Request for Additional Information No. 56 (942), Revision 0

9/12/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.09 - Data Communication Systems
Application Section: Section 7.1
ICE1 Branch

QUESTIONS

07.09-1

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

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

07.09-2

Clarify the classification of safety components within the SICS. In addition, how is independence achieved between safety portions and non-safety portions of the SICS to meet IEEE Std. 603-1991, Clause 5.6.3, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24?

Clause 5.6.3 of IEEE 603-1991 requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from completing their safety

functions. 10 CFR Part 50, Appendix A, GDC 24, “Separation of Protection and Control Systems,” requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. The D FSAR, Tier 2, Section 7.1.1.3.1 states that the SICS is classified as safety-related. However, this section also states that the SICS has safety-related portions and non-safety related portions. The safety-related portion of the SICS includes the panel interface (PI), service units (SU), and qualified display system (QDS), and the non-safety related portion of the SICS includes the SU, QDS, and gateway (GW). Clarify whether the PI, SU, and QDS are classified and qualified as safety related for all portions of the SICS. In addition, how is independence achieved between safety portions and non-safety portions of the SICS to meet IEEE Std. 603-1991, Clause 5.6.3 and 10 CFR Part 50, Appendix A, GDC 24? Provide the necessary ITAACs to demonstrate that communications independence requirements for SICS will be verified.

07.09-3

Demonstrate how the data communications system within the SICS meets IEEE Std. 603-1991, Clause 5.6.3, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24. Specifically, provide information regarding the design of hardwired connections and isolation devices between the SICS and non-safety-related I&C systems.

Clause 5.6.3 of IEEE Std. 603-1991 requires the safety system be designed such that credible failures in and consequential actions by other systems shall not prevent the safety systems from performing the intended safety functions. 10 CFR Part 50, Appendix A, GDC 24, “Separation of Protection and Control Systems,” requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system.

The DC FSAR, Tier 2, Section 7.1.1.3.1 states that the hardwired connections to non-safety-related I&C systems may be used as required by the SICS human factors design and are isolated. Provide the design details of the hardwired connections (e.g., connection medium, signal parameters, etc.) and where they are used to communicate with non-safety-related I&C systems. In addition, what types of isolation devices are used between the SICS and the non-safety-related I&C systems? Provide design information for these isolation devices, including a description of any type testing completed and how the devices address the acceptance criteria in Branch Technical Position 7-11 in the Standard Review Plan.

07.09-4

Demonstrate how the interface between the qualified display system (QDS) and the non-safety service unit (SU) satisfies IEEE Std. 603-1991, Clauses 5.6.3 and 5.9 requirements.

The DC FSAR, Tier 2, Section 7.1.1.3.1 states that the communication between the service unit (SU) and the qualified display system (QDS) uses bi-directional, networked data connections implemented with the TELEPERM XS Ethernet protocol. The SU is an auxiliary feature, and this network is a non-safety-related network provided for servicing of the QDSs. These data connections use dedicated ports on the QDS separate from the PI-QDS connections. The system software provides for isolation between the safety-related and non-safety-related data. Software modifications cannot be performed with the QDS in operation. Access is authorized only with appropriate administrative controls.

Clause 5.6.3 of IEEE Std. 603-1991 requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from performing the intended safety functions. Since the QDS is safety-related and the SU is non-safety-related, demonstrate how independence requirements are met. Specifically, provide specific details regarding the system software that provides the isolation between the QDS and the SU. In addition, Clause 5.9 of IEEE Std. 603-1991 provides access control requirements for safety systems. This clause requires the safety system design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof. Describe the specific access controls available for the SUs that service the QDS and how those controls meet Clause 5.9.

07.09-5

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

The DC FSAR, Tier 2, Section 7.1.1.3.1 provides a summary of the data communications within the safety portion of the SICS, including the interconnections to other I&C systems and components. This summary does not indicate whether there is redundancy built within these connections (i.e., cables) to meet IEEE Std. 603-1991, Clause 5.1. Clause 5.1 requires the safety systems to perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. Provide additional information to demonstrate how the data communications links within the SICS and from the SICS to other I&C systems and components meet the requirements of Clause 5.1.

07.09-6

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

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the SRP revision in effect six months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, "Data Communications Systems," provides the performance and reliability design considerations. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems. Data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes should be considered. There should be sufficient excess capacity margins to accommodate likely future increases in DCS demands or software or hardware changes to equipment attached to the DCS. The potential hazards to the DCS and from the DCS should be considered. Unneeded, but included, DCS functions should be reviewed to assure that they cannot be inadvertently activated and thereby prevent operation of the safety functions. The effects of error detection and recovery should be reviewed. Error detection should be at least as good as four byte cyclic redundancy check (CRC). The effects of DCS equipment malfunction or failure that generates erroneous signals, either in content or rate, should be examined. Corrupted messages (missing or corrupted packets), missing messages and duplicate messages should be detected and repaired. The error performance should be specified. Vendor test data and in situ test results should be reviewed to verify the performance. Analytical justifications of DCS capacity should be reviewed for correctness.

The DC FSAR, Tier 2, Section 7.1.1.3.1, provides the summary of data communications implemented within the SICS. The data communications summary only provides the description of the type of connection (i.e., point-to-point), indication of whether the connection is bi-directional or uni-directional, and the type of protocol used, but does not address the performance and reliability criteria. Provide the information addressing the performance and reliability criteria of SRP, Section 7.9, for the data communications systems within the SICS.

07.09-7

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

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the SRP revision in effect six months before the docket date of the application. The

evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, "Data Communications Systems," provides the performance design considerations. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems. The real-time performance should be reviewed with SRP Branch Technical Position 7-21.

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

07.09-8

Clarify the specific functionality of the data communications between the SICS and other I&C systems and components.

DC fsar, Tier 2, Section 7.1.1.3.1, provides the summary of data communications implemented within the safety-related and non-safety related portions of the SICS. The data communications summary only provides the description of the communication type (i.e., point-to-point), indication of whether the communication is bi-directional or uni-directional, and the type of protocol used. This summary does not provide the description of the communication functions. For example, the summary states that the PS communicates with the SICS for control purposes, but it does not state what exactly is the SICS controlling within the PS. Provide the description of the communication functions for each of the interfaces described.

07.09-9

Address IEEE Std. 603-1991, Clause 5.4, equipment qualification requirements, and 10 CFR Part 50, Appendix A, General Design Criterion 4, requirements for the subracks, I/O modules, function processors, Optical Link Module, and qualified isolation devices used in the safety automation system (SAS). In addition, identify the corresponding ITAACs and how they verify that the Maintenance Service Interfaces (MSI)s provide adequate communication isolation between safety and non-safety systems to meet the requirements of IEEE Std. 603, Clause 5.6.3 and GDC 24.

DC FSAR, Tier 2, Section 7.1.1.4.2, states that within the SAS, the Control Units (CU)s and the MSIs generally consist of subracks, I/O modules, function

processors, communication modules, optical link modules, and qualified isolation devices.

IEEE Std. 603-1991, Clause 5.4, provides equipment qualification requirements for safety systems. This clause requires safety system equipment to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std. 323-1983 and IEEE Std. 627-1980. Provide more information regarding how the CUs and MSIs have been qualified to meet Clause 5.4 of IEEE Std. 603-1991. In addition, GDC 4 requires structures, systems, and components important to safety to be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. Demonstrate how the requirements of GDC 4 are met for the data communications components within the SAS.

In addition, IEEE 603-1991, Clause 5.6.3, requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from completing their intended safety functions. GDC 24, “Separation of Protection and Control Systems” requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Identify the ITAACs and describe how they verify that the MSI provides adequate communications isolation between safety and non-safety systems as required by GDC 24 and IEEE Std. 603-1991, Clause 5.6.3. In addition, provide more information on the specific hardware and software design of subracks, I/O modules, function processors, communications link modules, and qualified isolation devices used (i.e. whether they are the same hardware and software qualified and approved in the Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System, [Adams Accession No. ML003732662].)

07.09-10

Demonstrate how the isolation devices used between the interface of the SAS and non-safety systems are designed to meet IEEE Std. 603-1991, Clause 5.6.3.

DC FSAR, Tier 2, Section 7.1.1.4.2, states that within the SAS, the functional units, CUs and MSIs, generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. IEEE 603-1991, Clause 5.6.3, requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from completing their intended safety functions. Describe what qualified isolation devices are used within the SAS. Provide the design of these qualified isolation devices and

demonstrate how this design supports the requirements of IEEE Std. 603-1991, Clause 5.6.3.

07.09-11

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

IEEE Std. 603-1991, Clause 5.1, requires the safety systems to perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions.

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

07.09-12

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

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

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

07.09-13

Address the acceptance criteria of NUREG-0800, the Standard Review Plan (SRP), Section 7.9, "Data Communications Systems," for the data communications systems and components within the Safety Automation System (SAS).

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, provides the performance design considerations for data communications systems used in the various I&C systems. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems.

DC FSAR, Tier 2, Section 7.1.1.4.2, provides a summary of the communication between the gateway (GW) and the plant data network within the SAS. However, it does not provide information on the network protocol used to implement this communication. The staff requests additional information regarding the communications protocol used to implement the point-to-point bi-directional communication between the GW and the plant data network. Demonstrate that the communications protocol selected adequately supports the required data communications between the SAS components and the non-safety I&C systems.

07.09-14

Address the acceptance criteria of NUREG-0800, the Standard Review Plan (SRP), Section 7.9, "Data Communications Systems (DCS)," for the data communications systems within the Safety Automation System (SAS).

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, states that the real-time performance should be reviewed with SRP Branch Technical Position 7-21. Data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes should be considered. There should be sufficient

excess capacity margins to accommodate likely future increases in DCS demands or software or hardware changes to equipment attached to the DCS. The potential hazards to the DCS and from the DCS should be reviewed. Unneeded, but included, DCS functions should be reviewed to assure that they cannot be inadvertently activated and thereby prevent operation of the safety functions. The effects of error detection and recovery should be considered. Error detection should be at least as good as four byte cyclic redundancy check. The effects of DCS equipment malfunction or failure that generates erroneous signals, either in content or rate, should be examined. Corrupted messages (missing or corrupted packets), missing messages and duplicate messages should be detected and repaired. The error performance should be specified. Vendor test data and in situ test results should be reviewed to verify the performance.

DC FSAR, Tier 2, Section 7.1.1.4.2, provides the summary of data communications implemented within the SAS. The data communications summary only provides the description of the type of connection (i.e., point-to-point), indication of whether the connection is bi-directional or uni-directional, and the type of protocol used, but does not address the performance and reliability criteria. Provide the information addressing the performance and reliability criteria of SRP Section 7.9 for the data communications within the SAS and between the SAS and non-safety I&C systems.

07.09-15

Describe the testing and calibration capabilities for the data communications components within the Safety Automation System (SAS) to meet IEEE Clause 603-1991, Clause 5.7.

IEEE Std. 603-1991, Clause 5.7, requires capability for testing and calibration of safety system equipment while retaining the capability of the safety systems to accomplish their safety functions.

DC FSAR, Tier 2, Section 7.1.1.4.2, provides the summary of data communications implemented within the SAS. This section does not describe the testing and calibration capabilities for the data communications systems and components used in the SAS. For example, what is method is used to determine whether a communications link is operating correctly? Provide information regarding the testing and calibration capabilities for the data communications components and systems used in the SAS, including the detection of faulty communications link, incomplete data transmission, and out of order messages to meet the requirements of IEEE Std. 603-1991, Clause 5.7.

07.09-16

Demonstrate how the optical link module used in the protection system meets IEEE Std. 603-1991, Clause 5.4, and 10 CFR Part 50, Appendix A, General Design Criteria 21.

IEEE Std. 603-1991, Clause 5.4, stipulates requirements for equipment qualification. This clause requires safety system equipment to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. In addition, GDC 21 requires the design to be shall be designed for high functional reliability and in-service 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.

Topical report ANP-10281P Revision 0, U.S. EPR Digital Protection System, has been submitted for NRC review in March, 2007. This topical report is currently under review by the NRC and has yet to be approved. This topical report provides a description of the network topologies implemented within the protection system. This topical report states that a redundant ring network topology consists of at least three OLMs and their corresponding double fiber optical links. A given redundant ring network topology can contain only a finite number of OLMs. Each network in the PS contains fewer OLMs than the maximum allowed. Each double fiber optical link consists of a separate transmit and receive channel. 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. The remaining units accessing the ring network can still communicate with one another. Although this topical report states that the OLM is mapped to the SLLM component qualified in the Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System [Adams Accession No. ML003732662], it does not indicate whether there have been any modifications or variations in the design of the OLM from the SLLM design that was qualified in the TELEPERM XS topical report. If there are modifications or variations in the design of the OLM, demonstrate how the hardware and software of the OLM is designed to meet IEEE Std. 603-1991, Clause 5.4, and GDC 21. In addition, demonstrate that the malfunction within the OLM will not influence the signal such that a failure will propagate to multiple redundant divisions.

07.09-17

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

IEEE Std. 603-1991, Clause 5.6.1, requires redundant portions of a safety system provided for a safety function to be independent of and physically separated from each other to the degree necessary to retain the capability to

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

07.09-18

Address the acceptance criteria of NUREG-0800, the Standard Review Plan (SRP), Section 7.9, "Data Communications Systems (DCS)," for the data communications systems used in the protection system.

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the SRP revision in effect 6 months before the docket date of the application. The

evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, provides the performance and reliability design considerations. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems. Data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes should be reviewed. There should be sufficient excess capacity margins to accommodate likely future increases in DCS demands or software or hardware changes to equipment attached to the DCS. The potential hazards to the DCS and from the DCS should be considered. Unneeded but included DCS functions should be reviewed to assure that they cannot be inadvertently activated and thereby prevent operation of the safety functions. The effects of error detection and recovery should be considered. Error detection should be at least as good as four byte cyclic redundancy check (CRC). The effects of DCS equipment malfunction or failure that generates erroneous signals, either in content or rate, should be examined. Corrupted messages (missing or corrupted packets), missing messages and duplicate messages should be detected and repaired. The error performance should be specified. Vendor test data and in situ test results should be verify the performance. Provide information addressing the performance and reliability criteria of SRP Section 7.9 for the data communications networks and components used within the PS.

Section 6 of the AREVA NP Topical Report ANP-10281 “U.S. EPR Digital Protection System Topical Report” provides a description of the network topologies implemented within the protection system. This topical report does not describe the network configurations implemented within these topologies. In addition, this topical report does not provide information on meeting the performance and reliability criteria described in SRP, Section 7.9. In addition, GDC 29 requires the protection system to be able to perform required safety functions in the presence of any anticipated operational occurrence. Describe how the data communications systems design implemented in the protection system adequately supports the reactor trip and engineered safety features actuation system functions that are necessary to sense accident conditions and anticipated operational occurrences in order to initiate protective actions consistent with the accident analysis presented in the FSAR Tier 2, Chapter 15. Provide the detailed network design, including network configurations (i.e., data rates, data precision, bandwidth capacity) in the PS. Provide details regarding system testing of the communications network within the PS.

07.09-19

Address the acceptance criteria of NUREG-0800, the Standard Review Plan (SRP), Section 7.9, "Data Communications Systems," for the data communications systems used in the protection system to support reactor trip

system (RTS) and engineered safety features actuation system (ESFAS) functions.

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the SRP revision in effect six months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, states that setpoint analyses should account for measurement inaccuracies attributable to the data communications systems in accordance with the guidance of Regulatory Guide 1.105, Revision 3. Show that the measurement inaccuracies attributable to the data communications systems are accounted for in the setpoint analyses.

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

07.09-20

Demonstrate how the cables for the Protection System data communications systems meet 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 2, "Design bases for protection against natural phenomena."

GDC 2, "Design bases for protection against natural phenomena" requires structures, systems, and components important to safety to be designed to withstand the effects of natural phenomena such as earthquakes, tornadoes, hurricanes, floods, tsunami, and seiches without loss of capability to perform their safety functions. Section 7 and 8 of the AREVA NP Topical Report ANP-10281 "U.S. EPR Digital Protection System Topical Report" provides a description of the system level reactor trip system (RTS) and engineered safety features actuation system (ESFAS) design.

DC FSAR, Tier 2, Sections 7.2 and 7.3, provide additional details on the RTS and ESFAS design. The protection system functional units are implemented with the TELEPERM XS platform, which the NRC has found to be in compliance with GDC 2. However, the cables used to interconnect these functional units have not been qualified to meet GDC 2. The staff requests additional information to demonstrate that adequate shielding or housing has been provided for the cables used to interconnect functional units within the Protection System.

07.09-21

Demonstrate how the Protection System (PS) data communications systems meet 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 4, “Environmental and Dynamic Effects Design Basis.”

GDC 4, “Environmental and Dynamic Effects Design Basis” requires structures, systems, and components important to safety to be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. Sections 7 and 8 of the AREVA NP Topical Report ANP-10281 “U.S. EPR Digital Protection System Topical Report” provides a description of the system level reactor trip system and engineered safety features actuation system design.

DC FSAAR, Tier 2, Sections 7.2 and 7.3, provide additional details on the reactor trip system and engineered safety features actuation system design. The protection system functional units are implemented with the TELEPERM XS platform, which the NRC has found to be in compliance with GDC 4. However, the cables used to interconnect these functional units have not been qualified to meet GDC 4. The staff requests additional information regarding the physical layout of the communications cables and the cabinets used to house the data communications systems within the PS. Demonstrate that there is adequate protection of the communications cables form the environmental effects described in GDC 4. Show that the physical layout of the communications cables cabinents adequately meets the requirements GDC 4.

07.09-22

Demonstrate how the safety I&C systems are physically separated to meet 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 22, "Protection System Independence," requirements.

GDC 22, “Protection System Independence” requires the protection system to be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.

DC FSAR, Tier 2, Section 7.1.1.6.4, provides a description of the independence requirements for redundant divisions of the safety I&C systems. This section states that independent divisions are located in each of the four physically separated Safeguards Buildings. Safety I&C systems may be implemented in other safety-related structures, where redundant divisions are adequately separated. The staff requests additional information regarding how redundant divisions will be physically separated for safety I&C systems that are located in other safety-related structures and what criteria is used to demonstrate that the physical separation is adequate to meet GDC 22.

07.09-23

Demonstrate how electrical isolation is maintained between redundant divisions to meet IEEE Std. 603-1991, Clause 5.6.1 requirements.

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

DC FSAR, Tier 2, Section 7.1.1.6.4, provides a description of the independence requirements for redundant divisions. This section states that electrical isolation is required for hardwired and data connections and is provided through the use of qualified isolation devices and fiber optic cable. The staff finds that insufficient information has been provided regarding how electrical isolation is achieved to meet IEEE Std. 603-1991, Clause 5.6.1. Provide additional information regarding how electrical isolation between redundant divisions is achieved. Specifically, provide design and equipment qualification information regarding the qualified isolation devices used.

07.09-24

Demonstrate how IEEE Std. 603-1991, Clause 5.6.1, requirements are met regarding communications independence as implemented within the U.S. EPR Instrumentation and Control (I&C) design.

DC FSAR, Tier 2, Section 7.1.1.6.4, provides a description of the independence requirements for redundant divisions within the safety I&C systems. This section states that the Safety Information and Control System, Protection System, and Safety Automation System implement interdivisional communications to support the system functional requirements. Communications independence is provided by implementing the communications independence principles described in the TELEPERM XS platform. The staff requests additional information to demonstrate that the communications processors, functional processors, and communications principles approved in the TELEPERM XS topical report safety evaluation report (ML003703082) have not been modified in the design of the U.S. EPR safety I&C systems. If any modifications have been completed, provide information regarding the changes in hardware and software design, equipment qualification, and type testing completed.

07.09-25

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

Independence requirements of IEEE Std. 603-1991, Clause 5.6, are addressed by guidance in interim staff guidance (ISG) (Digital I&C ISG #4) on communications. Digital I&C ISG #4 HICR-Communications provide further clarification on acceptable methods of data communications between redundant divisions of the safety system and between safety and non-safety systems. This

communications ISG states that vital communications among safety divisions should be point-to-point by means of a dedicated medium (copper or optical cable). In this context, “point-to-point” means that the message is passed directly from the sending node to the receiving node without the involvement of equipment outside the division of the sending or receiving node. The staff requests that the applicant demonstrate that data communications between redundant divisions for each of the safety systems (Safety Information and Control System, Safety Automation System, Protection System, Priority Actuation and Control System) addresses the guidance of ISG #4- HICR-Communications with respect to point-to-point communication.

07.09-26

Demonstrate how the instrumentation and control (I&C) systems listed Table 7.1-2 of the U.S. EPR DC-FSAR meet IEEE Std. 603-1991, Clauses 5.8.3.3 and 5.8.4.

IEEE Std. 603-1991, Clause 5.8.3.3, states that the capability shall exist in the control room to manually activate the display indications. In addition, IEEE Std. 603-1991, Clause 5.8.4, states that information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.

DC FSAR, Tier 2, Section 7.1.2.1.4, states that the applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(v). This is provided by compliance to Clause 5.8.2 (system status indication) and Clause 5.8.3 (indication of bypasses) of IEEE Std. 603-1998. Provide information to demonstrate that the U.S. EPR I&C design meets these two clauses of IEEE Std. 603-1991. Specifically, demonstrate that the capability exists in the control room to manually activate the display indications. In addition, provide a schematic of the location of the information displays and demonstrate how these displays are accessible to the operator.

07.09-27

Demonstrate how IEEE Std. 603-1991, Clause 5.6.3, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 24 requirements are met. Specifically, provide the detailed design of the qualified isolation device used between the Process Information and Control System (PICS) and the safety system.

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

the protection system. Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired.

DC FSAR, Tier 2, Section 7.5.2.2.4, states if any Post Accident Monitoring Type A, B, and C variable is bypassed or rendered inoperable, the Protection System and the Safety Automation System provide the appropriate display signals to the PICS. Outputs to PICS from safety systems are supplied through qualified isolation devices. Demonstrate how the qualified isolation devices used to supply outputs from the safety systems to the PICS meet IEEE Std. 603-1991, Clause 5.6.3, and GDC 24 requirements. Provide specific design and testing details regarding these qualified isolation devices.

07.09-28

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

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

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

07.09-29

Demonstrate how the Process Information and Control System (PICS) data communications system and the plant data network are designed to meet 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13. Specifically, provide information to demonstrate that the network performance, network segregations, communications protocols implemented, data rate, and bandwidth capacity support the control systems functions required by GDC 13.

GDC 13, “Instrumentation and Control” requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation,

for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges.

DC FSAR, Tier 2, Section 7.1.1.3.2, provides a description of the data communications that occur within the PICS. This section states that Processing Units (PU)s are provided for data exchange between the plant data network and the terminal data network. The PUs perform functions such as data message validation, short term data storage, and alarm management. The PUs transmit data to and receive data from the Level 1 instrumentation and control systems via the plant data network. The PUs, operator workstations, POP, and XUs exchange data via the terminal data network. These networks implement periodic communications and message validation for robust data communications. The staff finds that additional information is required regarding the data communications systems within the PICS and the plant data network to demonstrate that the control system functions required by GDC 13 can be adequately completed. Specifically, provide information to demonstrate that the network performance, network segregations, communications protocols implemented, data rate, and bandwidth capacity support the control systems functions required by GDC 13. In addition, provide information regarding what specific periodic communications occur, and how message validation is implemented.

07.09-30

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

GDC 19, “Control Room,” requires a control room be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents.

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

07.09-31

Demonstrate how access control is implemented to the U.S. EPR digital instrumentation and controls as required by IEEE Std. 603-1991, Clause 5.9.

IEEE Std. 603-1991, Clause 5.9, provides access control requirements for safety systems. This clause requires the design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

DC FSAR, Tier 2, Section 7.1.1.3.2, states that the processing units (PUs) within the Process Information and Control System (PICS) perform functions such as data message validation, short term data storage, and alarm management. The PUs transmit data to and receive data from the Level 1 instrumentation and control systems via the plant data network. The PUs, operator workstations, POP, and XUs exchange data via the terminal data network. These networks implement periodic communications and message validation for robust data communications. In addition, XUs provide an interface to other computers from the PICS. Specialized monitoring systems may utilize dedicated computers that require an interface to the PICS for operator monitoring and management. A firewall is provided for unidirectional transfer of information from the XUs to Level 3 instrumentation and control systems. Remote access to the PICS is prohibited. Although the PICS is not a safety system, it does perform some safety-related functions, and thus access control should be designed into the PICS. Provide additional information regarding the access control built into the PICS and plant data network, including information regarding the implementation of the unidirectional firewall, method for prohibiting remote access, network configurations to prevent unauthorized access and data storms, and methods for monitoring and detecting unauthorized access.

07.09-32

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

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

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

07.09-33

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

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

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

07.09-34

Demonstrate how data communications implemented within the Process Automation System (PAS) support the functions required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13 and 19. Specifically, provide information to demonstrate that the network performance, network segregations, communications protocols implemented, data rate, and bandwidth capacity support the control systems functions.

GDC 13, “Instrumentation and Control,” requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems

within prescribed operating ranges. In addition, GDC 19, “Control Room,” requires a control room to be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

DC FSAR, Tier 2, Section 7.1.1.4.6, provides a description of the data communications within the PAS. The staff finds that additional information is required to evaluate the data communications within the PAS. Demonstrate how data communications within the PAS supports the functions required by GDC 13 and GDC 19. Specifically, provide information to demonstrate that the network performance, network segregations, communications protocols implemented, data rate, and bandwidth capacity support the control systems functions required by GDC 13 and GDC 19.

07.09-35

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

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

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

07.09-36

Demonstrate how the data communications system within the Severe Accident Instrumentation and Control (SA I&C) System adequately supports the monitoring and control functions following a severe accident, as required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13 and 19.

GDC 13, “Instrumentation and Control” requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation,

for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. Appropriate controls shall be provided to maintain these variables and systems within prescribed operating ranges. In addition, GDC 19, "Control Room" requires a control room to be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. Equipment at appropriate locations outside the control room shall be provided (1) with a design capability for prompt hot shutdown of the reactor, including necessary instrumentation and controls to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures.

DC FSAR, Tier 2, Section 7.1.1.4.4, describes the data communications within the SA I&C. The staff requires additional information to evaluate the adequacy of the data communications systems within the SA I&C to complete the monitoring and control functions required by GDC 13 and GDC 19. The SA I&C performs the functions required by GDC 13 and GDC 19 for monitoring and control of I&C systems following severe accidents. Demonstrate how data communications systems within the SA I&C are designed with adequate performance and reliability to support the monitoring and control functions required for severe accident mitigation. Provide the specific bandwidth capacity, and transmission rate for the data communications modules within the SA I&C and the plant data network, and demonstrate how the specified bandwidth capacity and transmission rate are adequate to support the monitoring and control functions required for severe accident mitigation.

07.09-37

Describe the performance and reliability of the data communications system implemented in the Reactor Control, Surveillance, and Limitation (RCSL) to complete the necessary functions required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13 and 19.

GDC 13 "Instrumentation and Control" requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19, "Control Room" requires a control room to be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. 10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect six months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a

facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, "Data Communications Systems (DCS)," provides the performance and reliability design considerations. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems. Data rates, data bandwidths, and data precision requirements for normal and off-normal operation, including the impact of environmental extremes should be considered. There should be sufficient excess capacity margins to accommodate likely future increases in DCS demands or software or hardware changes to equipment attached to the DCS. The potential hazards to the DCS and from the DCS should be reviewed.

DC FSAR Tier 2, Section 7.1.1.4.5, provides a description of data communications within the RCSL system. This description does not include the performance and reliability of the data communications components used in the RCSL to perform the functions required by GDC 13 and GDC 19. Unneeded, but included, DCS functions should be reviewed to assure that they cannot be inadvertently activated and thereby prevent operation of the safety functions. Demonstrate that the performance and reliability guidance provided in SRP Section 7.9 has been addressed in the design of data communications components and links implemented in the RCSL to the degree necessary to support the required functions of GDC 13 and GDC 19.

07.09-38

Demonstrate how the communication path between the Reactor Control, Surveillance, and Limitation (RCSL) System and the other instrumentation systems meets IEEE Std. 603-1991, Clause 5.6.3, independence between safety and other systems.

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

DCFSAR, Tier 2, Section 7.1.1.4.5, provides a description of data communications within the RCSL System. The applicant states in this section that the RCSL receives hardwired inputs from the isolated outputs of the safety I&C system. In addition, the maintenance service interface (MSI) provide a communication path between the RCSL and other instrumentation and control (I&C) systems via the gateways (GW)s for both display of information and transfer of manual commands. Provide additional information regarding how outputs from the safety I&C systems to the RCSL are properly isolated to meet IEEE Std. 603-1991, Clause 5.6.3. Provide the specific design of this isolation device, including whether it is Class 1E qualified. In addition, clarify what manual commands are transferred from the RCSL system to the safety I&C system via the MSI and GW and which specific safety I&C systems is the RCSL communicating with?

07.09-39

Demonstrate how the Maintenance Service Interface (MSI) meets IEEE Std. 603-1991, Clause 5.3, 5.4, and 5.6.3, and 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 21.

IEEE Std. 603-1991, Clause 5.3, requires components and modules to be of a quality that is consistent with minimum maintenance requirements and low failure rates. Safety system equipment shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. IEEE Std. 603-1991, Clause 5.4, requires safety system equipment to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std. 323-1983. In addition, GDC 21, "Protection system reliability and testability" requires the protection system to be designed for high functional reliability and in-service testability commensurate with the safety functions to be performed.

FSAR Tier 2, Section 7.1.1.6.4, provides a description of the communications independence principles applied to the I&C design. This section states that the MSI provide the following communications features:

- Communication modules separate from the function processors for the purpose of handling communications to the GWs
- Communications between the function processors and communications modules are implemented with separate send and receive data channels
- The function processors and communications modules operate cyclically and asynchronous to each other.

The staff finds that the the specific hardware design (i.e. processors) has not been provided to the NRC. For the software design, the Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System [Adams Accession No. ML003732662] states that the SPACE tool, is used to create the software for the MSI, but does not provide additional information regarding the software design and qualification process used in the MSI. Demonstrate that the MSI hardware and software design, as well as equipment qualification process meet IEEE Std. 603-1991, Clause 5.3, 5.4, and GDC 21.

07.09-40

Demonstrate how the Maintenance Service Interface (MSI) meets IEEE Std. 603-1991, Clause 5.6.3.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety systems and other systems. This clause requires the safety system be designed

such that credible failures in and consequential actions by other systems shall not prevent the safety systems from performing their intended safety functions.

DC FSAR, Tier 2, Section 7.1.1.6.4, provides a description of the communications independence principles applied to the I&C design. This section states that only predefined messages are accepted by the MSI, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

Demonstrate that predefined allowable messages between the safety system and the non-safety systems will comply with IEEE Std. 603-1991, Clause 5.6.3, requirements. Provide a detailed list of all allowable predefined messages that is specific to each case in which communications are required between safety and non-safety systems.

Demonstrate that these predefined allowable messages will not allow the non-safety system to prevent the safety system from performing its safety functions. Provide the necessary ITAACs to verify that the MSI adequately supports the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.3.

Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System [Adams Accession No. ML003732662] section 4.2 states that serial data transmission between class 1E equipment and non class 1E equipment will be performed via a Class 1E qualified "message and service interface (MSI)" computer.

Is the MSI described in the U.S. EPR DC-FSAR the same class 1E qualified computer stipulated in the TELEPERM XS topical report? If not, how is the MSI described in the U.S. EPR DC-FSAR meeting the electrical isolation requirements of IEEE Std. 603-1991, Clause 5.6.3?

07.09-41

Demonstrate how electrical and communications isolation for hardwired connections between the safety and non-safety I&C systems is accomplished.

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

DC FSAR, Tier 2, Section 7.1.1.6.4, states that for hardwired signals, qualified isolation devices are used with the safety-related I&C systems for signal to and from the non-safety-related I&C systems. The Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System [Adams Accession No. ML003732662] was submitted and approved by the NRC. This topical report states that for single wire signal transmission, independence between class 1E circuits and non class 1E circuits will be achieved by one of the following ways:

a. Via a Class 1E electrical isolation device if the Class 1E signal is electrically connected to any equipment in the safety actuation channel.

b. Via the Class 1E Monitoring and Service Interface computer without an additional isolation device.

Verify that the single wire signal transmission electrical isolation principles between Class 1E and non-Class 1E equipment applies to the U.S. EPR I&C design for hardwired signals to and from non-safety-related I&C systems. In addition, provide the detailed design of this Class1E electrical isolation device to demonstrate how it meets IEEE Std. 603-1991, Clause 5.6.3.

07.09-42

Demonstrate how the developmental process of the TELEPERM XS platform and application software meets Regulatory Guide 1.152, regulatory positions C.2.1 through C.2.5.

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect six months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Appendix 7.1D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," provides review acceptance criteria for Regulatory Guide 1.152 regulatory positions C.2.1 through C.2.9.

DC FSAR, Tier 2, Section 7.1.1.6.6, states that the cyber security controls for TELEPERM XS application software development fully meets the intent of Regulatory Positions C.2.1 through C.2.5 of Regulatory Guide 1.152. However, the description of the developmental process of the TELEPERM XS platform and application has not provided sufficient information regarding what measures are in place to scan for backdoors, hidden code, and malicious code in the system software as stipulated in Regulatory Guide 1.152, Regulatory Position C.2.4. The staff finds that additional information is required to determine the adequacy of the software developmental process for the TELEPERM XS system to address the acceptance criteria provided in the Standard Review Plan Appendix 7.1D. Specifically, provide information regarding the measures taken to scan for backdoors, hidden code, and malicious code in the TELEPERM XS platform and application software.

07.09-43

Demonstrate how access control is achieved on the safety and non-safety data communications systems to meet IEEE Std. 603-1991 Clause 5.9, access control requirements.

IEEE Std. 603-1991, Clause 5.9, provides access control requirements for safety systems. This clause requires the safety system design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

The applicant stated in DC FSAR, Tier 2, Section 7.1.1.6.6, and in AREVA NP Topical Report ANP-10272 that control of access outside the safety system and critical control systems is the responsibility of the Combined License (COL) applicant. However, the staff did not identify a COL information item addressing these access control provisions. If no COL information item is provided, demonstrate where cyber security control of access outside the safety system and critical control systems is addressed. Provide details regarding the implementation of the plant data network and the interface between the plant data network to the terminal data network. Provide additional information regarding the implementation of the uni-directional firewall and any associated intrusion detection and monitoring systems.

07.09-44

Describe the performance and reliability of the data communications system implemented in the Turbine Generator Instrumentation and Control (TG I&C) system to complete the necessary functions required by 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 13 and 19.

GDC 13 “Instrumentation and Control” requires instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, for anticipated operational occurrences, and for accident conditions as appropriate to assure adequate safety, including those variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems. GDC 19, “Control Room” requires a control room to be provided from which actions can be taken to operate the nuclear power unit safely under normal conditions and to maintain it in a safe condition under accident conditions, including loss-of-coolant accidents. 10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect six months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Section 7.9, "Data Communications Systems (DCS)," provides the performance and reliability design considerations. This includes verification that the protocol selected for the DCS meets the performance requirements of all supported systems. Data rates, data bandwidths, and data precision requirements for normal and off-normal

operation, including the impact of environmental extremes should be considered. There should be sufficient excess capacity margins to accommodate likely future increases in DCS demands or software or hardware changes to equipment attached to the DCS. The potential hazards to the DCS and from the DCS should be reviewed. Unneeded but included DCS functions should be reviewed to assure that they cannot be inadvertently activated and thereby prevent operation of the safety functions.

DC FSAR, Tier 2, Section 10.2.2.5, provides a description of data communications within the TG I&C System. This description does not include the performance and reliability of the data communications components used in the TG I&C system to perform the functions required by GDC 13 and GDC 19. Demonstrate that the performance and reliability guidance provided in SRP Section 7.9 has been addressed in the design of data communications components and links implemented in the TC I&C system to the degree necessary to support the required functions of GDC 13 and GDC 19.

07.09-45

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

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