Response to Request for Additional Information – ANP-10281P "U.S. EPR Digital Protection System Topical Report" (TAC No. MD3971)

***RAI 1**: Please identify the portions of ANP-10281P, "U.S. EPR Digital Protection System Topical Report" (PS) that are "sense and command features" as defined in IEEE Std. 603-1991.*

Title 10 of the Code of Federal Regulations (10 CFR), Section 50.55a(h)(3), require that safety systems must meet the requirements of IEEE Std. 603-1991, including the correction sheet dated January 30, 1995. IEEE 603-1991 Section 6, "Sense and Command Features-Functional and Design Requirements," contains requirements for the Sense and Command Features. AREVA must have an idea of which components correspond to these features.

*IEEE 603-1991 defines: "**sense and command features.** The electrical and mechanical components and interconnections involved in generating those signals associated directly or indirectly with the safety functions. The scope of the sense and command features extends from the measured process variables to the execute features input terminals."*

Section 11.1 of the PS Topical Report says: " * * the PAC module prioritizes the various sense and command inputs and executes an output that reflects the plant licensing requirements and operational preferences." This seems to imply that the entire digital protection system, as described in the subject topical report, is part of the sense and command features and does not contain any execute features. Is this correct?*

Section 14.20 of the PS says: "The sense and command features present in the PS satisfy the requirements of Clause 5 and the requirements of Clause 6 as described below." However, this topical report does not explicitly describe what set of equipment constitute the Sense and Command Features.

Response 1:

The safety related portions of the digital protection system (PS), with the exception of the MSI-AU, are part of the sense and command features as defined by IEEE Std. 603-1991. As indicated in Figure RAI 1-1, the RAU, RCCAU, APU, ALU, and MSI-MU are the functional units of the PS described in ANP-10281P, "U.S. EPR Digital Protection System Topical Report," (referred to as the PS topical report) that are sense and command features. The MSI-AU is used in testing of the sense and command features, but does not function as part of the sense and command features. [1]

Sections 7.8, 7.9, and 7.10 of the PS topical report describe the reactor trip actuation devices. These are execute features as defined by IEEE Std. 603-1991. These sections provide information regarding how the four divisions of the PS are assigned to the reactor trip actuators. Section 8.4 describes divisional assignments of the engineered safety feature (ESF) actuation outputs of the PS. An example using a main steam isolation valve is provided in Figure 8-2 of the PS topical report. This example of

[1] The PS topical report provides a list of acronyms used in this submittal

an execute feature was provided to clarify how the four divisions of the PS are assigned to ESF actuators. The specific aspects of the PS design for which AREVA NP is requesting approval are listed on page 1-1 of the PS topical report. The examples of execute features described above are not included in this list.

The NRC quotes from section 11.1 of the PS topical report in the text of RAI 2:

> ". . . the PAC module prioritizes the various sense and command inputs and executes an output that reflects the plant licensing requirements and operational preferences."

AREVA NP agrees that this statement incorrectly implies that the priority and actuator control (PAC) module is part of the execute features. According to the definitions presented in IEEE 603-1991, the PAC module is part of the sense and command features. AREVA NP proposes to modify the previously quoted statement as follows:

> "The PAC module prioritizes the actuation requests for a single actuator from the various control systems and produces an actuation output that reflects the plant licensing requirements and operational preferences."

There are no execute features described in the PS topical report for which AREVA NP is seeking approval. As such, AREVA NP plans to remove sections 14.29 through 14.34 from the PS topical report. These sections describe compliance with the clauses of IEEE 603-1991 related to the execute features. Compliance with these clauses will be addressed in Section 7.1 of the U.S. EPR Design Control Document (DCD).

***RAI 2**: Please identify the execute features associated with the Digital Protection System.*

Federal Regulations, 10 CFR 50.55a(h)(3), require that safety system must meet the requirements of IEEE Std. 603-1991, including the correction sheet dated January 30, 1995. IEEE 603-1991 Section 7, "Execute Features- Functional and Design Requirements," contains requirements for the Execute Features. Please identify which components correspond to these features.

*IEEE 603-1991 defines: "**execute features.** The electrical and mechanical equipment and interconnections that perform a function, associated directly or indirectly with a safety function, upon receipt of a signal from the sense and command features. The scope of the execute features extends from the sense and command features output to and including the actuated equipment-to-process coupling. NOTE: In some instances, protective actions may be performed by execute features that respond directly to the process conditions (for example, check valves, self-actuating relief valves)."*

Section 11.1 of the PS Topical Report says: " * * the PAC module prioritizes the various sense and command inputs and executes an output that reflects the plant licensing requirements and operational preferences." This seems to imply that the Priority Actuation and Control System (PACS), is part of the execute features. Is this correct?*

Section 14.30 of the PS says: "The execute features associated with the PS are capable of receiving and acting upon the automatic actuation signals generated by the PS consistent with the design bases of the system." This quote is understood to mean that execute features are not part of the Digital Protection System, since the words "associated with" are used rather than "of."

If the execute features are not part of the PS, then Sections 14.29 through 14.34 are asserting that equipment not described in this report are in compliance with regulatory requirements. No references to what this equipment is, or where it is described are provided. Note: LIC-500, "Processing Requests for Reviews of Topical Reports," documents that the NRC, through it's website (Reference 1), provides guidance to applicants on the NRC's topical report (TR) program. Both the website (Reference 1) and LIC-500 (Reference 3) state that the report should contain complete and detailed information on the specific subject presented.

Response 2:

As noted in the response to RAI 1, there are no execute features described in the PS topical report for which AREVA NP is seeking approval. As such, AREVA NP plans to remove sections 14.29 through 14.34 from the PS topical report. These sections describe compliance with the clauses of IEEE 603-1991 related to the execute features. Compliance with these clauses will be addressed in Section 7.1 of the DCD.

RAI 3: *Please describe any features that support surveillance testing, and how surveillance testing will be addressed.*

Response 3:

Section 4.2 of the safety evaluation report (SER) for the TXS topical report contains the following passage:

> "By letter NRC:99:056, dated December 28, 1999, Siemens submitted report EMF-2341(P), "Generic Strategy for Periodic Surveillance Testing of TELEPERM XS Systems in U.S. Nuclear Generating Stations," for staff review. By letter NRC:00:017 dated March 3, 2000, Siemens provided additional clarification on recommended periodic surveillance test requirements for TXS applications. The report describes measures to be implemented in safety I&C systems configured with a TXS architecture to comply with requirements for channel checks, functional tests, channel calibration verification tests, response time verification tests, and logic system functional tests."

- The TXS platform contains extensive self monitoring features and online diagnostic checks, which provide a means for considerably reducing the required efforts of the operators for conducting periodic testing. **[**

]

The design of overlapping test steps results in a verification of the performance of the complete system. Due to the capabilities of TXS, several of these tests are performed by online monitoring without the need for human interaction.

The overlapping between the different types of periodic tests and the self-monitoring capabilities of the system, demonstrate that each protective channel is entirely tested. Figure RAI 3-1 depicts the data flow from the sensor to the actuator and shows the overlapping between self-monitoring and periodic tests for the main structure of the PS. As indicated in this figure, the following portions of the system are required to be tested by periodic testing:

The surveillance testing of the U.S. EPR digital protection system will be consistent with the requirements contained in EMF-2341(P). Additionally, the testing of output channels for ESF actuation functions utilizes the no-go testing capabilities of the PAC module which was not described in EMF-2341(P).

RAI 4: *Please identify when the Digital Protection System design will be completed.*

*The Abstract of the PS says: "This topical report describes the design of the U.S. EPR protection system * * * ." However, Section 6.1 of the PS says: "The detailed system architecture is represented through a series of figures (Figure 6-3 – Figure 6-20) showing network connections between the different units of the PS [i.e. the Protection System]. These figures represent the conceptual system design and may be modified in the detailed system design phases." Therefore, it is not clear as to whether AREVA considers the design presented to be a design or a conceptual system design. Furthermore, the Abstract of the PS says: "This report describes * * * the typical implementation of protective functions within this architecture."*

Section 4.1 of the PS says: "The networks shown in Figure 4-1 are intended to represent functional connections only, and are not representative of the detailed network topologies as implemented."

Since no specific inputs or outputs are identified, and only conceptual functionality is defined (i.e. Protection System & Engineered Safety Features Actuation). The design presented is understood to be a conceptual design of the architecture.

Note 1: NUREG-0800 Rev. 5, Chapter 7, Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real Time Performance," says: "The level of detail in the architectural description should be sufficient that the staff can determine the number of message delays and computational delays interposed between the sensor and the actuator. An allocation of time delays to elements of the system and software architecture should be available. In initial design phases (e.g., at the point of design certification application), an estimated allocation of time delays to elements of the proposed architecture should be available."

*Note 2: LIC-500 documents that the NRC, through it's website (Reference 1), provides guidance to applicants on the NRC's topical report (TR) program. Both the website (Reference 1) and LIC-500 (Reference 3) state that the report should contain complete and detailed information on the specific subject presented. LIC-500 says: "The review of TRs, for the most part, follows the guidance for reviewing license amendments in Office Instruction LIC-101," License Amendment Review Procedures" (Reference 2).' Section 4.1.1 of LIC-500 says: "(3) * * * Conceptual or incomplete preliminary information will not be reviewed." In addition, Section 2.3.4 of the TELEPERM XS (TXS) Topical Report (TR) (ML003732662) says: "For hardware architecture, application-specific descriptions will be compiled."*

Response 4:

The response to RAI 4 contains five parts. Item 1 addresses the level of detail contained in Figures 6-3 through 6-20. Item 2 addresses the level of detail of Figure 4-1. Item 3 addresses the typical functions presented in Sections 7.0 and 8.0. Item 4 addresses NRC Branch Technical Position (BTP) 7-21, "Guidance on Digital Computer Real-Time Performance," related to allocation of time delays to elements of the system. Item 5 addresses the relationship of LIC-500 to the PS topical report submittal.

1. The subject Section 6.1 of the PS topical was included to address potential future design complications such as:

   a. Detailed system logic is generated during detailed system design. It could become necessary to increase, or reduce the number of processing units in a division allocated to performing a specific function (e.g., APU function in sub-system B). These changes may be implemented to ensure processing load or response time requirements are met.

   b. New NRC guidance could be issued to clarify existing requirements that might affect some portion of the network architecture.

c. Human factors evaluations might require a change in the control room display structure, which could affect the interfaces between the PS and the human-machine interface (HMI) systems.

Specific changes that result from completion of the detailed design work may result in changes to the detailed system network connections presented in the PS topical report to ensure that critical system response requirements are met. For example,
[

]

The network architecture shown in Figures 6-3 through 6-18 and 6-20 of the PS topical report represent the PS architecture that will be described in the U.S. EPR application for design certification. A revised Figure 6-19 is attached.

AREVA NP plans to modify the subject statement from Section 6.1 as follows:

> The detailed system architecture is represented through a series of figures (Figure 6-3 – Figure 6-20) showing network connections between the different units of the PS. These figures represent the PS network design as submitted for design certification approval.

2. The subject statement from Section 4.1 of the PS topical report is accurate and it is not intended to imply that Figure 4-1 is conceptual in nature. A revised Figure 4-1 is attached and is representative of the architecture of the PS that will be described in the design certification application. Figures 6-3 through 6-20 of the PS topical report provide a more detailed perspective of this architecture that is consistent with the revised Figure 4-1.

3. Sections 7.0 and 8.0 of the PS topical report describe the typical implementation of RT and ESF actuation functions within the PS architecture. The design of the PS architecture is not conceptual. The typical implementation of functions within the architecture is provided to allow the staff to understand how the different functional units of the system work together to perform the RT and ESF actuation functions. By approving the system architecture and typical implementation of functions, AREVA NP understands that the NRC will only need to verify that the functions described in the DCD are bounded by what is approved in the PS topical report. This would reduce the resources required to review the DCD and allow the staff to focus on any functions that are not clearly bounded by the approved typical implementations.

   The PS topical report specifies the system architecture and will be referenced by the DCD. The DCD will specify the functional requirements of the system to the level of

detail required for design certification (i.e., specific inputs, outputs, and logical operations).

4. The information required to satisfy the subject statements from BTP 7-21 for the U.S. EPR PS is available. The level of architectural description provided in the PS topical report, along with the typical implementation of functions within this architecture is sufficient to estimate the various segments of time associated with the system functions.

   Realistic assumptions are made regarding sensor response times (including signal conditioning delays) and actuator response times to support the plant safety analysis. These response times are outside the scope of the PS topical report and will be established as part of the Chapter 15 analyses. I&C system performance will be verified in Chapter 7.

   The methodology used to estimate the response time of the computerized portion of the PS establishes a theoretical bounding response time for the typical types of functions performed by the PS. The bounding time delays possible due to asynchronous operation are taken into account, and full loading of function processors and networks is assumed. The final response time of the PS will be verified to be within the bounding time limits established for the PS.

   [ ]

   AREVA NP will provide the NRC with supporting documentation detailing the allocation of time delays to the computerized portion of the PS. This documentation will be submitted to NRC as part of the responses to the second set of RAIs for the PS topical report.

5. The discussion of LIC-500 in RAI 4 appears to suggest that the level of detail presented in the PS topical report is not sufficient for review because it appears to be conceptual or preliminary. Items 2, 3, and 4 above address this specifically.

   Further, AREVA NP notes that LIC-500 allows for NRC review in any case when "the report would contribute in resolving a safety-related subject or if the report presents advanced technologies that would maintain safety or reduce an unnecessary burden." AREVA NP believes this topical report contributes to resolution of I&C-related safety issues.

RAI 5: *Please identify when other concepts will be finalized.*

*Section 1.0 of the PS says: "AREVA NP requests NRC approval of the following aspects * * * Typical RT concepts * * * Typical ESFAS concepts * * *" However, Section 4.1.1 of LIC-500 says: "(3) * * * Conceptual * * * information will not be reviewed." In addition, Section 2.3.4 of the TELEPERM XS (TXS) Topical Report (TR) (ML003732662) says: "For hardware architecture, application-specific descriptions will be compiled."*

Response 5:

The U.S. EPR PS topical report specifies the PS architecture, and will be referenced by in the U.S. EPR DCD. The DCD will specify the functional requirements of the PS to the level of detail required for design certification.

The Typical RT and ESF actuation concepts were submitted to the NRC at a similar level of detail as the architecture configurations shown in Section 2.7.2 of topical report EMF-2110, Revision 1, "TELEPERM XS: A Digital Reactor Protection System" (Reference 1, which is referred to as the TXS topical report). In the TXS topical report, three typical architectural concepts were identified, none of which is used in the U.S. EPR design. Given that the individual functions of the PS are specified in the DCD, AREVA NP found it appropriate to submit the typical implementation of the functions as part of the PS topical report since they are different than what was presented in the TXS topical report.

The discussion of LIC-500 in RAI 5 appears to suggest that the level of detail presented in the PS topical report is not sufficient for review because it appears to be conceptual or preliminary. Items 2, 3, and 4 of the response to RAI 4 above address this specifically.

Further, AREVA NP notes that LIC-500 allows for NRC review in any case when "the report would contribute in resolving a safety-related subject or if the report presents advanced technologies that would maintain safety or reduce an unnecessary burden." AREVA NP believes this topical report contributes to resolution of I&C-related safety issues.

RAI 6: *Please describe the safety classification of all components and connections shown in Figure 8-4.*

Figure 8-4 shows a feedback path from the Priority Actuation and Control (PAC) module to Class 1E logic. The use of the term "1E" implies that this is a safety system. Is this correct? Are all parts of this feedback path through safety system components? Please identify where, in the PAC module Topical Report, the "1E" feedback signals are described.

Response 6:

The components shown in Figure 8-4 of the PS topical report are safety-related components. Specifically, all parts of the "feedback path" are safety-related components.

RAI 7: *Please describe AREVA's understanding of the "generic approval" of the TELEPERM XS (TXS) platform as it applies to changes and associated review requirements.*

The Abstract of the PS TR says: "The TELEPERM XS platform has been generically approved by the U.S. Nuclear Regulatory Commission for use in safety-related instrumentation and

control applications in the United States." In addition, Section 15.0 says: "Second generation hardware is currently in development following the established TXS design principles, including qualification and testing methods, and is expected to operate in the same reliable manner." Furthermore, Section 2.1 says: "The generic approval of the TXS system design principles and methods eliminates the need for regulatory review of each individual TXS hardware or software upgrade. Instead, each applicant must demonstrate that the equipment and software used in the as-built system adheres to the approved TXS design principles and methods." However, a statement to this effect has not been found in the TXS SER, or in the TXS TR. Generic use of specific versions of specific equipment was provided in the SER. AREVA must realize that certain vendors have an NRC approved QA program, and this programmatic approval does not mean that all designs produced under these program do not require NRC review, nor that the NRC review of items produce would only be to ensure that they followed their QA program. Therefore, AREVA's understanding of the review requirements for the I&C equipment that will be used on the U.S. EPR is unclear. What is planned to be submitted for review, and when?

Section 1.0 of the PS says: "AREVA NP is not requesting approval for a specific set of TXS hardware components or version of the software to be used in the PS." Therefore, any approval of the PS TR will be, qualified in that specific versions of equipment and software will need to be identified, and those versions must be acceptable to the NRC. The NRC will need to decide if this qualification will be in the form of an open item to the SER, COL Action Item, or an ITAAC. This decision will be based on the anticipated timing of the submitted material.

Response 7:

The PS topical report supports implementation of all versions of the TXS platform. Advances in digital technology have resulted in revisions to the TXS platform since the TXS topical report was initially submitted in 1999. Further revisions to the TXS platform will continue into the foreseeable future. The PS topical report also supports the U.S. EPR design certification and will be referenced in the DCD.

In order to support construction of the U.S. EPR well into the future, an I&C architecture must be approved at the design certification level, based on safety-related software life cycle and equipment qualification processes rather than approval of specific versions of hardware and software.

In the text of RAI 7, the staff states:

> "Generic use of specific versions of specific equipment was provided in the SER."

AREVA NP believes this is a misstatement, and no similar statement appears in the SER for the TXS topical report. The SER for the TXS platform topical report approves the TXS design principles and methods as outlined in AREVA NP's response to RAI 11. This approval provides a framework to accommodate the continued evolution of TXS technology under approved design, testing and qualification controls in accordance with the approved TXS design principles.

AREVA NP does not dispute the need for the NRC staff to be informed of the specific versions of hardware and software used in the as-built system for each U.S. EPR constructed. AREVA NP expects that NRC will perform audits that the staff deems necessary to assure that the versions used adhere to the approved TXS design principles and methods.

As previously noted, the PS topical report will be referenced by the DCD, and specifies the system architecture in which the TXS platform will be applied. The DCD will specify the functional requirements of the system to the level of detail required for design certification. Specific versions of the TXS platform will be addressed as an element of an Inspections, Test, Analyses, and Acceptance Criteria (ITAAC) item.

This approach is consistent with the NRC's review process described in the SRP. Specifically, SRP 7.0 states:

> "Review of DC applications should normally extend to cover detailed design. However, for digital computer-based I&C systems, it may be premature to complete final design details at the DC stage. Waiting until the COL stage to complete the final design of such systems allows the COL applicant/licensee to use the most recent technology for each plant. Therefore, the review of DC applications for digital computer-based I&C systems may be limited to (1) a detailed review at the functional block diagram level, (2) a review of the applicant/licensee's commitment to prescribed limits, parameters, procedures, and attributes for the detailed design process, and (3) ITAAC adequate to demonstrate that the as-built facility conforms to these commitments."

RAI 8: *Please describe all of the changes to "design principles and methods" described in the TXS TR.*

Siemens submitted a Topical Report (TR) on a Digital Reactor Protection System (ML003732662), and the NRC reviewed and approved that TR (i.e. the TXS TR). Subsequently Areva submitted the subject TR on the Digital Protections System (PS). The PS TR references the TXS TR. It is not clear if the only similarities between the two TRs are those that are referenced in the PS TR. It is also not clear, what all of the differences between these two TRs are. If there are a small number of differences, then it may be quicker to review just the differences, and the affect that these differences have on the approved material. Furthermore, the PS TR, Section 2.1, says: "The generic approval of the TXS system design principles and methods eliminates the need for regulatory review of each individual TXS hardware or software upgrade. Instead, each applicant must demonstrate that the equipment and software used in the as-built system adheres to the approved TXS design principles and methods." In what ways are the "design principles and methods" that will be used on the application development, different that what was approved? In what ways are the "design principles and methods" that are being used on the platform development, different that what was approved?

Response 8:

The NRC SER for the TXS topical report states that:

> "The TXS design is intended to provide a qualified generic digital I&C platform that meets the regulatory requirements and that can be used for a wide range of plant-specific applications. When using this platform for any plant-specific application, the licensee or applicant will need to verify that the qualification details in this topical report meet the plant license requirements. Because this topical report is for a generic platform, licensees referencing this topical report will need to document the details regarding the use of TXS design in plant-specific applications and address all plant-specific interface items including, but not limited to, those listed in Section 6.0 of this safety evaluation."

The typical RT and ESF actuation concepts were submitted to the staff at a similar level of detail as the architecture configurations shown in Section 2.7.2 of the TXS topical report. Three typical architectural concepts were identified, none of which is used in the U.S. EPR design. Given that the individual functions of the PS are specified in the DCD, AREVA NP found it appropriate to submit the typical implementation of the functions as part of the PS topical report since they are different than what was presented in the TXS topical report.

Additionally, the NRC SER for the TXS topical report (Reference 2) identified plant-specific action items to be addressed by an applicant when requesting installation of a TXS system. The scope of the PS topical report does not apply to the installation of the TXS system; therefore, the resolution of the action items in Reference 2 is not within the scope of this report. For informational purposes, Appendix A to the PS topical report identifies the documentation that AREVA NP anticipates will disposition each plant-specific action item from the SER.

RAI 9: *Please describe any changes in terminology between the TXS TR and the PS TR.*

The PS TR seems to use the term "function computer" in the same way that the TXS TR uses "function processor." Please identify any other changes in terminology.

Response 9:

AREVA NP has not made any intentional changes in terminology between the TXS topical report and the PS topical report.

The staff states in the text of the RAI:

> "The PS TR seems to use the term 'function computer' in the same way that the TXS TR uses 'function processor'."

AREVA NP recognizes this point but notes that it is not a change in terminology. Both terms, "function processor" and "function computer" are used throughout the TXS topical report in an interchangeable way. For example, the following passage appears in Section 2.5.7 of the TXS topical report:

> "If the receiving function computer is in cyclic operating mode, all signals received with the status TEST are converted to the signals with status ERROR and therefore masked by selection blocks with active status processing. In this case the receiving function processor behaves as if the transmitting function processor had failed."

AREVA NP introduces some new terminology in the PS topical report that was not used in the TXS topical report. One set of new terms is introduced to generically refer to equipment that performs a specific type of functionality. These terms are defined in Table 1-1 of the PS topical report.

The term "functional unit" is introduced in the PS topical report. This term is used to refer to a group of components that function as one "box" in the system architecture of Figure 4-1 (e.g., APU, ALU, RAU, etc.). A functional unit generally consists of one or more function computers and associated input modules, output modules and communication modules.

The term "interchannel communication" is used in the PS topical report to describe communication between two or more redundant divisions of the PS. The interchannel communication principles discussed in the PS topical report are also described in TXS topical report Section 2.9, "Interference Free Communication."

RAI 10: *For each reference to the TXS TR, please identify the specific passage being referenced.*

Response 10:

The PS topical report references the TXS topical report (i.e. Reference 24 of the PS topical report). The following is a list of the page number from the PS topical report for each reference to the TXS topical report and the specific section in the TXS topical report related to the reference. For multiple instances of the reference appearing on the same page of the PS topical report, the references are identified as instance 1, instance 2, or instance 3 corresponding to the order in which they appear.

- Page 1-1: This is a general reference that does not require clarification.

- Page 1-2: This is a general reference that does not require clarification.

- Page 2-1, Instance 1: This is a general reference that does not require clarification.

- Page 2-1, Instance 2: This is a general reference that does not require clarification.

- Page 2-1, Instance 3: This is a general reference that does not require clarification.

- Page 2-2: This is a reference to multiple sections of the TXS topical. While relevant information related to the TXS system design principles is found throughout the report, specific sections with particular relevance are listed below.
  - System hardware: Section 2.4.3.1
  - System operating software: Sections 2.4.3.2, 3.2.1.3, 3.1.3
  - Application software: Sections 2.4.3.2, 3.2.1.3, 3.1.3
  - SPACE tool: Sections 2.1.2, 2.4.3.3
  - Equipment qualification: Section 2.2
  - Operating system software development: Section 3.0
  - Processing principles: Section 3.1
  - Interchannel communication principles: Section 2.9
  - Service Unit: Section 2.5

- Page 7-5: This is a reference to Section 2.7 of the TXS topical report.

- Page 14-4: This is a reference to Section 3.0 of the TXS topical report.

- Page 14-5, Instance 1: This is a reference to Section 2.2 of the TXS topical report.

- Page 14-5, Instance 2: This is a reference to Section 2.4.2 of the TXS topical report.

- Page 14-5, Instance 3: This is a reference to Section 2.6 of the TXS topical report.

- Page 14-6: This is a reference to Section 2.7.1.1 of the TXS topical report.

- Page 14-7: This is a reference to Section 2.6 of the TXS topical report.

- Page 14-8: This is a reference to Section 2.7.1.1 of the TXS topical report.

- Page 14-9: This is a reference to Section 3.1.1.5 of the TXS topical report.

RAI 11: *Please identify where in the NRC's safety evaluation of the TXS platform, approval of the design principles and methods was explicitly stated.*

*Section 2.1 of the PS says: "The NRC's approval of the TXS platform as a qualified, generic digital I&C platform also constitutes approval of the TXS system design principles and methods for safety-related applications that were documented * * *."*

Response 11:

This subject statement is based on the fact that the TXS design principles and methods are explicitly described throughout the SER for the TXS topical report. Specifically, the staff's method of review clearly identifies that the focus of the review was on the design processes under which the TXS hardware and software are produced, tested, and qualified.

Page 2-2 of the PS topical report lists those items that AREVA NP considers to be the TXS system design principles and methods. These items are again listed below, followed by specific passages from the SER that address the design principle or method.

- Use of the four system building blocks

  Pages 1 and 2 of the SER identify the "TXS system architecture basic building blocks." Each of the building blocks is described by the staff in a generic manner.

  The use of these system building blocks is a TXS system design principle that is clearly identified and approved by the SER.

- Equipment qualification methods

  Page 2 of the SER states:

  > "Equipment qualification was performed through type testing according to German safety standards which were compared by the staff against the U.S. nuclear industry equipment qualification standards. Except for minor deviations between German and U.S. standards, the equipment qualification design was considered to be acceptable."

The TXS design method for equipment qualification is approved by the SER, contingent on an applicant demonstrating closure of action item 1 on page 52 of the SER.

- Operating system software development process, including verification and validation methods.

  The following statements appear on Page 46 of the SER:

  > "On the basis of its review of the software processes used throughout the software life cycle, and on the basis of its audit of software development documentation, the staff concludes that the software development process used at Siemens is acceptable.
  >
  > The independent verification and validation (IV&V) process for the Siemens TXS is consistent with the IV&V process described in IEEE 1012-1998. . .The staff concludes that the Siemens IV&V effort is sufficiently independent in personnel, management, and financial resources.
  >
  > On the basis of its review of the Siemens engineering procedures and the results of its audit of Siemens software development processes, the staff concludes that Siemens has an acceptable software development methodology and follows this methodology consistently in developing safety-related software. The staff also determines that SPACE (specification and coding environment) tool for designing and assembling safety-related applications has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis."

  The TXS software development process for operating system software, application software development tools, and function block library development, including verification and validation are approved by the SER. AREVA NP has submitted topical report ANP-10272, "Software Program Manual for TELEPERM XS Safety System Topical Report," by letter dated December 21, 2006, to address action item 2 from page 52 of the SER for the TXS application software development process used for U.S. projects (Reference 3).

- Processing Principles

  Page 2 of the SER states:

  > "The design principle for software of Class 1E systems is to ensure that the sequence of processing executed for each expected

> situation can be deterministically established. It discourages the use of non-deterministic data communications, non-deterministic computations, multitasking, dynamic scheduling, use of non-deterministic interrupts and event driven designs. Based on its review, the NRC staff determined the design of the TXS system satisfies this design principle for Class 1E system software."

The TXS design principles related to processing are approved by the SER.

- Interchannel communication principles

  Page 7 of the SER states:

  > "Specific communication methods are applied to ensure interference-free communication inside the TXS system and within the plant process information system. The TXS design requires that in case of a single failure of one of the independent processing channels or within one communication path in the same processing channel, the channels still available will continue to operate as designed on the basis of the remaining information to ensure the required safety functions do not fail."

  Additionally, page 19 of the SER describes in greater detail the "specific communication methods" mentioned above.

  The TXS interchannel communication methods and principles are clearly identified and approved by the SER.

- Service Unit maintenance interface

  Pages 5 and 6 of the SER describe the principles of the service unit interface in several statements:

  > "The MSI serves as a gateway between the computers of the automatic path and other non-safety-related systems such as service units.
  >
  > The non-safety-related service unit requests access through the MSI to perform the diagnostic function at the safety-related processor.
  >
  > The service unit contains the central data of the I&C system. It is the central means for interventions into the safety-relevant software of the function processors.
  >
  > The service unit is protected against unauthorized interventions. The control mechanisms are installed by software so that only authorized

> persons may access the service unit, only authorized interventions may be performed, and interventions are restricted to a single redundant channel."
>
> The TXS principles and methods related to the service unit maintenance interface are clearly identified and approved by the SER.

Statements are made in the safety evaluation to indicate that specific hardware and software were audited to verify the acceptability of the processes under which they were designed. For example, page 45 of the SER includes the following statement:

> "The adequacy of the Siemens development process was reviewed by the staff during an audit at the vendor facility. The staff conducted a life cycle process audit of the TXS by tracing three requirements through the software life cycle."

However, there are no statements in the SER to indicate that approval was limited to specific versions of hardware or software that were audited as part of the review.

Finally, Section 3.2 "Method of Review" of the SER states on page 39 that:

> "This topical report was submitted for generic review, and will be referenced in the future for a plant protection system upgrade or replacement. To ensure that the digital plant protection system will perform its safety function as designed, the staff concentrated on the basic operation of the TXS software system, the life cycle activities of TXS hardware and software systems, and the qualification testing."

AREVA NP construes this passage as an explicit statement that the staff's review and subsequent approval of the TXS platform focused on the basic operating principles of the TXS platform, the life cycle activities used in development of TXS platform software and hardware, and the TXS qualification testing methods; all of which are TXS design principles and methods.

Therefore, AREVA NP believes that approval of the TXS platform as a qualified generic digital I&C platform constitutes approval of the TXS system design principles and methods.

RAI 12: *Figure 4-1: Is the connection to the PAC a hardwired or a buss connection? Why are the connections to the PACs shown as links to another division?*

Response 12:

The connections from the ALUs to the PAC system are hardwired connections. The arrowheads on the connection lines were erroneously included on the figure to show

direction of signal propagation. A revised Figure 4-1 is attached which indicates hardwired connections consistent with the figure legend.

RAI 13: *Please clarify the use of the terms "TELEPERM XS" and "TXS."*

It is understood that within Areva, the terms "TELEPERM XS" and "TXS" refer to a family of components. Please list all of the components that Areva currently considers to be part of the TXS family.

It is understood that TXS platform described in the Siemens Topical Report EMF-2110, was a subset of the TXS family described above. It is also understood that the NRC review and approval was for specific versions of each component in this platform. Please list all of the component types, and specific versions, that were reviewed as part of the safety evaluation.

It is understood that the TXS family of components could change. That is to say: 1) More components could be added, 2) Some components may no longer be supported, and 3) Existing components could be revised.

It is understood that the TXS components that AREVA intends for nuclear application may not be identical to those approved in the Siemens topical report. However AREVA has not identified the specific components or version that will be used.

It is not clear when the terms "TELEPERM XS" or "TXS" are used, if reference is being made to the family of components, or to specific versions of the specific set of components approved by the NRC.

Response 13:

The DCD will specify the functional requirements and network architecture. It is recognized that TXS hardware and software will continue to evolve as technology changes. As noted in Section 2 of the PS topical report, each applicant must demonstrate that the equipment and software used in the as-built system adheres to the TXS design principles and methods approved by NRC in the safety evaluation report for the TXS topical report. The DCD will specify the use of the TXS platform. Specific versions of the TXS platform will be addressed as an element of an ITAAC item. Similarly, licensees that submit license amendments that support plant modifications will specify the versions of the TXS platform planned for use. Additional information regarding this RAI is provided in the response to RAI 7.

RAI 14: *Please list all of the tools that are part of SPACE.*

Note: NUREG-0800, Revision 5, "Standard Review Plan for the Review of Safety Analysis Reports for Nuclear Power Plants," says: "Methods/tools -- It is important to remember that if the output of any tool can not be proven to be correct, such as may occur if the tool produces

machine language software code, the tool itself should be developed or dedicated as safety-related, with all the attendant requirements."

Response 14:

As stated in Section 2.1 of the PS topical report, the use of the SPACE tool for application software development was approved by NRC in the SER for the TXS topical report. On page 2 of the SER for the TXS topical report, NRC describes the SPACE tool that was reviewed as follows:

3. Application software - The application software performs the plant-specific TXS safety-related functions using function block modules which are grouped into function diagram modules. The application software is generated by SPACE tools which use the qualified software modules from the function block library to construct a specific application.

4. SPACE tool - The SPACE (specification and coding environment) tool is an engineering system that is used to implement the requirements of plant-specific I&C features.

On page 46 of the SER for the TXS topical report, NRC makes the following conclusion:

> "On the basis of its review of the Siemens engineering procedures and the results of its audit of Siemens software development processes, the staff concludes that Siemens has an acceptable software development methodology and follows this methodology consistently in developing safety-related software. The staff also determines that SPACE (specification and coding environment) tool for designing and assembling safety-related applications has the capability and safeguards to ensure that the implementation of the application programs can be successfully accomplished on a plant-specific basis."

Further information on SPACE may be found in the TXS topical report.

[ ]

These additional SPACE tools have been developed in accordance with AREVA NP (GmbH) internal quality standards. AREVA NP has significant operating experience with these tools, which provides additional confidence in the suitability of the tools to support TXS projects.

References

1. Siemens Topical Report EMF-2110, Revision 1, “TELEPERM XS: A Digital Reactor Protection System,” May 2000 Enclosure to letter, James F. Mallay (Siemens Power Corporation) to Document Control Desk (NRC), "Publication of EMF-2110(NP)(A) Revision 1, TELEPERM XS: A Digital Reactor Protection System," NRC:00:033, July 12, 2000).

2. Letter dated May 5, 2000, from Stuart A. Richards, NRC, to Jim Mallay, Siemens Power Corporation, “Acceptance for Referencing of Licensing Topical Report EMF-2110 (NP), Revision 1, “TELEPERM XS: A Digital Reactor Protection System” (TAC NO. MA1983),” and associated Safety Evaluation Report.

3. AREVA NP Topical Report ANP-10272, Revision 0, “Software Program Manual for TELEPERM XS Safety System Topical Report,” December 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10272, "Software Program Manual TELEPERM XS Tm Safety Systems Topical Report," NRC:06:061, December 21, 2006).

4. AREVA NP Topical Report ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report",” November 2006, Enclosure to letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), Request for Review and Approval of ANP-10273P, "AV42 Priority Actuation and Control Module Topical Report, NRC:06:054, November 28, 2006).

Figure RAI 1-1

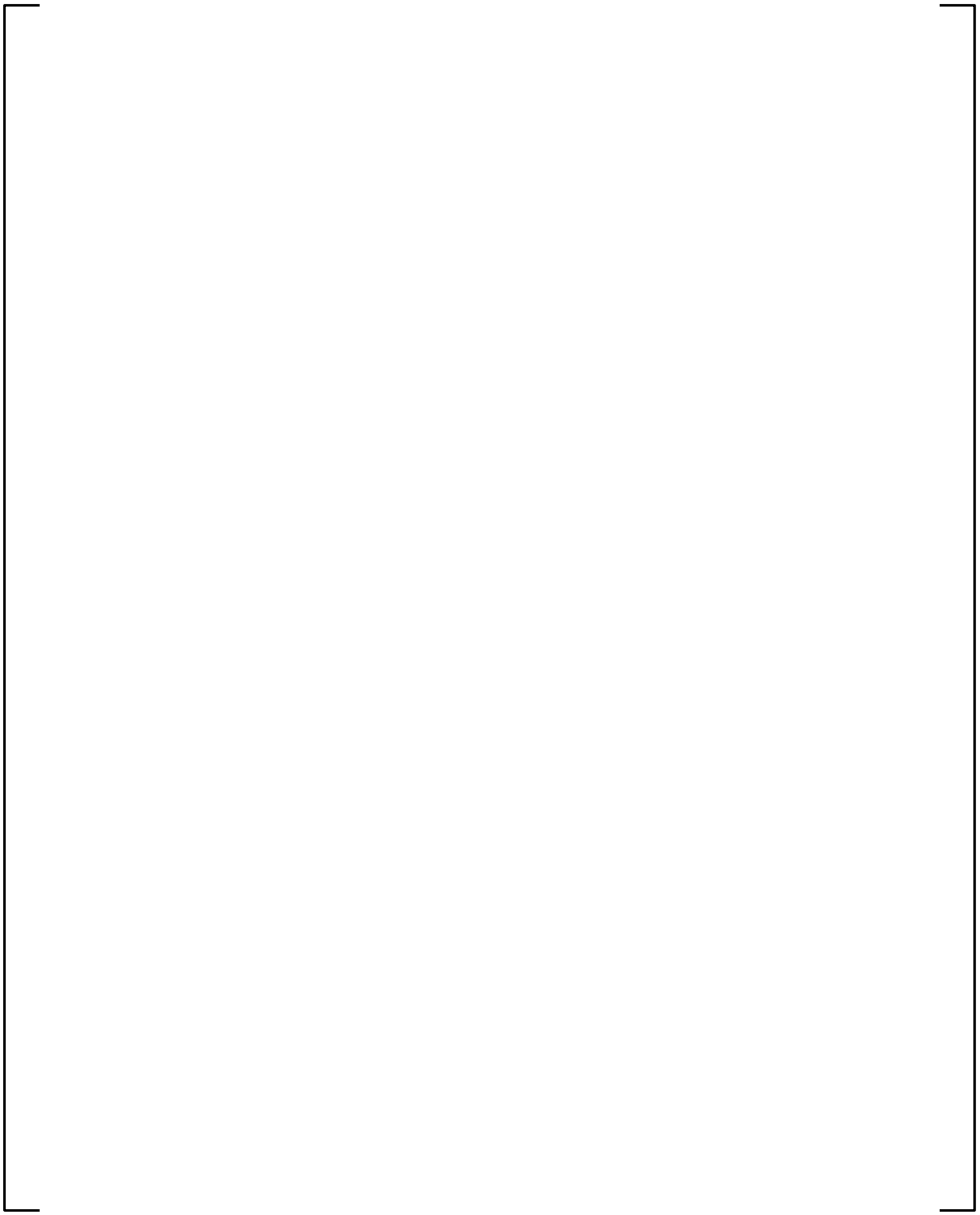
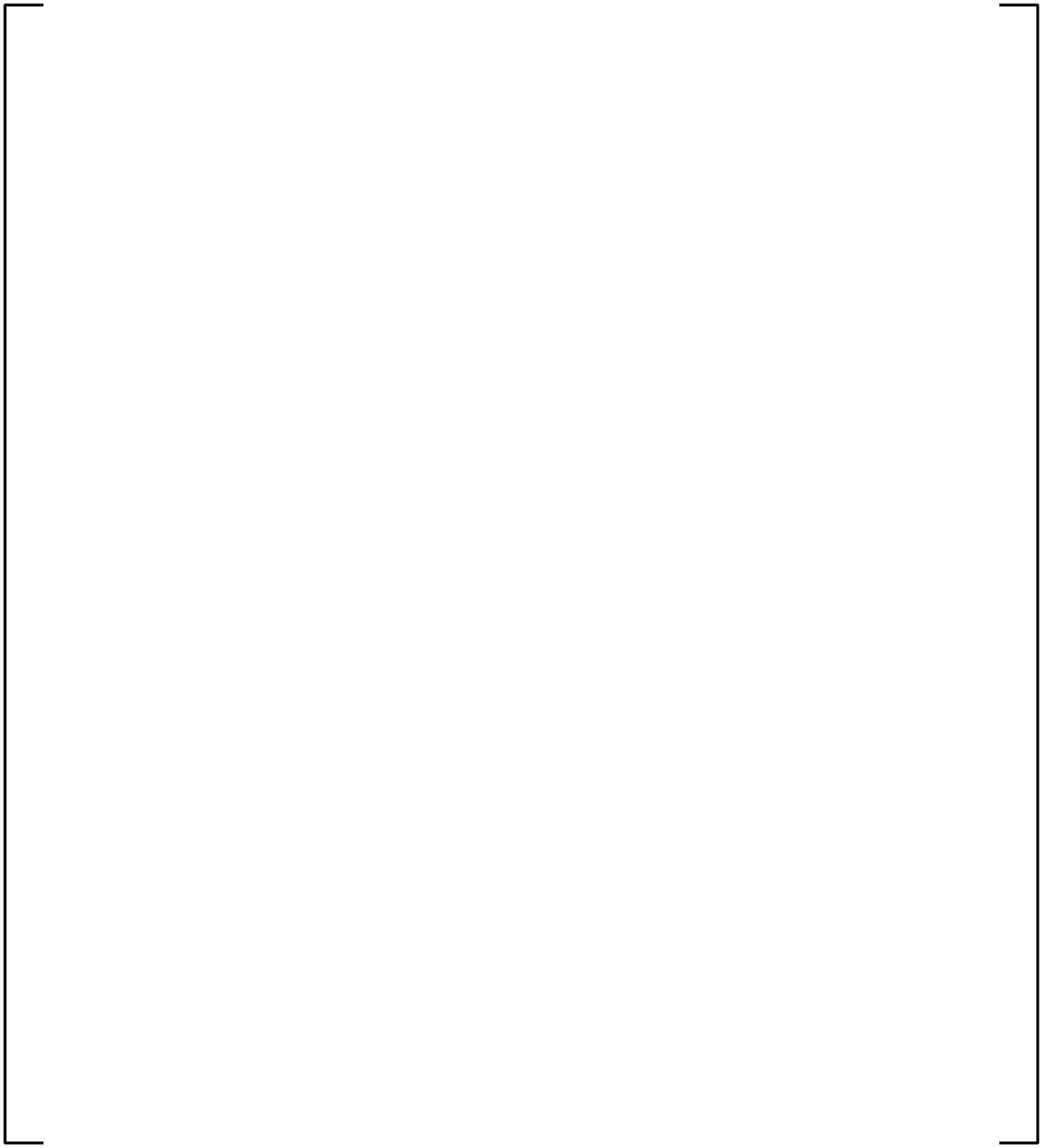


Figure RAI 3-1



Revised Figure 4-1 - Protection System Architecture

Revised Figure 6-19—MSI-MU – PI Architecture