Introduction to Table 07.09-46-1

Table 07.09-46-1 identifies the data communication interfaces between safety divisions and between safety- and non-safety-related systems in the U.S. EPR. These interfaces are identified in the ”Types of Interface” and “Data Communication Interface” columns. The ”Independence Aspect” row identifies the independence aspects (i.e., physical separation, electrical isolation, communication independence) addressed. Each cell in the matrix references a “note.” The notes provide the technical information to address independence related to a specific data communication interface.

Table 07.09-46-1 does not provide a column for “functional independence” as requested by this question. As agreed in the January 25-26 public meeting between AREVA NP and the NRC, the concept of “functional independence” is addressed through conformance with the 20 criteria in ISG-04, which are discussed in the communications independence notes.

Table 07.09-46-1 includes an entry for priority and actuator control system (PACS) to process automation system (PAS) data communication. This interface is shown as safety to non-safety because the PACS is a safety-related system. The PAS communicates only with the non-safety-related portion of the PACS, and this interface is not relevant to this response. A specific note is provided to clarify the PACS to PAS communication interface.

Table 07.09-46-1—Data Communication Interfaces and Independence Aspects

Type of Interface	Data Communication Interface	Independence Aspects		
		Physical Separation	Electrical Isolation	Communications Independence
Safety to Safety	PS division - PS division	Note 1	Note 2	Note 10
	SAS division - SAS division	Note 1	Note 2	Note 10
	SICS division - SICS division	Note 3	Note 2	Note 10
Safety to Nonsafety	PS - PICS	Note 4	Note 5	Note 10
	SAS - PICS	Note 4	Note 5	Note 10
	PS – SU	Note 6	Note 6	Note 10
	SAS – SU	Note 6	Note 6	Note 10
	SICS – SU	Note 7	Note 8	Note 10
	PACS – PAS	Note 9		

Notes:

1. Physical separation between divisions of the protection system (PS) and the safety automation system (SAS).

   The equipment of each independent PS and SAS division is located in physically separated Safeguards Buildings (SBs). See U.S. EPR FSAR Tier 2, Section 7.1.1.6.4. Location of redundant divisions in separate buildings prevents internal hazards (e.g., fire or flooding) in one division from affecting the redundant divisions.

   U.S. EPR FSAR Tier 1, Sections 2.4.1 and 2.4.4 contain ITAAC commitments for verification of physical separation between PS and SAS divisions.

   Physical separation of cabling is addressed in U.S. EPR FSAR Tier 2, Section 8.3.1.1.9.

2. Electrical isolation between safety-related divisions.

   Electrical isolation between safety-related divisions is achieved through the application of qualified isolation devices or fiber optic cable. See U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 for more information.

Electrical isolation devices used in the U.S. EPR will conform to the guidance of Regulatory Guide (RG) 1.75 and IEEE Std 384-1992. See U.S. EPR FSAR Tier 2, Section 7.1.2.4.5.

Electrical isolation devices used in the U.S. EPR will conform to the guidance of BTP 7-11. See U.S. EPR FSAR Tier 2, Section 7.1.2.5.9 for more information.

ITAAC regarding electrical isolation between safety-related instrumentation and controls (I&C) divisions are provided in U.S. EPR FSAR Tier 1, Sections 2.4.1, 2.4.2, 2.4.4.

3. Physical separation between safety information and control system (SICS) divisions.

   Physical separation is addressed differently for the panel interfaces (PIs) and the human machine interface (HMI) equipment located in the main control room (MCR) or remote shutdown station (RSS).

   The four divisions of PIs are located in the four separate SBs. Location of redundant divisions in separate buildings prevents internal hazards (e.g., fire or flooding) in one division from affecting the redundant divisions.

   The four divisions of HMI equipment located in the MCR or RSS are physically separated in accordance with the guidance of RG 1.75 and IEEE Std 384-1992. See U.S. EPR FSAR Tier 2, Section 7.1.2.4.5 for more information.

   U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 states:

   > "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."

   U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 will be revised to specify that the PIs (not all of the safety-related portion of SICS) are located in separate SBs.

   U.S. EPR FSAR Tier 1, Section 2.4.2 will be revised to add ITAAC to verify physical separation exists between safety-related SICS divisions.

   Cabling separation is addressed in U.S. EPR FSAR Tier 2, Section 8.3.1.1.9.

4. Physical separation of the PS and the SAS from the process information and control system (PICS).

   Safety-related I&C equipment is physically separated from non-safety-related equipment in accordance with the guidance of RG 1.75 and IEEE Std 384-1992. See U.S. EPR FSAR Tier 2, Section 7.1.2.4.5 for more information.

   PICS equipment is located in SBs 2 and 3. Within these buildings, physical separation of the PICS from divisions 2 and 3 of the SAS and the PS is achieved through safety-related grade structures, separation distance, barriers or any combination. Divisions 1 and 4 of the SAS and the PS are located in separate SBs than PICS equipment.

   U.S. EPR FSAR Tier 1, Section 2.4.1 will be revised to add ITAAC to verify that physical separation exists between safety-related PS equipment and non-safety-related equipment.

U.S. EPR FSAR Tier 1, Section 2.4.4 will be revised to add ITAAC to verify that physical separation exists between safety-related SAS equipment and non-safety-related equipment.

5. Electrical isolation of the PS and SAS from the PICS.

   U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 states:

   > "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 nonsafety- related I&C. Fiber optic cable is used for data connections between safety related and non-safety-related I&C."

   Consistent with this description, fiber optic cabling is used between the PICS and the monitoring service interfaces (MSIs) of the SAS and the PS.

   Electrical isolation in the U.S. EPR will conform to the guidance of RG 1.75 and IEEE Std 384-1992. See U.S. EPR FSAR Tier 2, Section 7.1.2.4.5 for more information.

   Electrical isolation used in the U.S. EPR design will conform to the guidance of BTP 7-11. See U.S. EPR FSAR Tier 2, Section 7.1.2.5.9 for more information.

   U.S. EPR FSAR Tier 2, Figure 7.1-20 illustrates isolation between safety-related systems and non-safety-related entities.

   Technical Report ANP-10309P, Figure 12-2—Safety to Non-Safety-Related Communication Interface (U.S. EPR Implementation) illustrates isolation between the PS and the PICS. The same electrical isolation approach applies to the SAS - PICS interface.

   U.S. EPR FSAR Tier 1, Sections 2.4.1 and 2.4.4 contain ITAAC to verify that the PS and the SAS are electrically isolated from non-safety-related equipment.

6. Physical separation and electrical isolation of the SAS and PS from service units (SUs).

   Technical Report ANP-10309P, Section 12.2, "Protection System – Service Unit Interface," states:

   > "Electrical isolation is provided through optical connections between the SU and the MSI."

   This statement also applies to the SAS.

   U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 states:

   > "The safety related I&C systems are physically separated from non-safety related I&C systems."

   Physical separation between safety-related I&C equipment and non-safety equipment is provided in accordance with the guidance of RG 1.75 and IEEE Std 384-1992. See U.S. EPR FSAR Tier 2, Section 7.1.2.4.5 for more information.

U.S. EPR FSAR Tier 1, Sections 2.4.1 and 2.4.4 contain ITAAC to verify that the PS and the SAS are electrically isolated from non-safety-related equipment.

As described in Note 4, U.S. EPR FSAR Tier 1, Section 2.4.1 will be revised to add ITAAC to verify that physical separation exists between safety-related PS equipment and non-safety-related equipment, and U.S. EPR FSAR Tier 1, Section 2.4.4 will be revised to add ITAAC to verify that physical separation exists between safety-related SAS equipment and non-safety-related equipment.

7. Physical Separation between SICS and SUs.

   U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 states:

   > "The safety related I&C systems are physically separated from non-safety related I&C systems."

   Physical separation between safety-related I&C equipment and non-safety-related equipment is provided in accordance with the guidance of RG 1.75 and IEEE Std 384-1992. See U.S. EPR FSAR Tier 2, Section 7.1.2.4.5 for more information.

   U.S. EPR FSAR Tier 1, Section 2.4.2 will be revised to add ITAAC to verify that physical separation exists between safety-related SICS equipment and non-safety-related equipment.

8. SICS to SU electrical isolation.

   The SICS architecture is described in U.S. EPR FSAR Tier 2, Section 7.1.1.3.1, "Safety Information and Control System."

   U.S. EPR FSAR Tier 2, Section 7.1.1.3.1 explains that the SICS has two types of connection to SUs: from the PIs and from the qualified display systems (QDSs).

   The PI-to-SU connection is implemented in the same manner as those for PS and SAS, and electrical isolation for that interface type is described in **Error! Reference source not found.**.

   Electrical isolation between safety-related QDSs and their SUs is addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.3.1:

   > "The QDSs have dedicated non-safety related SUs that are only connected to the QDS when the QDS is out of service. They are normally isolated through a key lock switch."

   U.S. EPR FSAR Tier 1, Section 2.4.2 contains ITAAC to verify that the safety-related SICS equipment is electrically isolated from non-safety-related equipment.

9. PACS to PAS communications.

   U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 states:

   > "Data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related PACS communication module. Connections

between the communication module and safety related priority module are hardwired. The communication module is qualified as an associated circuit."

The PACS to PAS data communication interface is non-safety-related to non-safety-related, and is not interdivisional communication.

The PACS internal "hardwired" communications (i.e., between the safety-related priority module and the separate non-safety-related communication module) is not a data communication interface and is not pertinent to this RAI.

10. Communications independence.

U.S. EPR FSAR Tier 1, Section 2.4.1 contains ITAAC to verify that communications independence exists between PS divisions and between the PS and non-safety-related equipment.

U.S. EPR FSAR Tier 1, Section 2.4.2 contains ITAAC to verify that communications independence exists between safety-related SICS divisions and between the safety-related SICS equipment and non-safety-related equipment.

U.S. EPR FSAR Tier 1, Section 2.4.1 contains ITAAC to verify that communications independence exists between SAS divisions and between the SAS and non-safety-related equipment.

The technical information in this response is supported by and described further in Siemens Power Corporation Topical Report EMF-2110NP(A), "TELEPERM XS: A Digital Reactor Protection System." The EMF-2110NP(A) sections that contain this information are:

- Sections 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, and 2.9.
- Sections 3.1, 3.2, 3.3, and 3.4.
- Section 4.
- Sections 7.3, 7.4, and 7.6.

The following numbered sections correspond with the 20 staff position criteria of ISG04, Section 1, "Interdivisional Communications."

Staff Position 1:

A safety-related channel should not be dependent upon any information or resource originating or residing outside its own safety-related division to accomplish its safety-related function. This is a fundamental *consequence of the independence requirements of IEEE Std 603. It is recognized that division voting logic must receive inputs from multiple safety-related divisions.*

PS conformance:

The PICS provides information to the PS to validate/inhibit permissive functions and to reset engineered safety feature actuation system (ESFAS) actuation signals. The PS does not

depend on this information from the PICS to perform its safety-related function because this information can be supplied from the safety-related SICS.

ISG04, Section 1, Staff Position 1 recognizes that "division voting logic must receive inputs from multiple safety divisions." The voting logic in each division of the PS uses information from the four PS divisions as input, and no PS division is dependent on other single divisions. The voting logic is modified to a predefined condition if invalid information or no information is received from other divisions. Modification of the voting logic is described in Technical Report ANP-10309(P), "U.S. EPR Digital Protection System," Sections 7.3 and 8.2.

Communication between PS divisions is used to transmit self-powered neutron detector (SPND) measurement values from the division that acquires the measurement to the other PS divisions. Loss of or invalid communication between divisions results in setpoint changes that conservatively accommodate a limited number of invalid signals or an automatic reactor trip (RT) if seven or more individual measurements are invalid.

SAS conformance:

The PICS provides information to the SAS for manual control of safety-related actuators. The SAS does not depend on this information from the PICS to perform its safety-related function because control of safety-related actuators is available from the safety-related SICS.

Communication between SAS divisions is used to transmit sensor measurement values between divisions. Signal selection algorithms (e.g., 2nd Min, 2nd Max, and average) are used to accommodate loss or invalid communication between any two divisions. Assuming a loss of communication between divisions, each SAS division can perform its function using the sensor information directly acquired in its own division.

SICS conformance:

U.S. EPR FSAR Tier 2, Figure 7.1-3 illustrates the safety-related SICS architecture and indicates separate equipment used for control and for monitoring. No interdivisional data communication is used in the "control" portion of the SICS. Regarding monitoring functionality, communication between SICS divisions is used at the PI level to transmit redundant divisional information for processing before display to the operator. Signal selection algorithms (e.g., 2nd Min, 2nd Max, and average) are used to accommodate loss of or invalid communication between any two divisions. Assuming a loss of communication between divisions, each SICS division can perform its monitoring function by displaying its own divisional information to the operator.

Staff Position 2:

The safety-related function of each safety-related channel should be protected from adverse influence from outside the division of which that channel is a member. Information and signals originating outside the division must not be able to inhibit or delay the safety-related function. This protection must be implemented within the affected division (rather than in the sources outside the division), and must not itself be affected by any condition or information from outside the affected division. This protection must be sustained despite any operation,

malfunction, design error, communication error, or software error or corruption existing or originating outside the division.

PS conformance:

For manual validation/inhibition of permissives from the PICS, the PS uses safety-related input sensors to determine that the current plant state provides acceptable validation/inhibition of the permissive. If the plant conditions are not acceptable, the PS will not change the permissive state, regardless of commands from PICS. This protection is implemented separately within each PS division.

For a manual reset of ESFAS actuation signals from the PICS, the safety-related function is protected. If the PICS requests a reset, the PS actuation output signal is removed. The removal of the actuation signal does not change the state of the ESFAS actuators. The ESFAS actuators will continue to perform their function. Separate, additional operator action is required to change the state of the actuators.

Controls on SICS to block PICS commands to the PS provide additional protection. This logic is implemented within each division of the PS and is shown on U.S. EPR FSAR Tier 2, Figure 7.1-1, Sheet 9 (Manual Interface Block).

The PS is protected from adverse influence by the SU, which is implemented independently in each processor that is part of the PS and is described further under Staff Position 10.

Where data communication is used between PS divisions, each PS division is protected from adverse influence by the other divisions. Protection against spurious or missing partial trigger signals is provided by the voting logic, which is implemented separately in each division.

Protection against communication faults is provided for data communication between PS divisions and between the PS and non-safety-related systems. This protection is described under Staff Position 12.

SAS conformance:

Protection of the SAS from adverse influence by the PICS is provided by controls that are available on the SICS to block the PICS commands to the SAS. This logic is implemented within each division of the SAS and is shown on U.S. EPR FSAR Tier 2, Figure 7.1-1, Sheet 9 (Manual Interface Block).

The SAS is protected from adverse influence by the SU, which is implemented independently in each processor that is part of the SAS and is described further under Staff Position 10.

Where data communication is used between SAS divisions, each SAS division is protected from adverse influence by the other divisions. Protection against transmission of erroneous sensor measurements is provided by signal selection algorithms, which are implemented separately in each division.

Protection against communication faults is provided for data communication between SAS divisions and between the SAS and non-safety-related systems. This protection is described under Staff Position 12.

SICS conformance:

The SICS is protected from adverse influence by its SUs, which is implemented separately in each division and is described further under Staff Position 10.

Where data communication is used between safety-related SICS divisions, each SICS division is protected from adverse influence by the other divisions. Signal selection algorithms are implemented separately in each division to protect against erroneous transmitted data.

Protection against communication faults is provided for data communication between SICS divisions and between the SICS and non-safety-related systems. This protection is described under Staff Position 12.

Staff Position 3:

A safety-related channel should not receive any communication from outside its own safety-related division unless that communication supports or enhances the performance of the safety-related function. Receipt of information that does not support or enhance the safety-related function would involve the performance of functions that are not directly related to the safety-related function. Safety-related systems should be as simple as possible. Functions that are not necessary for safety, even if they enhance reliability, should be executed outside the safety-related system. A safety-related system designed to perform functions not directly related to the safety-related function would be more complex than a system that performs the same safety-related function, but is not designed to perform other functions. The more complex system would increase the likelihood of failures and software errors. Such a complex design, therefore, should be avoided *within the safety-related system. For example, comparison of readings from sensors in different divisions may provide useful information concerning the behavior of the sensors (for example, On-Line Monitoring). Such a function executed within a safety-related system, however, could also result in unacceptable influence of one division over another, or could involve functions not directly related to the safety-related functions, and should not be executed within the safety-related system. Receipt of information from outside the division, and the performance of functions not directly related to the safety-related function, if used, should be justified. It should be demonstrated that the added system/software complexity associated with the performance of functions not directly related to the safety-related function and with the receipt of information in support of those functions does not significantly increase the likelihood of software specification or coding errors, including errors that would affect more than one division. The applicant should justify the definition of "significantly" used in the demonstration.*

PS conformance:

The PS performs only safety-related functions. Each PS division receives information, via data communication, from three external sources. In these three cases, the information supports performance of the required safety functions:

1. Permissive validation/inhibition and ESFAS actuation output signal reset from PICS.

   The ability to validate/inhibit permissives is required to support the PS safety-related functions. The permissives are validated or inhibited to enable PS functions when they are required, and to disable PS functions when they are not required. The ability to reset ESFAS actuation outputs is required to allow manual control of actuators in transitioning to the safe shutdown state following mitigation of a design basis event.

2. Service requests from the PS SU.

   Service requests support safety-related functions because they verify that the correct software and parameter values are used in safety-related functions. Staff Position 10 describes measures implemented to prevent adverse influence on the safety-related functions through the SU interface.

3. SPND measurements and partial trigger signals from other PS divisions.

   To address transients leading to an asymmetrical power distribution, the 72 SPND measurements representing a complete flux mapping of the core are required for processing in each PS division. The 18 SPND measurements initially acquired in each division are transmitted to the other divisions.

   Partial trigger signals are required from other PS divisions to verify that protective functions are performed despite single failures. Each division of the PS independently performs monitoring of plant conditions. If plant conditions require a protective action, each division will issue a partial trigger signal to the other divisions. Each division then performs voting logic (e.g., two out of four) on the partial triggers from the four divisions. The failure of one division to issue a partial trigger does not prevent the protective action from occurring.

SAS conformance:

The SAS contains logic required only for safety-related functions. Each SAS division receives information, via data communication, from three sources outside its safety-related division. In these three cases, the information supports performance of the required safety-related functions:

1. Manual control commands for safety-related actuators from the PICS.

   Manual control of safety-related actuators is required to reach the safe shutdown state following mitigation of a design basis event. This functionality cannot be solely automatic because the operator needs to take different actions for different scenarios as dictated by procedures.

2. Service requests from the SAS SU.

   Service requests support safety-related functions because they verify that the correct software and parameter values are used in safety-related functions. Staff Position 10 describes measures implemented to prevent adverse influence on the safety-related functions through the SU interface.

3. Sensor measurements from other SAS divisions.

   Sensor measurements are required from other SAS divisions to verify that safety-related functions are performed despite single failures. When multiple SAS divisions acquire redundant sensors, that information is transmitted to the division that needs to take a control action. The signal selection logic used in each SAS division verifies that an erroneous measurement caused by a single failure in another division is not used as a basis for the SAS control action.

SICS conformance:

The safety-related portion of the SICS performs only safety-related functions. Each SICS division receives information, via data communication, from two external sources. In both cases, the information supports performance of the required safety-related functions.

1. Service requests from the SICS SUs.

   Service requests support safety-related functions because they verify that the correct software and parameter values are used in safety-related functions. Staff Position 10 describes measures implemented to prevent adverse influence on the safety-related functions through the SU interface.

2. Sensor measurements from other SICS divisions.

   Redundant divisional information is required from other SICS divisions to verify that correct information is displayed to the operator despite single failures. Each SICS division receives redundant divisional information from the other SICS divisions for processing and display to the operator. The signal selection logic in each SICS division verifies that erroneous information caused by a single failure in another division does not result in inaccurate information displayed to the operator

Staff Position 4:

The communication process itself should be carried out by a communications processor separate from the processor that executes the safety-related function, so that communications errors and malfunctions will not interfere with the execution of the safety-related function. The communication and function processors should operate asynchronously, sharing information only by means of dual-ported memory or some other shared memory resource that is dedicated exclusively to this exchange of information. The function processor, the communications processor, and the shared memory, along with all supporting circuits and software, are all considered to be safety-related, and must be designed, qualified, fabricated, etc., in accordance with 10 C.F.R. Part 50, Appendix A and B. Access to the shared memory should be controlled in such a manner that the function processor has priority access to the shared memory to complete the safety-related function in a deterministic manner. For example, if the communication processor is accessing the shared memory at a time when the function processor needs to access it, the function processor should gain access within a timeframe that does not impact the loop cycle time assumed in the plant safety analyses. If the shared memory cannot support unrestricted simultaneous access by both processors, then the access controls should be configured such that the function processor always has precedence. The safety-related function

circuits and program logic should ensure that the safety-related function will be performed within the timeframe established in the safety analysis, and will be completed successfully without data from the shared memory in the event that the function processor is unable to gain access to the shared memory.

U.S. EPR Conformance:

The safety-related I&C systems use separate communication processors and safety-related function processors. The two processors operate asynchronously and share information through dual-ported random access memory (DPRAM). The safety-related function processors operate autonomously, and their processing is not compromised by communication activities. These devices are qualified for use in safety-related applications.

Technical Report ANP-10309(P), Sections 11 and 12 provide further detail on the communication techniques employed by PS processors. The descriptions in Technical Report ANP-10309(P), Sections 11 and 12 are applicable to the SAS processors. The SICS interdivisional communication is performed at the PI level. The descriptions in Technical Report ANP-10309(P) Sections 11 and 12 are also applicable to the SICS PIs.

Staff Position 5:

The cycle time for the safety-related function processor should be determined in consideration of the longest possible completion time for each access to the shared memory. This longest-possible completion time should include the response time of the memory itself and of the circuits associated with it, and should also include the longest possible delay in access to the memory by the function processor assuming worst-case conditions for the transfer of access from the communications processor to the function processor. Failure of the system to meet the limiting cycle time should be detected and alarmed.

U.S. EPR conformance:

To meet the requirements for deterministic system behavior with guaranteed maximum computing and reaction times and constant communication loads, each safety-related processor executes its assigned function cyclically with a predefined cycle time. This is a fundamental design feature of the safety-related processors used in the U.S. EPR.

Each function processor has a cycle time parameter that determines its rate of processing. The cycle time parameter is specified based on required processing load and required response times for its functions. Response time calculations consider the qualified response time of the components in the communication path and the asynchronous behavior of the qualified processors in the signal path. Worst-case processor and communication network loadings are assumed in the calculations.

At the beginning of a processing cycle, a local cycle counter is incremented and a watchdog timer is started. If the processing cycle does not reach completion in the expected amount of time, the watchdog timer expires and puts the processor into a predefined fault state. Indication of this occurrence is provided by other processors on the network that recognize a loss of communication with the failed processor. This indication is provided consistent with requirements for bypassed/inoperable status indications.

Staff Position 6:

The safety-related function processor should perform no communication handshaking and should not accept interrupts from outside its own safety-related division.

U.S. EPR conformance:

The communication protocols used by the safety-related I&C systems do not include acknowledgements by the receiving safety-related function processor. Teleperm XS (TXS)-based safety-related function processors are not interrupted by communications. (See Staff Position #4 on the use of DPRAM in processor communications.)

Staff Position 7:

Only predefined data sets should be used by the receiving system. Unrecognized messages and data should be identified and dispositioned by the receiving system in accordance with the pre-specified design requirements. Data from unrecognized messages must not be used within the safety-related logic executed by the safety-related function processor. Message format and protocol should be pre-determined. Every message should have the same message field structure and sequence, including message identification, status information, data bits, etc. in the same locations in every message. Every datum should be included in every transmit cycle, whether it has changed since the previous transmission or not, to ensure deterministic system behavior.

U.S. EPR conformance:

Communications performed by the safety-related I&C systems use predefined messages. These predefined messages are exclusively in standard formats. The validity of a message is checked by the receiver prior to acceptance. Unrecognized or invalid messages and data within recognized messages that are marked “faulty” are excluded from use in function processing. Data messages of the same length and structure are generated every processor cycle, whether individual datum in the message have changed or not.

Staff Position 8:

Data exchanged between redundant safety-related divisions or between safety-related and non-safety divisions should be processed in a manner that does not adversely affect the safety-related function of the sending divisions, the receiving divisions, or any other independent divisions.

U.S. EPR conformance:

Data exchanged between redundant safety-related divisions and between safety- and non-safety-related divisions does not adversely affect performance of safety-related functions. This is demonstrated by the communication features and requirements described in this response.

Staff Position 9:

Incoming message data should be stored in fixed predetermined locations in the shared memory and in the memory associated with the function processor. These memory locations should not be used for any other purpose. The memory locations should be allocated such that input data and output data are segregated from each other in separate memory devices or in separate pre-specified physical areas within a memory device.

U.S. EPR conformance:

In the safety-related I&C systems, DPRAM locations for storing incoming messages are predefined during application software generation. Separate, fixed memory locations are used for input (receive) and output (send) messages.

Staff Position 10:

Safety-related division software should be protected from alteration while the safety-related division is in operation. On-line changes to safety-related system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants, setpoints, parameters, and other settings associated with a safety-related function only by way of the dual-processor / shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time. The restriction should be by means of physical cable disconnect, or by means of keylock switch that either physically opens the data transmission circuit or interrupts the connection by means of hardwired logic. "Hardwired logic" as used here refers to circuitry that physically interrupts the flow of information, such as an electronic AND gate circuit (that does not use software or firmware) with one input controlled by the hardware switch and the other connected to the information source: the information appears at the output of the gate only when the switch is in a position that applies a "TRUE" or "1" at the input to which it is connected. Provisions that rely on software to effect the disconnection are not acceptable. It is noted that software may be used in the safety-related system or in the workstation to accommodate the effects of the open circuit or for status logging or other purposes.

U.S. EPR conformance:

Each safety-related function processor in the SAS, PS, and PIs of the SICS uses a combination of hardware and software features to control access to the processors. A mechanical keyswitch for each processor does not interrupt the signal path physically, but does via software. A safety-related processor receiving a SU command to change a parameter must have a "change enable" command input via keyswitch before it will consider the command as valid. The software access controls reside within the safety-related processor. Access is provided via the SU, which connects to the safety-related processors through the MSI. The SU is always connected to the MSI to provide monitoring and to support constant busload operation. Administrative controls are used to limit access to one division at a time during plant operation. The standard TXS SU interface has been reviewed (including source code reviews) and accepted by the NRC staff. AREVA NP document 51-9118047-000, "TELEPERM XS Cyber Security Features" was submitted to the NRC by letter on August 14, 2009, to support review of Topical Report ANP-10272, "Software Program

Manual for TELEPERM XS Safety Systems." Appendix A to 51-9118047-000 describes the results of the NRC staff review of the TXS SU interface.

SU access to the safety-related QDS processors used in the SICS is controlled via mechanical keyswitch. The keyswitch physically interrupts the signal path, and is open while the QDS is in operation. Administrative controls limit access to one division at a time during plant operation.

Staff Position 11:

Provisions for interdivisional communication should explicitly preclude the ability to send software instructions to a safety-related function processor unless all safety-related functions associated with that processor are either bypassed or otherwise not in service. The progress of a safety-related function processor through its instruction sequence should not be affected by any message from outside its division. For example, a received message should not be able to direct the processor to execute a subroutine or branch to a new instruction sequence.

U.S. EPR conformance:

In the safety-related I&C systems, the data messages are received and sent as part of the deterministic processing cycle and do not affect or alter the progress of safety-related function processors through their predefined sequences.

Service request messages are used to send software instructions to the safety-related function processors. These messages are processed only after the safety-related function logic processing is complete and are terminated at the end of each processing cycle. Service request messages are sent from the SU and do not interrupt the safety-related function processor as discussed under Staff Position 10.

Staff Position 12:

Communication faults should not adversely affect the performance of required safety-related functions in any way. Faults, including communication faults, originating in non-safety equipment, do not constitute "single failures" as described in the single failure criterion of 10 C.F.R. Part 50, Appendix A. Examples of credible communication faults include, but are not limited to, the following:

12.1. Messages may be corrupted due to errors in communications processors, errors introduced in buffer interfaces, errors introduced in the transmission media, or from interference or electrical noise.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Messages are checked for correct cyclic redundancy checks (CRC), addressing length and content. Analog values contained in messages receive a not-a-number check.
- If corruption results in invalid addressing, the computers on the network mark the message as faulty.

- If corruption results in invalid message length, the computers on the network mark the message as faulty.
- If corruption results in incorrect content, the individual signals in the message are marked as faulty before being used in processing.

12.2. Messages may be repeated at an incorrect point in time.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Each time a message is sent from the same processor, a value is incremented and attached to the message. The receiving processor uses this information to determine message age.
- Messages are not repeated. New messages with an incremented message age are generated every cycle.
- If a failure results in a message being spuriously repeated, the computers on the network recognize from the message age that the message is old, and the message is marked faulty.

12.3. Messages may be sent in the incorrect sequence.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Processors receive one command message per cycle. No additional commands are accepted until the current command is finished processing.
- New messages with incremented message age are generated every cycle. If a message is received with a message age out of sequence, it is marked as faulty.
- Information within a message that is not in the correct place or sequence is detected by the receiving computer (CRC check), and the message is marked as faulty.

12.4. Messages may be lost, which includes both failures to receive an uncorrupted message or to acknowledge receipt of a message.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Messages are checked for age when they are received.
- One message is allowed to be missed. If the message age indicates that two or more messages have been missed, a fault is indicated.
- Communication techniques do not rely on the receiving processor to acknowledge receipt of messages.

12.5. Messages may be delayed beyond their permitted arrival time window for several reasons, including errors in the transmission medium, congested transmission lines, interference, or by delay in sending buffered messages.

The following techniques are used by safety-related processors in the U.S. EPR design to mitigate this failure type:

- Messages are checked for age when they are received, and old messages are marked as faulty.
- There is no “permitted arrival time window” associated with the communication techniques. The processor accesses the most recent message received once every clock cycle, whether a new message has been received or not.

12.6. Messages may be inserted into the communication medium from unexpected or unknown sources.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Messages contain information about the sender and receiver location.
- The information identifying sender and receiver locations is predefined at code generation.
- Messages from unexpected or unknown sources are marked as faulty.

12.7. Messages may be sent to the wrong destination, which could treat the message as a valid message.

The following techniques are used by safety-related processors in the U.S. EPR design to mitigate this failure type:

- Messages contain information about the sender and receiver location.
- The information identifying sender and receiver locations is predefined at code generation.
- Only messages addressed to the receiver are used, and other messages are marked as faulty.

12.8. Messages may be longer than the receiving buffer, resulting in buffer overflow and memory corruption.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Messages are a predetermined, fixed length.
- Messages contain information indicating the proper message length.
- Messages of incorrect length are marked as faulty.

12.9. Messages may contain data that is outside the expected range.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- The individual data within a message are validated by CRC check.
- Analog data contained within a message receive a “not-a-number” check.
- Range checking is performed on analog input values. If the value is outside a predefined acceptable range, it is marked faulty.

12.10. Messages may appear valid, but data may be placed in incorrect locations within the message.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Messages use standard frames, and messages that do not conform are marked as faulty.
- The receiving processor detects this type of individual bit error by CRC check.

12.11. Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm).

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Each processor operates with a deterministic cycle.
- Each message is generated and sent every cycle to provide a constant bus load.
- Each processor obtains one set of messages from the input DPRAM each cycle, independently of the sending operation.
- Postulated communication events that overload an interdivisional connection to the point of failure will result in the loss of data transfer on the affected network. As described under Staff Position 1, the safety-related function processors are not dependent on information from a single source outside their division.
- The MSI acts as a qualified communication barrier with the non-safety-related systems. It only accepts and transmits one set of messages each cycle, using the same deterministic processing cycle. This protects the safety-related function processors from communication events outside their safety-related system. Loss of communication with either the SU or gateway does not impair performance of the safety-related functions.

12.12. Message headers or addresses may be corrupted.

The following techniques are used by safety-related processors in the U.S. EPR to mitigate this failure type:

- Message headers, including addresses, are checked for validity when received.
- Addresses are predefined at code generation, and messages with invalid addresses are marked as faulty.

Staff Position 13:

Vital communications, such as the sharing of channel trip decisions for the purpose of voting, should include provisions for ensuring that received messages are correct and are correctly understood. Such communications should employ error-detecting or error-correcting coding along with means for dealing with corrupt, invalid, untimely, or otherwise questionable data. The effectiveness of error detection/correction should be demonstrated in the design and proof testing of the associated codes, but once demonstrated is not subject to periodic testing. Error-correcting methods, if used, should be shown to always

reconstruct the original message exactly or to designate the message as unrecoverable. None of this activity should affect the operation of the safety-function processor.

U.S. EPR conformance:

Interdivisional data communication messages are checked for message authenticity, validity, and age. Analog data within a message undergoes a not-a-number check. The message checking is performed as part of the normal cyclic operation of the processors and does not adversely impact the operation of the safety-related function processors. Faulty messages are identified and marked. The safety-related systems use fault accommodation techniques (i.e., voting logic, signal selection logic) to properly handle data contained in messages identified as faulty. No error correcting methods are used.

Staff Position 14:

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 or receiving node. Implementation of other communication strategies should provide the same reliability and should be justified.

U.S. EPR conformance:

Vital communications between divisions in the safety-related I&C systems utilize point-to-point topologies with the following two exceptions:

- Remote acquisition units (RAU) – acquisition and processing units (APU) networks in the PS.
- Subsystem A APU – ALU networks in the PS.

These networks utilize TXS ring topology networks and are shown on Technical Report ANP-10309(P), Figures 6-4 through 6-12. Based on discussions during the January 26, 2010 NRC staff audit of U.S. EPR I&C, AREVA NP understands that the APU-ALU ring networks are not problematic because they each span two PS divisions. In this response, AREVA NP will address only the RAU-APU networks, which span the four PS divisions.

The RAU-APU ring networks have been the subject of questions that were issued and responded to during the review of Topical Report ANP-10281(P), "U.S. EPR Digital Protection System." ANP-10281(P) has been withdrawn and replaced with Technical Report ANP-10309(P)." AREVA NP understands that the RAI responses regarding the withdrawn topical report contain an adequate basis and justification for use of the ring networks, but can no longer be referenced by the NRC staff in a Safety Evaluation Report (SER). The following information is provided as attachments to this response:

- ANP-10281Q2P, "Response to Second Request for Additional Information ANP-10281(P)," RAI 30 and Response to RAI 30 (Attachment A to this response).
- ANP-10281Q3P, "Response to Third Request for Additional Information ANP-10281(P)," RAI 37 and Response to RAI 37 (Attachment A to this response).

- ANP-10281Q3P, "Response to Third Request for Additional Information ANP-10281(P)," RAI 38 and Response to RAI 38 (Attachment A to this response).
- " Supplemental Information for the Digital Protection System Topical Report (ANP-10281P)", transmitted via email from Russell Wells to Getachew Tesfaye, Aug. 15, 2008 (Attachment B to this response).

These attachments provide basis and justification for use of the RAU – APU ring networks, discuss failure modes and mitigation, and address communication independence.

Staff Position 15:

Communication for safety-related functions should communicate a fixed set of data (called the "state") at regular intervals, whether data in the set has changed or not.

U.S. EPR conformance:

Data communication between divisions of the I&C safety-related systems consists of fixed data sets each cycle whether data in the set has changed or not. The data sets are predefined during application software generation.

Staff Position 16:

Network connectivity, liveness, and real-time properties essential to the safety-related application should be verified in the protocol. Liveness, in particular, is taken to mean that no connection to any network outside the division can cause an RPS/ESFAS communication protocol to stall, either deadlock or livelock. (Note: This is also required by the independence criteria of: (1) 10 C.F.R. Part 50, Appendix A, General Design Criteria ("GDC") 24, which states, "interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."; and (2) IEEE 603-1991 IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations.) (Source: NUREG/CR-6082, 3.4.3)

U.S. EPR conformance:

The I&C safety-related systems monitor communication processing. Liveness of the communications connectivity is determined by monitoring message age. Communication processors are used to separate the communication functions from the safety-related function processors so that failures on a given network do not affect the operation of a safety-related function processor. Isolation provided by the MSI prevents failures on a non-safety-related network from affecting the communication activities within the safety-related system.

Staff Position 17:

Pursuant to 10 C.F.R. § 50.49, the medium used in a vital communications channel should be qualified for the anticipated normal and post-accident environments. For example, some optical fibers and components may be subject to gradual degradation as a result of prolonged exposure to radiation or to heat. In addition, new digital systems may need

susceptibility testing for EMI/RFI and power surges, if the environments are significant to the equipment being qualified.

U.S. EPR conformance:

Communications equipment in the I&C safety-related systems is qualified for anticipated normal and post-accident environments. U.S. EPR FSAR Tier 1, Sections 2.4.1, 2.4.2, and 2.4.4 contain ITAAC to verify the environmental qualification of the equipment in the I&C safety-related systems.

Staff Position 18:

Provisions for communications should be analyzed for hazards and performance deficits posed by unneeded functionality and complication.

U.S. EPR conformance:

The TXS communication protocol used for data communication between safety-related divisions is standardized as part of the qualified TXS platform. This standardization precludes added complexity or unnecessary communication functionality from being introduced during the application-specific design of a system using the TXS platform. The SPACE tool code generators automatically generate data messages and configuration data for each processing module, which includes the set of function diagram group modules to be processed, the cycle time, the list of messages and communication channels, and the list of input/output modules to be used.

Staff Position 19:

If data rates exceed the capacity of a communications link or the ability of nodes to handle traffic, the system will suffer congestion. All links and nodes should have sufficient capacity to support all functions. The applicant should identify the true data rate, including overhead, to ensure that communication bandwidth is sufficient to ensure proper performance of all safety-related functions. Communications throughput thresholds and safety-related system sensitivity to communications throughput issues should be confirmed by testing.

U.S. EPR conformance:

Safety-related I&C systems are designed to operate with a constant bus load for communications between safety-related divisions. This is achieved through the cyclic nature of the communications, a token-passing protocol that allows only one processor to send information to the network at a time and through the continuous messaging with the SU. Response time testing is used to verify that adequate throughput exists for the safety-related systems to satisfy their performance requirements.

Staff Position 20:

The safety-related system response time calculations should assume a data error rate that is greater than or equal to the design basis error rate and is supported by the error rate observed in design and qualification testing.

U.S. EPR conformance:

Response time calculations account for the qualified response times of the components in a communication path, as well as the asynchronous behavior of qualified processors in a signal path. Response time testing is performed to verify that as-built system performance is consistent with the calculated response times. Attachment C to this response describes the methodology to perform response time calculations for the U.S. EPR protection system (PS).

FSAR Impact:

U.S. EPR FSAR Tier 1, Section 2.4.1, Section 2.4.2, and Section 2.4.4 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR FSAR Tier 2, Section 7.1 will be revised as described in the response and indicated on the enclosed markup.

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:

AREVA NP believes that the application for design certification of the U.S. EPR complies with 10 CFR 52.47(a)(22). NUREG-0800, Chapter 1.0, Section I.9 states the following as acceptance criteria for compliance with 10 CFR 52.47(a)(22):

> "Information from the applicant that demonstrates how operating experience insights from generic letters and bulletins issued after the most recent revision of the applicable standard review plan and 6 months before the docket date of the application, or comparable international operating experience, have been incorporated into the plant design is reviewed."

10 CFR 52.47(a)(22) does not require applicants for design certification to address disposition of NRC Information Notices in the application. U.S. EPR FSAR Tier 2, Section 1.9.4 addresses compliance with 10 CFR 52.47(a)(22).

Sound engineering and design practices will be applied to development of the U.S. EPR plant data network and the instrumentation and controls (I&C) systems connected to the network. The plant data network will be designed to withstand data traffic, and the interfacing I&C systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the network. Specific design details regarding preclusion of data storm events on a non-safety-related network will be developed later in the design process, and are thus not planned for inclusion in the application for design certification.

AREVA NP believes that identification of design features of the safety-related I&C systems that protect the safety-related functions in case of data storm events on the non-safety-related plant data network is appropriate for design certification. See the Response to Question 07.09-46 for more information.

FSAR Impact:

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

Attachment A

the APUs and/or ALUs of the protection system. For these functions, the manual initiation is combined with the automatic initiation logic so that the manual function is subject to the same operating bypasses as the automatic function.

The manual initiations of protective actions that are not processed by the APUs and/or ALUs (i.e., wired directly to PAC modules) are not subject to operating bypasses.

The statements in PS TR Sections 14.26 and 14.27 are true for both automatic and manual functions processed by the PS. PS TR Sections 14.33 and 14.34 have been deleted from the PS TR as part of the response to RAI 1.

***RAI 30**: Please describe how the redundant ring network topology is immune to single failures.*

Section 6.1.2 says: "In this topology, a break in one of the double fiber optical connections, or a failure in one optical port of one OLM, does not affect network availability. If an OLM is lost, only the unit(s) directly connected to the failed OLM is affected." However, these are not the only failure modes that are possible in a network (e.g NRC Information Notice 2007-15). Please describe, or provide a reference, to a description of the possible failure modes in: 1) a profibus network, and 2) in a token ring network. How are each of these failure modes addressed by the AREVA design? Will this information be in the Failure Modes and Affects Analysis (FMEA)?

Response 30:

Section 6.1.2 of the PS TR does not claim that a redundant ring network is immune to single failures. Section 6.1.2 describes the features of the network topology that accommodate specific failures. These features add to overall system reliability.

A single redundant ring network, as used in the U.S. EPR PS architecture, is not required to demonstrate single failure tolerance. Single failure tolerance is required of the safety function as a whole, not of any individual segment of a system that contributes to the safety function. In the case of the U.S. EPR protection system, the complete loss of function of any single network within the system does not prevent the performance of any safety function by the system. The remaining portions of the system are adequate to perform the functions required of the system.

Item 12 in the staff position of Reference 6 provides examples of credible communication failures. These are the communication failures that are taken into account in the U.S. EPR safety systems design.

Network failures are addressed in the system level FMEA as described in the response to RAI 24. Bounding network failures are analyzed to demonstrate single failure tolerance at the system level. The specific failures described in Reference 6 will be verified to be bounded by the system level FMEA, or will be addressed specifically, as

part of a more detailed FMEA to be performed following equipment layout and software definition.

The communication failure described in NRC Information Notice 2007-15, "Effects of Ethernet-Based, Non-Safety Related Controls on the Safe and Continued Operation of Nuclear Power Stations," corresponds to the failure in position 12 of Reference 6, "Messages may occur at a high rate that degrades or causes the system to fail (i.e., broadcast storm)."

The communications within the PS that are the subject of this RAI are not ethernet-based, nor are they non-safety related. Specific features of the TXS platform related to interchannel communication methods (described in Section 12 of the PS TR and in Section 2.9 of Reference 3) preclude this type of failure from occurring. However, if this were a credible failure mode for a redundant ring network, as implemented in the PS, it would result in the failure of only one network. The remaining portions of the PS are adequate to perform the system's safety functions.

RAI 31: *Please describe all of the types of maintenance bypasses and their associated affect on the RT or ESF functions.*

Section 14.4 says: "If one redundancy within the PS is bypassed for testing or maintenance, and a credible single failure occurs in another redundancy, the ability to perform the required protective actions is maintained." However it is not clear as to what redundancies can be bypassed, how bypassing is accomplished, or the affect of bypassing of each on system function:

1) *Each division has separate sensors, and therefore the sensors can be considered redundant to each other. Can the sensors be bypassed? How is sensor bypass accomplished, and how does the system functionality change?*

2) *The divisions can be considered redundant to each other. Can a division be bypassed? How is division bypass accomplished, and how does the system functionality change?*

3) *Each division contains racks of equipment (e.g. Remote Acquisition Units, Acquisition and Processing Units, Actuation Logic Units, Power Supplies, Gateways, ...) that could be considered to be redundant to similar units in the other divisions. Can each rack of equipment be bypassed? How is the system functionality affected by bypassing this equipment? How is the functioning of the Optical Link Modules (OLMs) associated with each bypassed rack affected?*

4) *Each division contains Optical Link Modules (OLMs) that could be considered to be redundant to each other. Can these OLMs be bypassed? How does the network and system functionality change when these modules are bypassed?*

Response to Third Request for Additional Information Regarding ANP-10281P, "U.S. EPR Digital Protection System Topical Report" (TAC NO. MD4977)

RAI-37:

Demonstrate that the U.S. EPR digital protection system (PS) design and architecture for providing self powered neutron detector (SPND) measurements between the remote acquisition units (RAU) and certain acquisition and processing units (APU) are not susceptible to single failure as required by General Design Criterion (GDC) 21 of Title 10 of the Code of Federal Regulations (CFR) 50, Appendix A.

GDC 21 states, in part, that the protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. Section 6.3 of the U.S. EPR Digital Protection System Topical Report discusses the RAU-APU architecture. This section states that the measurements from the SPNDs are required for processing by the APU within each division of the U.S. EPR digital protection system (PS). While the RAU in each division only acquires one-fourth of the SPND measurements, all 72 measurements are required by the APU in each division to accurately compute the 3-D power distribution. Therefore, communication from the RAU to the APU is established to satisfy this requirement. The RAU – APU architecture consists of five redundant ring topology networks. The first four networks each connect the RAU 1 of all four divisions to two APUs in one division. The fifth network connects the RAU 2 of the four divisions to the APU in the four divisions. Therefore, the fifth network is redundant to the first four networks collectively.

Provide information to demonstrate how GDC 21 is met. Specifically, given that when RAU1 within a division is removed from service and RAU2 within the same division has a single failure, demonstrate how the protective functions provided by the SPND measurements continue to be accomplished. Describe how many SPND measurements out of the 72 total measurements are required to complete the required protective function. In addition, provide a detailed description of the method by which the multiple measurements are used to arrive at the estimated power level and the method for determining the uncertainty in the measured power level. Include in the analyses the assumptions employed regarding the ability of the digital network to reliably acquire and transfer information, including timing considerations.

Response to RAI-37:

For clarity, the response to this question is provided in four parts.

Part 1: "…when RAU1 within a division is removed from service and RAU2 within the same division has a single failure, demonstrate how the protective functions provided by the SPND measurements continue to be accomplished."

The U.S. EPR reactor core / thermal-hydraulic analyses do not support the continued effectiveness of SPND-based RT functions with both RAU in a division unavailable. Thus, an automatic reactor trip function when seven or more SPND measurements are invalid has been

added to the U.S. EPR design. The case where both RAU in a division are unavailable results in 18 SPND measurements seen as invalid by the APUs in all four protection system (PS) divisions. This condition will now result in an automatic reactor trip (RT).

The conservative approach described provides surety that the single failure tolerance of the system as well as the assumptions used in the plant safety analyses are valid.

Part 2: "Describe how many SPND measurements out of the 72 total measurements are required to complete the required protective function.

See the response to U.S. EPR FSAR RAI 103, Question 16-195, for updated technical specifications that address the number of SPND measurements required for functional capability.

The reactor core / thermal-hydraulic analyses support the continued effectiveness of SPND-based RT functions with any combination of up to five SPND measurements unavailable. For this reason, U.S. EPR technical specifications dictate that if fewer than 67 SPND measurements are not operable, the plant must be taken to less than 10 percent reactor thermal power within 6 hours. The protective functions supported by the SPND measurements are not required below this power level. This approach is consistent with U.S. EPR FSAR Tier 2, Section 7.2.2.1.5, which states that the protection system setpoints accommodate up to five failed SPND measurements.

Further analysis may determine the feasibility of operating with fewer than 67 SPND measurements available. Pending the results of such an analysis, the conservative technical specification approach described above is employed to provide surety that the assumptions used in the plant safety analyses are valid.

Part 3: "…provide a detailed description of the method by which the multiple measurements are used to arrive at the estimated power level and the method for determining the uncertainty in the measured power level."

AREVA topical report ANP-10287P, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report" has been submitted to NRC and is currently under review. This topical report describes the algorithms using the SPND measurements and the determination of setpoint uncertainties for the high linear power density (HLPD) and low departure from nucleate boiling ratio (DNBR) reactor trip functions. The pertinent sections of ANP-10287P follow:

- Section 3.2: Functional description of DNBR RT including inputs and algorithm.
- Section 5.0: DNBR reactor trip setpoint methodology including uncertainties.
- Section 6.2: Functional description of HLPD RT including inputs and algorithm.
- Section 8.0: HLPD reactor trip setpoint methodology including uncertainties.

Part 4: "Include in the analyses the assumptions employed regarding the ability of the digital network to reliably acquire and transfer information, including timing considerations."

In March 2007, AREVA NP submitted ANP-10275P, "U.S. EPR Instrument Setpoint Methodology Topical Report" for NRC review. This topical report was approved by on the NRC in December 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 do not introduce inaccuracies beyond those described in ANP-10275P, Section 2.4.

Attachment B to the AREVA NP response to the second request for additional information regarding the Protection System Topical Report includes a detailed analysis of the response times for protection system (PS) functions, including those using SPNDs as inputs. These response times include the delays assumed due to network communication within the PS.

RAI-38:

Describe the failure modes of the ring communications network employed in the U.S. EPR digital protection system (PS) to provide self powered neutron detector measurements (SPND) between the remote acquisition units (RAU) and certain acquisition and processing units (APU) as required by General Design Criterion (GDC) 23 of 10 CFR 50, Appendix A.

GDC 23 states, in part, that the protection system shall 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." Section 6.3 of the U.S. EPR Digital Protection System Topical Report discusses the RAU-APU architecture. This section states that the measurements from the SPNDs are required for processing by the APU within each division of the PS. While the RAU in each division only acquires one-fourth of the SPND measurements, all 72 measurements are required by the APU in each division to accurately compute the 3-D power distribution. Therefore, communication from the RAU to the APU is established to satisfy this requirement. The RAU – APU architecture consists of five redundant ring topology networks. The first four networks each connect the RAU1 of all four divisions to two APUs in one division. The fifth network connects the RAU2 of the four divisions to the APU in the four divisions. Therefore, the fifth network is redundant to the first four networks collectively.

Describe how the system design of the APU can accommodate failure (e.g., loss of signal, or loss of confidence in signal) of any one of the first four ring networks (those connected to RAU1). Specifically, describe the methods used by the APU to detect the validity of the SPND measurements, and how measurements acquired from the redundant fifth network are used to provide the estimated power level.

Response to RAI-38:

[

]

Attachment B

Ring Networks – Summary of Use:

Networks arranged in ring topologies are used in the U.S. EPR protection system (PS) between the remote acquisition units (RAU) and certain acquisition and processing units (APU). Each RAU-APU ring network contains stations in each of the four PS divisions. The information transmitted over these networks is the measurement values of the self-powered neutron detectors (SPND) from the RAU to the APU; no information is sent from the APU to the RAU. The SPND measurements are used in the Low DNBR and High Linear Power Density (HLPD) reactor trip functions. Section 7.2 and Figure 7-2 of ANP-10281P (Reference 1) describe the use of these measurements in the reactor trip functions. The Low DNBR and HLPD reactor trip functions are described in further detail in Section 7.2 of the U.S. EPR FSAR (Reference 2).

The TXS ring network topology and operation is described in Section 6.0 of Reference 1. An example of a TXS ring network topology is given in Figure 6-2, and the RAU-APU ring networks are depicted in Figures 6-4, 6-5, 6-6, 6-7, and 6-8 of Reference 1.

Basis for Distribution of SPND Measurements:

DRAFT

Basis for Use of Ring Networks:

Two types of physical network topologies were considered for implementing the sharing of SPND measurements described above: Point-to-point topologies, and ring topologies. The following points are relevant when comparing the two topologies for use in this application:

- The TXS communication equipment is designed to utilize either topology; no new design work is required for either topology.
- The same communication fault detection and accommodation techniques are always used by each computer on a network, regardless of physical network topology.
- Communication independence is achieved in the same manner for either type of topology.
- Each protective function using these networks satisfies the single failure criterion with either type of topology.
- An implementation using strictly point-to-point topologies would result in 64 individual networks (each of 8 RAU with an individual network connection to each of 8 APU).
- A configuration using redundant ring topologies, that satisfies all system and functional requirements, can be implemented with five individual networks.

Given the equality of all other design aspects between the two topologies, the ring topology was chosen based on the significantly lower number of individual networks required. This design choice is consistent with the principle of simplifying the design of safety systems to the extent possible.

The two safety system requirements with primary relevance to the issue of the RAU-APU ring networks are:

DRAFT

1.) The requirement to maintain independence between redundant divisions of the protection system; specifically, communication independence.

2.) The ability of the protection system to perform its safety functions in the presence of any credible single failure.

Compliance of the protection system with these two requirements is discussed below. These discussions are focused specifically on the RAU-APU ring networks and how they support system-level compliance with the requirements.

Communication Independence:

Section 12.2 of Reference 1 describes how communication independence is achieved in a TXS-based system. The communication independence techniques described there are equally applicable to ring topologies and point to point topologies.

The TXS communication principles are such that communication independence is a function of the standard features and communication techniques employed by each individual computer on the network. The physical network topology itself is irrelevant to establishing communication independence.

This view of communication independence was presented to the NRC at the Digital Protection System Topical Report meeting on June 25, 2007 (see NRC accession numbers ML071700810 and ML070720353). The relevant presentation material from that meeting is contained in Attachment 1.

Additionally, Section 6.1.3 of Reference 1 states AREVA NP's view of communication independence:

> "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. Communication independence is addressed further in Section 12.0."

AREVA NP has responded to 36 requests for additional information (RAIs) on Reference 1. There were no RAIs regarding this view of communication independence. Therefore AREVA NP believes that the NRC understands and accepts this view, and the NRC's concern regarding the RAU-APU networks is not related to the establishment of communication independence. Therefore, the NRC's concern regarding the RAU-APU networks appears to be related to single failures and possible effects on the connected divisions.

DRAFT

Single Failure Tolerance:

Note: In the paragraphs below, and in Table 1, Reference is made to the networks depicted in Figures 6-4, 6-5, 6-6, 6-7, and 6-8 of Reference 1. These networks are referred to as networks 6-4, 6-5, 6-6, 6-7, and 6-8 respectively.

The single failure criterion is applied to the safety function as a whole, not to any smaller segment of a system that participates in the safety function. The failure modes and effects analysis (FMEA) presented in Section 7.2 of Reference 2 describes how the protection system satisfies the single failure criterion for the reactor trip function. In that FMEA, communication failures are bounded by failures of the sending or receiving equipment. Those bounding assumptions remain valid; however, to assist the NRC in reaching a conclusion regarding the acceptability of the RAU-APU networks, specific communication failures are analyzed in Table 1. For each failure, the way in which the RAU-APU arrangement accommodates the failure while maintaining the ability to perform the reactor trip function is described. The communication failures in Table 1 are those found in DI&C-ISG-04 Rev. 0 (Reference 3).

It is worth noting, separately from Table 1, that in the current design of the RAU-APU networks sufficient redundancy is present so that if any one network is completely disabled, the safety function is still performed. The following example illustrates the benefit of this redundancy:

The TXS communication protocol uses a token passing protocol to ensure that only one processor can transmit to the network at a time. The current design of the RAU-APU networks consists of five separate token rings. In case of a 'lost' token on any network, the response time of a function using that network could be affected by the time required to 'retrieve' the 'lost' token. In the U.S. EPR design, if the token is 'lost' on network 6-4, there is no effect on the communication times of the other four RAU-APU networks. In this case, network 6-8 is unaffected and can perform the function with no degradation of response time for the function as a whole. This failure mitigation strategy is applicable for any single failure that, in the worst case, results in complete loss of a network.

References:

1 ANP-10281P, Revision 0, "U.S. EPR Digital Protection System Topical Report."

2 U.S. EPR Final Safety Analysis Report, Revision 0.

3 DI&C-ISG-04, Revision 0, "Task Working Group #4: Highly-Integrated Control Rooms- Communications Issues (HICRc)," dated September 28, 2007.

DRAFT

DRAFT

DRAFT

DRAFT

DPS TR Correction

As identified in an e-mail from AREVA NP to NRC (Ronda M Pederson (AREVA NP) to Getachew Tesfaye (NRC), "RE: Quick Question for AREVA on Digital Protection System Topical Report," dated July 29, 2008), a typo was identified in Table 1-1 on page 1-3 of the Digital Protection System Topical Report. **[** Specifically, the reference to the S340 module should be S430. **]** A marked-up page to Table 1-1 is provided in Attachment 2.

DRAFT

Attachment 1

Excerpts from the Digital Protection System Topical Report Meeting Presentation on June 25, 2007 Regarding Communication Independence

DRAFT

Topical Report

Inter-Divisional Communication

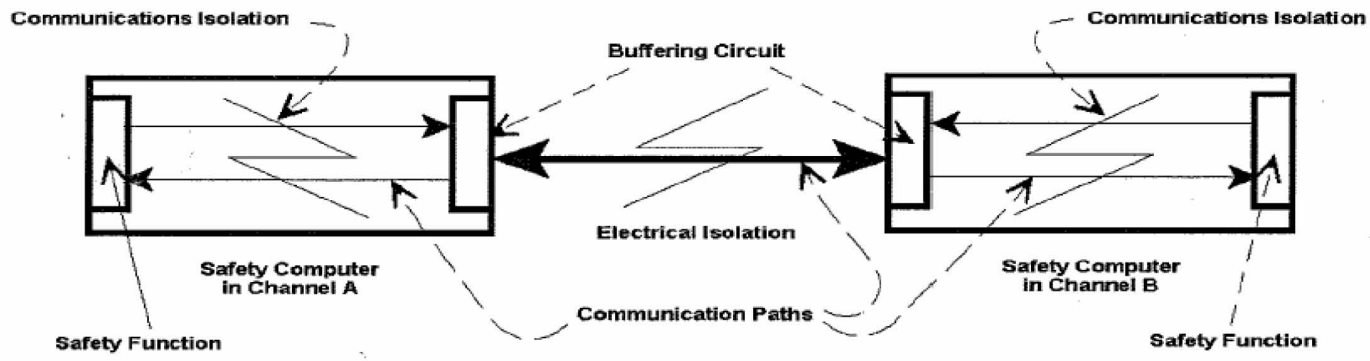
- Two basic network configurations
  - Two station token ring (redundant point to point topology)
  - More than two station token ring (redundant ring topology)
  - Independence achieved in the same manner regardless of network topology
- Electrical isolation
  - Fiber optic communication paths
- Communications isolation
  - Buffering circuits
  - Separation of data flow
  - Network communication performed independently of function computer processing

DRAFT

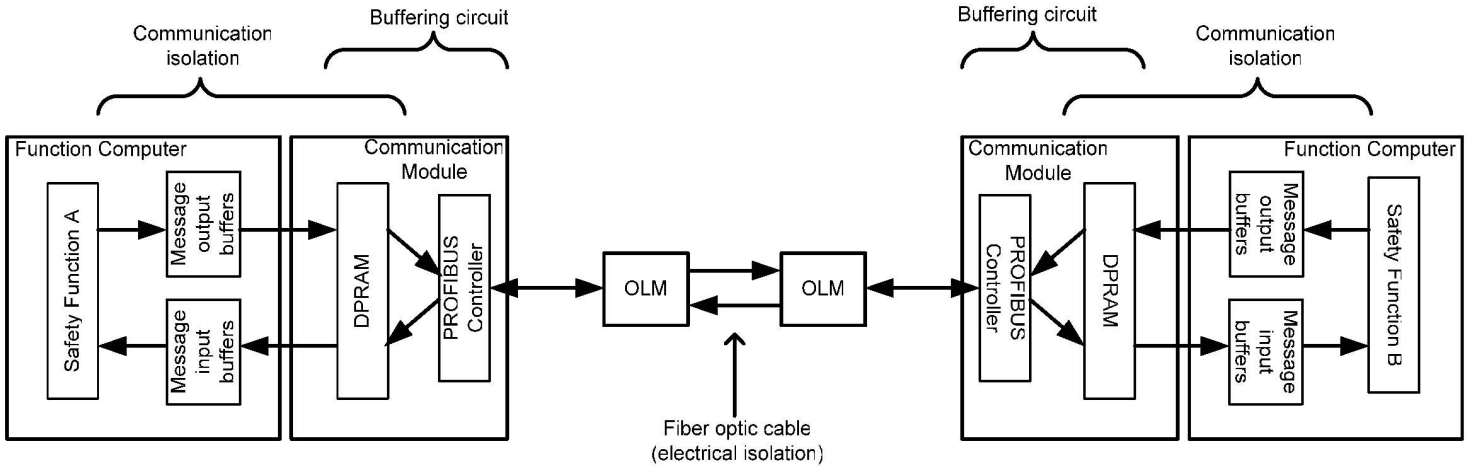
Topical Report

Inter-Divisional Communication

IEEE 7-4.3.2



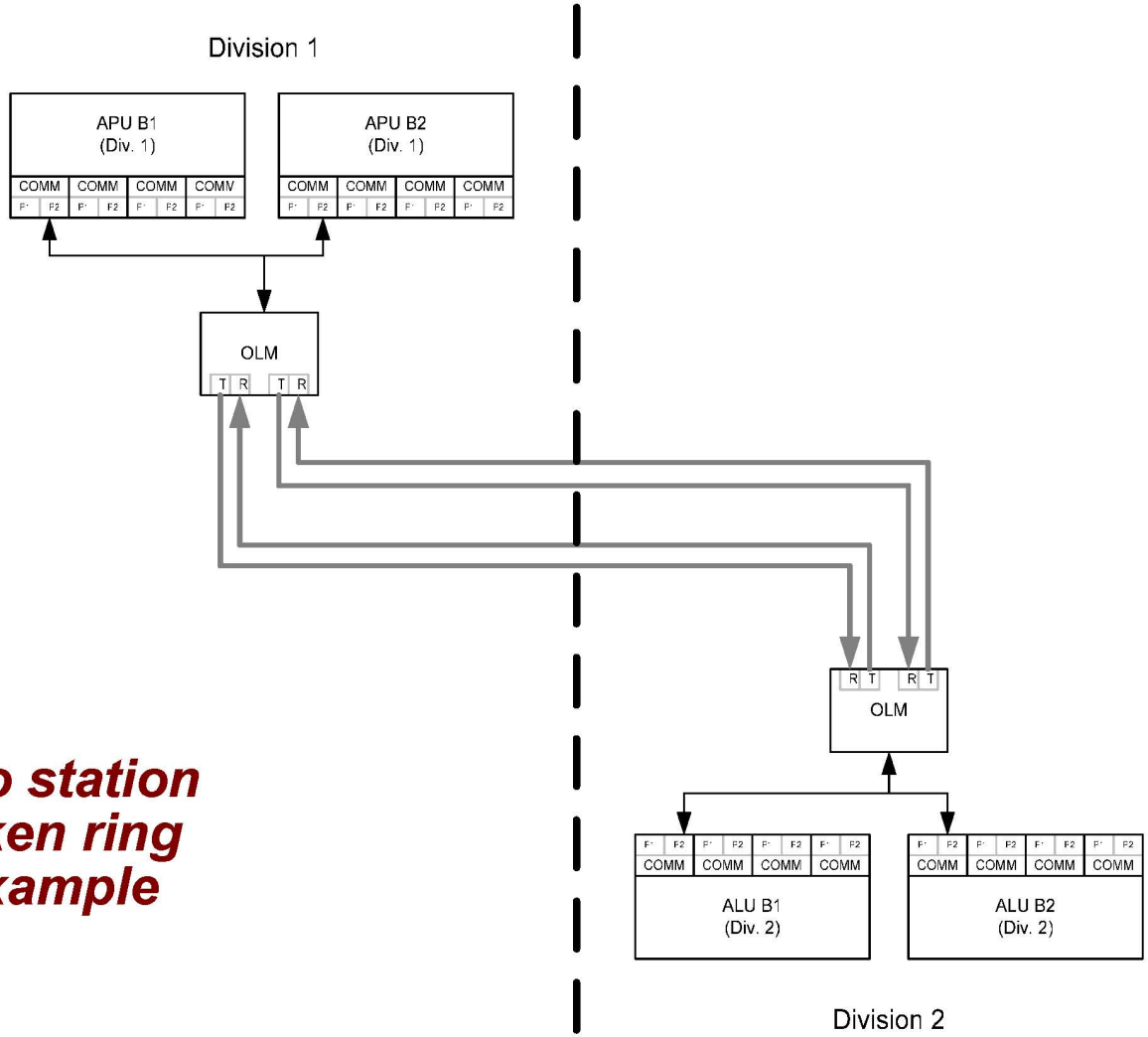
U.S. EPR



DRAFT

Topical Report

Inter-Divisional Communication

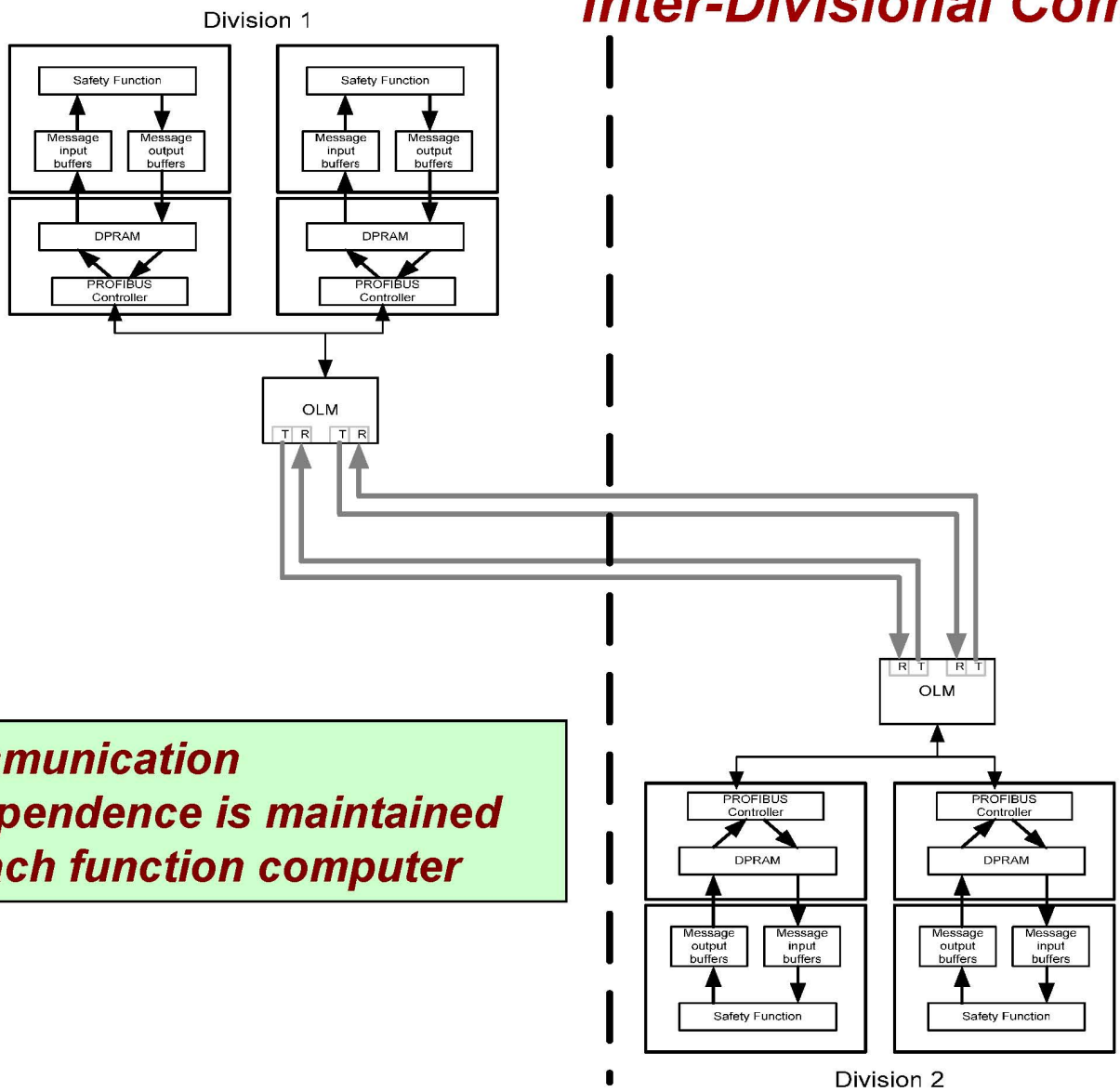


Two station token ring example

DRAFT

Topical Report

Inter-Divisional Communication



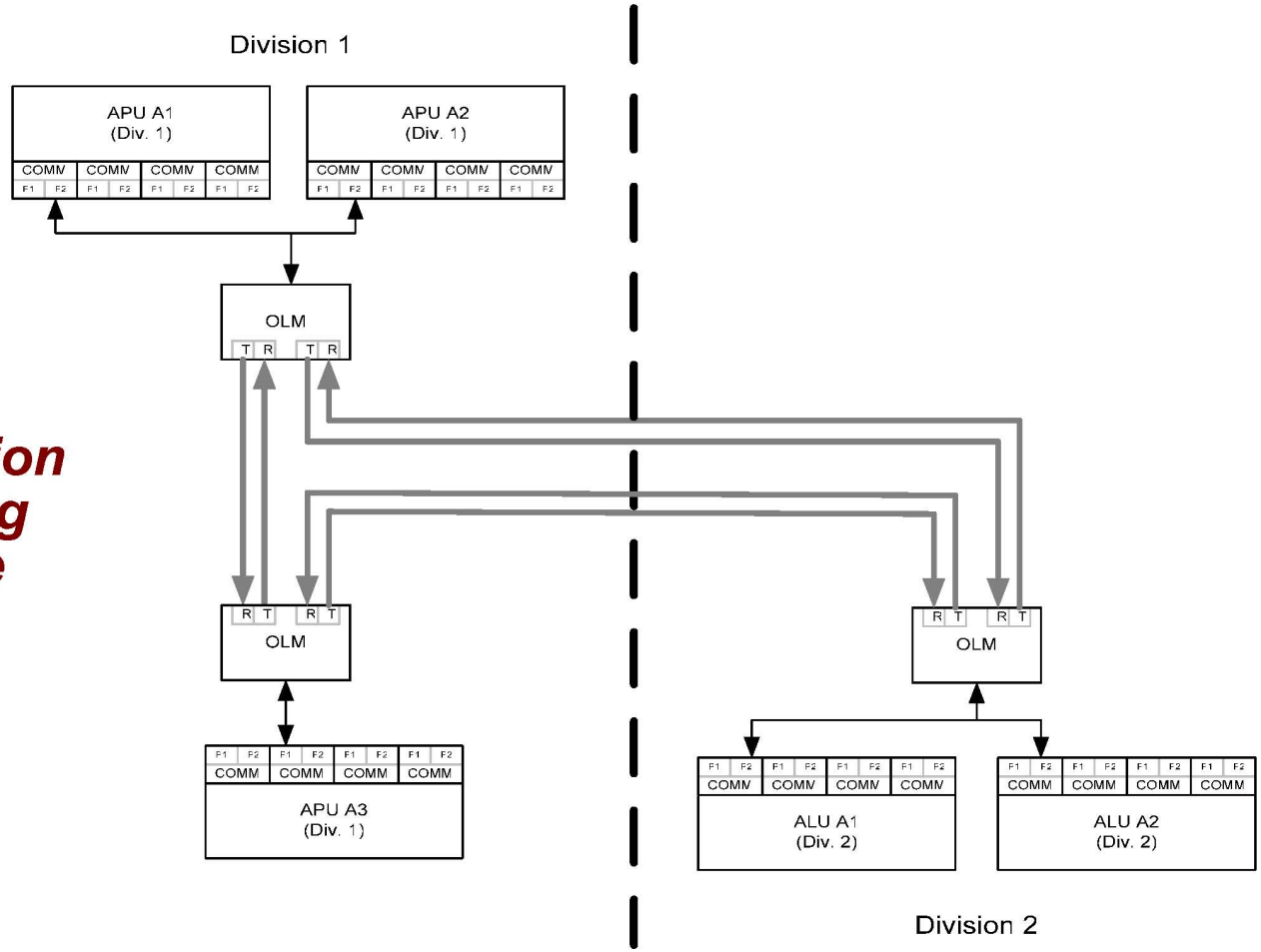
Communication independence is maintained at each function computer

DRAFT

Topical Report

Inter-Divisional Communication

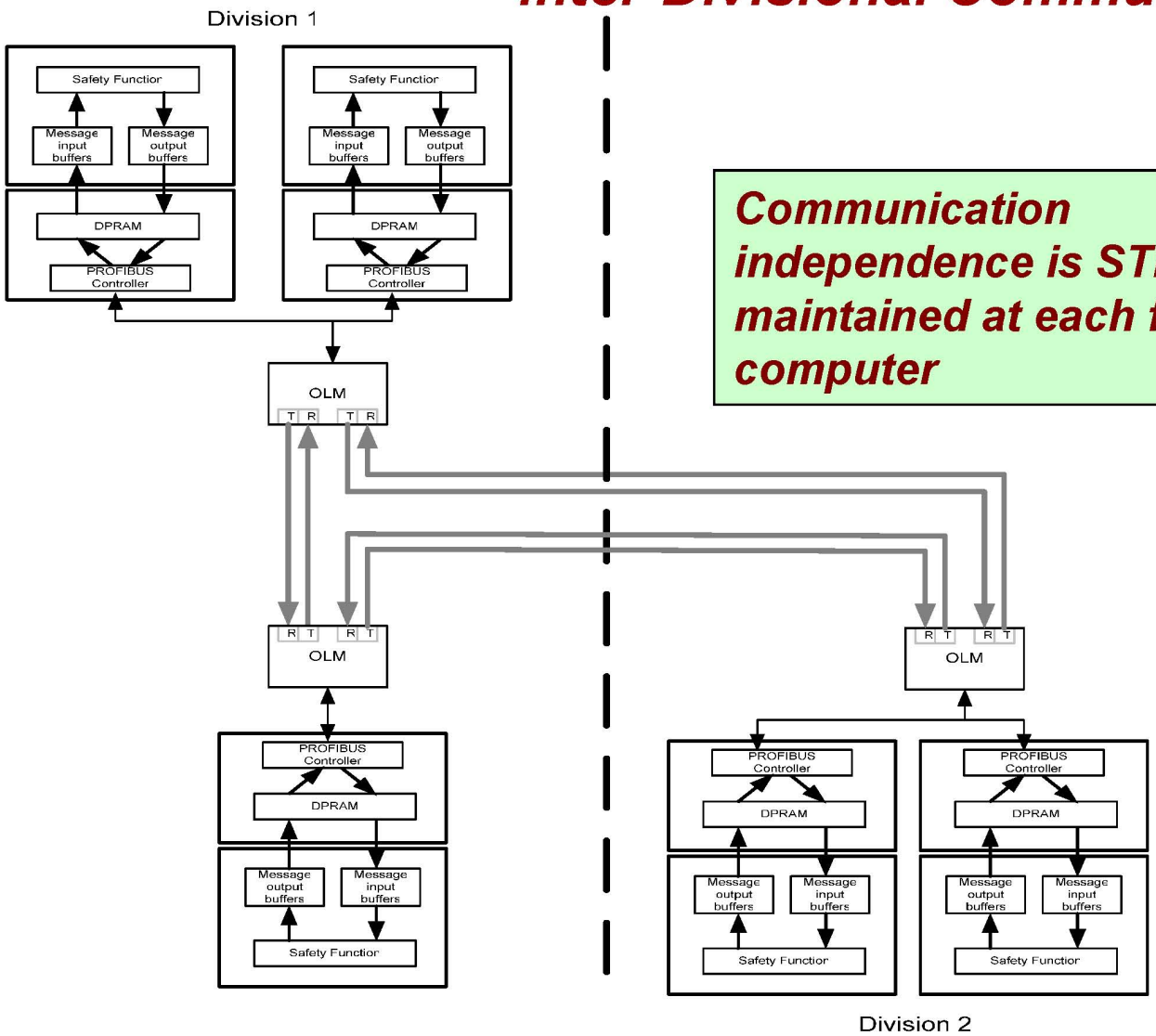
Three station token ring example



DRAFT

Topical Report

Inter-Divisional Communication



Communication independence is STILL maintained at each function computer

Attachment C

Additional Information in Support of a Request for Additional Information – ANP-10281P, "U.S. EPR Digital Protection System" (TAC No. MD4977)

In the response to RAI 4 (see Reference 4 of the cover letter), AREVA NP stated that supporting documentation would be provided to the NRC detailing the allocation of time delays to the computerized portion of the PS. This information is provided below.

Scope of Digital Response Time Allocation

TELEPERM XS Timing Concepts

Limiting Response Time

Acquisition of an Input Signal (Time Fragment <1>)

Processing Within one FDG (Time Fragment <2>)

Signal Exchange between FDGs within the Same Processor (Time Fragment <3>)

Signal Exchange between Function Processors over a Network Link (Time Fragment <4>)

Generation of an Output Signal (Time Fragment <5>)

Timing Assumptions

Function Type 1: Typical Function not Using APU A3

Function Type 2: Typical Function Using APU A3

Function Type 3: Three Level Function not Using APU A3

Function Type 4: Three Level Function Using APU A3

Function Type 5: Special Case for Low DNBR Reactor Trip Function

Figure B-1

Figure B-2

Figure B-3

Figure B-4

[ ]

Figure B-5

[ ]

Figure B-6

[ ]

Figure B-7

[ ]

Figure B-8

Figure B-9

Figure B-10

Figure B-11

Figure B-12

U.S. EPR Final Safety Analysis Report Markups

2.4 Instrumentation and Control Systems

2.4.1 Protection System

1.0 Description

The protection system (PS) is provided to sense conditions requiring protective action and automatically initiate the safety systems required to mitigate the event.

The PS provides the following safety related functions:

- Performs automatic initiation of reactor trip (RT) functions.
- Performs automatic initiation of engineered safety feature (ESF) functions.
- Provides for manual initiation of RT functions.
- Provides for manual actuation of ESF functions.
- Generates permissive signals that authorize the activation or deactivation of certain protective actions according to current plant conditions.
- Generates permissive signals that maintain safety related interlocks.

2.0 Arrangement

2.1 ~~The location of the safety related~~ PS equipment is located as listed in Table 2.4.1-1—Protection System Equipment.

2.2 Physical separation exists between the four divisions of the PS.

07.09-46

2.3 Physical separation exists between Class 1E PS equipment and non-Class 1E equipment.

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.

4.0 I&C Design Features, Displays and Controls

4.1 The PS generates ~~an~~ automatic RT signals. ~~for each of the parameters identified in Table 2.4.1-3—Protection System Automatic Reactor Trips.~~

4.2 The PS generates automatic~~ally~~ ~~actuated engineered safety feature~~ESF signals.~~, as identified in Table 2.4.1-4—Protection System Automatically Actuated Engineered Safety Features.~~

4.3 ~~The PS~~The permissives provide~~s~~ operating bypass~~es~~ capability for the corresponding PS functions. ~~identified in Table 2.4.1-6—Protection System Operating Bypasses.~~

Table 2.4.1-79—Protection System ITAAC (5 12 Sheets)

07.09-46

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	PS equipment is located as listed in Table 2.4.1-1.	Inspections will be performed of the location of the PS equipment.	The PS equipment listed in Table 2.4.1-1 is located as listed in Table 2.4.1-1.
2.2	Physical separation exists between the four divisions of the PS.	Inspections will be performed to verify that the divisions of the PS are located in separate safeguard buildings	The four divisions of the PS are located in separate safeguard buildings.
2.3	Physical separation exists between Class 1E PS equipment and non-Class 1E equipment.	a. Design analyses will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E PS equipment and non-Class 1E equipment. b. Inspections will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E PS equipment and non-Class 1E equipment.	a. A report exists and defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E PS equipment and non-Class 1E equipment. b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E PS equipment and non-Class 1E equipment. Reconciliation is performed of any deviations to the design.
3.1	Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment listed as Seismic Category I in Table 2.4.1-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements.	a. Tests/analysis reports exist and conclude that the equipment listed as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.

2.4.2 Safety Information and Control System

1.0 Description

The safety information and control system (SICS) provides the human-machine interface (HMI) means to perform control and information functions needed to monitor the plant safety status and bring the unit to and maintain it in a safe shutdown state in case of the inoperability of the process information and control system (PICS).

In case of the unavailability of the PICS, the SICS provides the following safety related functions:

- Manual actuation of reactor trip in the main control room (MCR) and remote shutdown station (RSS).
- Manual actuation of engineered safety features (MCR only).
- Monitoring and control of systems required to achieve and maintain safe shutdown (MCR~~ and RSS~~).
- Display of Type A through Type C post-accident monitoring variables (MCR only).

2.0 Arrangement

07.09-46

2.1 ~~The location of the~~ SICS equipment is located as listed in Table 2.4.2-1—Safety Information and Control System Equipment.

2.2 Physical separation exists between the four Class 1E panel interface divisions of the SICS.~~Deleted~~

2.3 Physical separation exists between the four Class 1E QDS divisions of the SICS.

2.4 Physical separation exists between Class 1E SICS equipment and non-Class 1E equipment.

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I in Table 2.4.2-1 can withstand seismic design basis loads without loss of safety function.

4.0 I&C Design Features, Displays and Controls

4.1 The capability to transfer control of the SICS from the MCR to the RSS exists~~.~~ in a fire area separate from the MCR. The transfer switches are each associated with a single division of the safety-related control and allow transfer of control without entry into the MCR.

4.2 Deleted.

07.09-46

Table 2.4.2-1—Safety Information and Control System Equipment (2 Sheets)

~~Equipment~~ Description	~~Equipment~~ Tag Number (1)	~~Equipment~~ Location	Seismic Category	IEEE Class 1E (2)
SICS PI Cabinets, Division 1	30CWY1	Safeguard Building 1	I	1^N 2^A
SICS PI Cabinets, Division 2	30CWY2	Safeguard Building 2	I	2^N 1^A
SICS PI Cabinets, Division 3	30CWY3	Safeguard Building 3	I	3^N 4^A
SICS PI Cabinets, Division 4	30CWY4	Safeguard Building 4	I	4^N 3^A
SICS QDS Units MCR for ~~safety~~ safety-related I&C functions, Division 1	N/A	MCR	I	1^N 2^A
SICS QDS Units MCR for ~~safety~~ safety-related I&C functions, Division 2	N/A	MCR	I	2^N 1^A
SICS QDS Units MCR for ~~safety~~ safety-related I&C functions, Division 3	N/A	MCR	I	3^N 4^A
SICS QDS Units MCR for ~~safety~~ safety-related I&C functions, Division 4	N/A	MCR	I	4^N 3^A
SICS QDS Units MCR for non-~~safety~~ safety-related I&C functions	N/A	MCR	N/A	~~No~~N/A
SICS QDS Units RSS, Division 1	N/A	RSS	I	1^N 2^A
SICS QDS Units RSS, Division 2	N/A	RSS	I	2^N 1^A
SICS QDS Units RSS, Division 3	N/A	RSS	I	3^N 4^A
SICS QDS Units RSS, Division 4	N/A	RSS	I	4^N 3^A
Hardwired (Conventional) I&C, Division 1	N/A	MCR, RSS	I	1^N 2^A
Hardwired (Conventional) I&C, Division 2	N/A	MCR, RSS	I	2^N 1^A
Hardwired (Conventional) I&C, Division 3	N/A	MCR, RSS	I	3^N 4^A

Table 2.4.2-2—Safety Information and Control System ITAAC (~~4~~ 8 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	~~The location of the~~ SICS equipment is located as listed in Table 2.4.2-1.	Inspection will be performed of the location of the SICS equipment.	The SICS equipment listed in Table 2.4.2-1 is located as listed in Table 2.4.2-1.
2.2	Physical separation exists between the four Class 1E panel interface divisions of the SICS.~~Deleted.~~	Inspections will be performed to verify that the divisions of Class 1E panel interface cabinets are located in separate Safeguards Buildings.~~Deleted.~~	The four divisions of Class 1E panel interface cabinets are located in separate Safeguards Buildings.~~Deleted..~~
2.3	Physical separation exists between the four Class 1E QDS divisions of the SICS.a.	a. Design analyses will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between the four Class 1E QDS divisions of the SICS. b. Inspections will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between the divisions of Class 1E QDS equipment.	a. A report exists and defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between the four Class 1E QDS divisions of the SICS. b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between the divisions of Class 1E QDS equipment. Reconciliation is performed of any deviations to the design.
2.4	Physical separation exists between Class 1E SICS equipment and non-Class 1E equipment.	a. Design analyses will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E SICS equipment and non-Class 1E equipment.	a. A report exists and defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E SICS equipment and non-Class 1E equipment.

07.09-46

Table 2.4.2-2—Safety Information and Control System ITAAC (~~4~~ 8 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
	07.09-46	b. Inspections will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SICS equipment and non-Class 1E equipment.	b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SICS equipment and non-Class 1E equipment.. Reconciliation is performed of any deviations to the design.
3.1	Equipment identified as Seismic Category I in Table 2.4.2-1can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment listed as Seismic Category I in Table 2.4.1-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements. b. Inspections will be performed of the ~~as-installed~~ Seismic Category I equipment listed in Table 2.4.2-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	a. Tests/analysis reports exist and conclude that the equipment listed as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function. b. Inspection reports exist and conclude that the ~~as-installed~~ Seismic Category I equipment listed in Table 2.4.2-1 including anchorage is installed as specified on the construction drawings.
4.1	The capability to transfer control of the SICS from the MCR to the RSS exists in a fire area separate from the MCR. The transfer switches are each associated with a single division of the safety-related control and allow transfer of control without entry into the MCR.	a. Inspections will be performed to verify the existence of procedures. b. Tests will be performed to verify that control of the SICS can be transferred from the MCR to the RSS.	a. A report exists and concludes that procedures exist for transfer of control of the SICS from the MCR to the RSS. b. A report exists and concludes that the test results confirm that control of the SICS can be transferred from the MCR to the RSS.

2.4.4 Safety Automation System

1.0 Description

The safety automation system (SAS) provides control and monitoring of safety systems.

The SAS ~~has~~ provides the following safety related functions:

- Provides control and monitoring of systems required to transfer the plant to cold shutdown and maintain it in this state following a design basis event.
- Provides control and monitoring of safety related functions of auxiliary support systems.
- Provides acquisition and processing of Type A, B and C post-accident monitoring variables for display to the operators in the main control room (MCR) and on the remote shutdown station (RSS).
- Provides a safety interlock function.

2.0 Arrangement

2.1 ~~The~~ SAS equipment is located as listed in Table 2.4.4-1—Safety Automation System Equipment.

07.09-46

2.2 Physical separation exists between the four divisions of the SAS.

2.3 Physical separation exists between Class 1E SAS equipment and non-Class 1E equipment.

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without loss of safety function.

4.0 I&C Design Features, Displays and Controls

4.1 ~~The~~ Class 1E SAS equipment ~~classified as Class 1E in Table 2.4.4-1~~ can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

4.2 The SAS receives input signals from the sources listed in Table 2.4.4-2—Safety Automation System Input Signals.

4.3 The SAS provides the output signals listed in Table 2.4.4-3—Safety Automation System Output Signals.

4.4 The SAS provides the interlocks listed in Table 2.4.4-4—Safety Automation System Interlocks.

Table 2.4.4-5—Safety Automation System ITAAC (~~3~~ 9 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	~~The location of the~~ SAS equipment is located as listed in Table 2.4.4-1.	~~An i~~Inspections will be performed of the location of the SAS equipment ~~listed in Table 2.4.4-1~~.	The SAS equipment listed in Table 2.4.4-1 is located as listed in Table 2.4.4-1.
2.2	Physical ~~Separation~~ separation exists between the four divisions of the SAS.	Inspections will be performed to verify that ~~redundant~~ the divisions of the SAS are located in separate safeguard buildings.	The four divisions of the SAS are located in separate safeguard buildings.
2.3	Physical separation exists between Class 1E SAS equipment and non-Class 1E equipment.	a. Design analyses will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E SAS equipment and non-Class 1E equipment. b. Inspections will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SAS equipment and non-Class 1E equipment.	a. A report exists and defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E SAS equipment and non-Class 1E equipment. b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SAS equipment and non-Class 1E equipment. Reconciliation is performed of any deviations to the design.
3.1	Equipment identified as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the equipment listed as Seismic Category I in Table 2.4.4-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements.	a. Tests/analysis reports exist and conclude that the equipment listed as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without loss of safety function.

07.09-46

Communication Module – A device that is used to transmit digital information from one device to another over one or several data communication links using a predetermined protocol.

Channel – an arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.

Class 1E – the safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

Component Level – actuation or control of a single actuation device (component).

Credited – designation for a system that can perform a safety function, and is qualified and relied upon to do so.

Data Communication – a method of sharing information between devices that involves a set of rules, formats, encodings, specifications, and conventions for transmitting data over a communication path, known as a protocol.

Division – the designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

Design Basis Event (DBE) – postulated events used in the design to establish the acceptable requirements for the structures, systems, and components.

Function Processor – a device that contains hardware, system software, and application software that executes instrumentation and control functions.

Functional Unit – a set of assembled components within a system that perform specific functions to support overall system operation.

I&C Platform – a generic set of system hardware, system software, and engineering tools that can be configuration for a wide variety of instrumentation and control functions.

Hardwired I&C – operator controls and indicators that are connected with other I&C equipment using an analog signal path. This includes devices such as buttons, switches, analog indicators, or standalone digital indicators.

07.09-46 Hardwired Signal – an analog or discrete digital signal that does not use a data communications protocol.

07.09-46

The safety-related portion of the SICS is organized into four independent divisions. The four divisions of safety-related panel interfaces are located in separate Safeguards Buildings. The four divisions of the safety-related QDS and other safety-related HMI equipment ~~is~~are located in the MCR and RSS, and ~~is~~are physically separated by safety-related structures, separation distance, barriers, or any combination thereof.

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

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

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.

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.

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.