ArevaEPRDCPEm Resource

From: BRYAN Martin (EXT) [Martin.Bryan.ext@areva.com]
Sent: Friday, April 30, 2010 5:08 PM
To: Tesfaye, Getachew
Cc: DELANO Karen V (AREVA NP INC); ROMINE Judy (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 321, FSARCh. 7, Supplement 3
Attachments: RAI 321 Supplement 3 Response US EPR DC.pdf

Getachew,

AREVA NP Inc. provided a schedule for a technically correct and complete response to RAI No. 321 on November 20, 2009. AREVA NP submitted Supplement 1 on January 29, 2010 providing a revised schedule. AREVA NP submitted RAI 321 Supplement 2 on March 5, 2010. RAI 321 Supplement 3 Response US EPR DC.pdf" provides a technically correct and complete response to the last question 07.01-19, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 321 Question 07.01-19.

The following table indicates the respective pages in the response document, "RAI 321 Supplement 3 Response US EPR DC.pdf," that contain AREVA NP's response to the subject question.

Question #	Start Page	End Page
RAI 321 — 07.01-19	2	4

This concludes the formal AREVA NP response to RAI 321, and there are no questions from this RAI for which AREVA NP has not provided responses.

Sincerely,

Martin (Marty) C. Bryan
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
Tel: (434) 832-3016
702 561-3528 cell
Martin.Bryan.ext@areva.com

From: BRYAN Martin (EXT)
Sent: Friday, March 05, 2010 5:07 PM
To: 'Tesfaye, Getachew'
Cc: DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); ROMINE Judy (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 321, FSARCh. 7, Supplement 2

Getachew,

AREVA NP Inc. provided a schedule for a technically correct and complete response to RAI No. 321 on November 20, 2009. AREVA NP submitted Supplement 1 on January 29, 2010 providing a revised schedule. The attached file, "RAI 321 Supplement 2 Response US EPR DC.pdf" provides technically correct and complete responses to 2 of the remaining 3 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 321 Question 07.01-20.

The following table indicates the respective pages in the response document, "RAI 321 Supplement 2 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 321 — 07.01-18	2	4
RAI 321 — 07.01-20	5	5

The schedule for technically correct and complete responses to the remaining question has been changed and is provided below:

Question #	Response Date
RAI 321 — 07.01-19	April 30, 2010

Sincerely,

Martin (Marty) C. Bryan
Licensing Advisory Engineer
AREVA NP Inc.
Tel: (434) 832-3016
Martin.Bryan@areva.com

From: DUNCAN Leslie E (AREVA NP INC)
Sent: Friday, January 29, 2010 5:49 PM
To: 'Tesfaye, Getachew'
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 321, FSARCh. 7, Supplement 1

Getachew,

AREVA NP is unable to provide a response to RAI 321, Questions 07.01-18, 07.01-19, and 07.01-20 at this time. The commitment date for these questions has been changed to allow time to incorporate comments and feedback from the recent 1/25/10-1/26/10 meeting with the NRC related to U.S. EPR FSAR Chapter 7.

The schedule for technically correct and complete responses has been revised and is provided below:

Question #	Response Date
RAI 321 — 07.01-18	March 5, 2010
RAI 321 — 07.01-19	April 30, 2010
RAI 321 — 07.01-20	March 5, 2010

Sincerely,
Les Duncan
Licensing Engineer
AREVA NP Inc.
An AREVA and Siemens Company
Tel: (434) 832-2849
Leslie.Duncan@areva.com

From: Pederson Ronda M (AREVA NP INC)
Sent: Friday, November 20, 2009 7:40 PM
To: 'Tesfaye, Getachew'
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 321, FSARCh. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information RAI 321. The attached file, "RAI 321 Response US EPR DC.pdf," provides a schedule since a technically correct and complete response to the 3 questions is not provided.

The following table indicates the respective page in the response document, "RAI 321 Response US EPR DC.pdf," that contained AREVA NP's response to each of the subject questions.

Question #	Start Page	End Page
RAI 321 — 07.01-18	2	2
RAI 321 — 07.01-19	3	3
RAI 321 — 07.01-20	4	4

A complete answer is not provided for the 3 questions. The schedule for a technically correct and complete response to these questions is provided below.

Question #	Response Date
RAI 321 — 07.01-18	January 29, 2010
RAI 321 — 07.01-19	January 29, 2010
RAI 321 — 07.01-20	January 29, 2010

Sincerely,

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

From: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Thursday, October 29, 2009 7:26 PM
To: ZZ-DL-A-USEPR-DL
Cc: Spaulding, Deirdre; Jackson, Terry; Guardiola, Maria; Canova, Michael; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 321 (3910), FSARCh. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on October 26, 2009, and discussed with your staff on October 29, 2009. No changes were made to the draft RAI questions as a result of that discussion. The schedule we have established for review of your

application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 1372

Mail Envelope Properties (BC417D9255991046A37DD56CF597DB710600FA3D)

Subject: Response to U.S. EPR Design Certification Application RAI No. 321, FSARCh. 7, Supplement 3
Sent Date: 4/30/2010 5:08:27 PM
Received Date: 4/30/2010 5:08:31 PM
From: BRYAN Martin (EXT)

Created By: Martin.Bryan.ext@areva.com

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

Post Office: AUSLYNCMX02.adom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	6600	4/30/2010 5:08:31 PM
RAI 321 Supplement 3 Response US EPR DC.pdf	268945	

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

Response to

Request for Additional Information No. 321, Supplement 3

10/29/2009

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.01 - Instrumentation and Controls - Introduction
Application Section: 7.1

QUESTIONS for Instrumentation, Controls and Electrical Engineering 1 (AP1000/EPR Projects) (ICE1)

Question 07.01-19:

Describe the software development process (SDP) used for the video display that will be used in the safety information and control systems (SICS), particularly with respect to identification of aspects that differ from the SDP used for the TELEPERM XS.

The applicant needs to provide a description of the differences in the SDP for the safety-related video display. The staff needs to be able to determine acceptability with regards to the quality requirements of 10 CFR 50.55a(a)(1); 10 CFR Part 50, Appendix A, General Design Criteria 1; 10 CFR Part 50, Appendix B; and 10 CFR 50.55a(h) are met.

Response to Question 07.01-19:

The discussion of the qualified display system (QDS) software involves system software and application software. System software is present in the instances of a QDS and does not depend on the specific application where the QDS is used. Application software is configured uniquely for the specific application where the QDS is used.

QDS System Software:

QDS system software is commercial software. Some of the system software is developed by AREVA NP to meet the requirements of specific safety classifications in Europe (e.g., SC3 in Finland, F1B in France) that do not conform to the U.S. safety-related classification. There are portions of the system software (e.g., video driver software) that are acquired from a third party commercial source. It is appropriate to qualify the QDS system software for use in U.S. safety-related applications through a commercial dedication process that conforms to the guidance of EPRI TR-106439, “Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications.” This process includes the following activities:

1. Identification of the critical characteristics the system software must exhibit.
2. Definition of a combination of supplemental testing, supplier surveys, source verifications, or performance reviews, which demonstrate that the system software exhibits the critical characteristics.
3. Performance of the defined combination of supplemental testing, supplier surveys, source verifications, or performance reviews.
4. Creation of a dedication acceptance package that documents the results of activity 3 and provides evidence that the QDS system software exhibits the required critical characteristics.

QDS Application Software:

The development of the QDS application software is performed in accordance with the lifecycle and configuration controls defined in Topical Report ANP-10272, “Software Program Manual for TELEPERM XS Safety Systems,” but has one difference. The development tools to create the application software (i.e., SPACE) described in Topical Report ANP-10272 are not used to create QDS application software. The QDS-specific tools will be qualified as part of the commercial grade dedication process described in this response. Verification and validation (V&V) of the tools will be performed as part of the qualification. Once qualified, these tools will be controlled under configuration management as required by IEEE 7-4.3.2-2003, Section 5.3.2.

As opposed to the SPACE tool, use of the QDS development tool will require additional V&V of the application software at the implementation phase, unless demonstration of the correct implementation of logic diagrams to code is independently verified and certified, as it was for the SPACE tool.

U.S. EPR FSAR Tier 2, Section 7.1 will be revised to reflect the use of the commercial grade dedication process for QDS system software and to clarify that Topical Report ANP-10272 governs QDS application software development. Corresponding changes will be made to U.S. EPR FSAR Tier 1, Section 2.4.2.

Related Revisions for other I&C Systems:

AREVA NP believes it is important to distinguish between system software and application software for the safety-related instrumentation and controls (I&C) systems. U.S. EPR FSAR Tier 1, Section 2.4.1 and Section 2.4.4 will be revised to clarify this software distinction and to verify that the application software development process agrees with Topical Report ANP-10272.

The diverse actuation system (DAS) was originally a subsystem of the process automation system (PAS). A design change was made, and is being reviewed by NRC staff, which created a stand-alone DAS by removing it from the PAS. As part of this design change, a software design process was specified for the DAS to reflect augmented quality requirements. This process was included in letter NRC:09:119 and its enclosures that converted protection system (PS) Topical Report ANP-10281P to Technical Report ANP-10309P, which revised U.S. EPR FSAR Tier 2, Section 7.1, but was not reflected in the corresponding U.S. EPR FSAR Tier 1 section. U.S. EPR FSAR Tier 1, Section 2.4.24 will be revised to reflect the software design process for the DAS.

FSAR Impact:

U.S. EPR FSAR Tier 1, Section 2.4.1, Section 2.4.2, Section 2.4.4, and Section 2.4.24 will be revised as described in the response and indicated on the enclosed markup.

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

U.S. EPR Final Safety Analysis Report Markups

4.4 Communication independence is provided ~~in~~ between the ~~inter~~ four PS divisions. ~~communication paths within the PS.~~

4.5 The PS is capable of performing its safety function when PS equipment is in maintenance bypass (inoperable). Bypassed PS equipment is indicated in the MCR. ~~Bypassed or inoperable PS channels status information is retrievable in the MCR.~~

4.6 Setpoints associated with the automatic RT signals ~~reactor trips listed in Table 2.4.1-3~~ and the automatic~~ally actuated engineered safety features~~ESF signals ~~listed in Table 2.4.1-4~~ are determined using a methodology that addresses the determination of applicable contributors to instrumentation loop errors, the method in which the errors are combined, and how the errors are applied to the design analytical limits.

4.7 Input variables provide the inputs for generating RT signals and ESF signals. ~~The PS receives input signals from the sources listed in Table 2.4.1-2—Protection System Input Signals.~~

4.8 Electrical isolation is provided on connections between PS equipment and non-Class 1E equipment. ~~The PS provides signals to the non safety related control systems through electrical isolation devices.~~

4.9 Deleted. ~~Electrical isolation devices exist in the data communication paths between the PS and the non safety related displays and controls.~~

4.10 ~~The~~ Class 1E PS equipment ~~listed as Class 1E in Table 2.4.1-1~~ can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

4.11 Controls exist in the MCR to allow manual actuation ~~-~~at the system level. ~~of the functions identified in Table 2.4.1-5—Protection System Manually Actuated Functions.~~

4.12 Controls exist in the MCR and RSS to allow validation or inhibition of manual permissives. ~~listed in Table 2.4.1-7—Protection System Permissives.~~

4.13 The PS performs interlock functions. ~~interlocks exist as provided in Table 2.4.1-8—Protection System Interlocks~~.

4.14 The PS ~~hardware and software~~system design and application software are developed using a ~~design~~ process composed of ~~five~~ six life ~~-~~cycle phases with each phase having ~~design~~ outputs which must conform to the requirements of that phase. The ~~five~~ six life cycle phases are the following:

07.01-19

1. Basic ~~design~~ Design ~~phase~~Phase.
2. Detailed ~~design~~ Design ~~phase~~Phase.
3. Manufacturing ~~phase~~Phase.
4. System Integration and Testing Phase. ~~Testing phase~~
5. Installation and Commissioning Phase.

07.01-19

~~5.~~6. ~~Installation and commissioning phase~~Final Documentation Phase.

4.15 Controls exist in the RSS that allow manual actuation of RT.

4.16 Electrical isolation is provided on connections between the four PS divisions.

4.17 Communications independence is provided between PS equipment and non-Class 1E equipment.

4.18 The PS is designed so that safety-related functions required for design basis events (DBE) are performed in the presence of the following:

- Single detectable failures within the PS concurrent with identifiable but non-detectable failures.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the DBE requiring the safety function.

4.19 The equipment for each PS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.

4.20 Locking mechanisms are provided on the PS cabinet doors. Opened PS cabinet doors are indicated in the MCR.

4.21 Key lock switches are provided at the PS cabinets to restrict modifications to the PS software.

4.22 The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.

07.01-19

4.23 The PS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods.

4.24 The PS response time for RT and ESF signals is less than the value required to satisfy the design basis safety analysis response time assumptions.

5.0 Electrical Power Design Features

5.1 ~~The~~ Class 1E PS components ~~identified as Class1E in Table 2.4.1-1~~ are powered from ~~the~~ a Class 1E division ~~as listed in Table 2.4.1-1~~ in a normal or alternate feed condition.

6.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.1-7~~9~~ lists the PS ITAAC.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.13	The PS performs interlock functions.interlocks exist as provided in Table 2.4.1-8.	Tests will be performed on the as-built PS using test signals to simulate plant conditions that require the interlock functions operation of the interlocks listed in Table 2.4.1-86.	The PS generates the correct output signals for each interlock function listed in Table 2.4.1-6 when the test signals are such that the interlock function is required.interlocks exist as provided in Table 2.4.1-8.
4.14	The PS system design and application software are developed using a process composed of six life cycle phases, with each phase having outputs which must conform to the requirements of that phase. The six life cycle phases are the following: 1) Basic Design Phase. 2) Detailed Design Phase. 3) Manufacturing Phase. 4) System Integration and Testing Phase 5) Installation and Commissioning Phase. 6) Final Documentation Phase.The PS hardware and software are developed using a design process composed of five life cycle phases with each phase having design outputs which must conform to the requirements of that phase. The five life cycle phases are the	a. Analyses will be performed to verify that the outputs for the PS basic design phase conform to the requirements of that phase.Inspections will be performed to verify that the PS basic design phase process has design outputs. **{{DAC}}** b. Analyses will be performed to verify that the outputs for the PS detailed design phase conform to the requirements of that phase.Analyses will be performed to verify that the design outputs for the PS basic design phase conform to the requirements of that phase. **{{DAC}}** c. Analyses will be performed to verify that the outputs for the PS manufacturing phase conform to the requirements of that phase.Inspections will be performed to verify that the PS detailed design phase process has design outputs.	a. A report exists and concludes that the outputs conform requirements of the basic design phase of the PS. A report exists and provides the design outputs for the basic design phase of the PS hardware and software design process. **{{DAC}}** b. A report exists and concludes that the outputs conform to requirements of the detailed design phase of the PS.A verification and validation (V&V) report exists and concludes that the design outputs conform to the requirements of the PS basic design phase. **{{DAC}}** c. A report exists and concludes that the outputs conform to the requirements of the manufacturing phase of the PS.A report exists and provides the design outputs for the detailed design phase of the PS hardware and software design process.

07.01-19

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

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
~~following:~~ ~~1) Basic design phase.~~ ~~2) Detailed design phase.~~ ~~3) Manufacturing phase.~~ ~~4) Testing phase.~~ ~~5) Installation and commissioning phase.~~	d. ~~-~~Analyses will be performed to verify that the outputs for the PS system integration and testing phase conform to the requirements of that phase.~~Analyses will be performed to verify that the design outputs for the PS detailed design phase conform to the requirements of that phase.~~	d. A report exists and concludes that the outputs conform to the requirements of the system integration and testing phase of the PS.~~A V&V report exists and concludes that the design outputs conform to the requirements of the PS detailed design phase.~~
	e. Analyses will be performed to verify that the outputs for the PS installation and commissioning phase conform to the requirements of that phase.~~ Inspections will be performed to verify that the PS manufacturing phase process has design outputs~~.	e. A report exists and concludes that the outputs conform to the requirements of the installation and commissioning phase of the PS.~~A report exists and provides the design outputs for the manufacturing phase of the PS hardware and software design process.~~
	f. Analyses will be performed to verify that the outputs for the PS final documentation phase conform to the requirements of that phase. ~~Inspections will be performed to verify that the PS testing phase process has design outputs.~~	f. A report exists and concludes that the outputs conform to the requirements of the final documentation phase of the PS.~~A report exists and provides the design outputs for the testing phase of the PS hardware and software design process.~~
	~~g. Analyses will be performed to verify that the design outputs for the PS testing phase conform to the requirements of that phase.~~	~~g. A V&V report exists and concludes that the design outputs of the testing phase conform to the requirements of the PS testing phase.~~
	~~h. Inspections will be performed to verify that the PS installation and commissioning phase process has design outputs.~~	~~h. A report exists and provides the design outputs for the installation and commissioning phase of the PS hardware and software design process.~~

07.01-19

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
	07.01-19	i. Analyses will be performed to verify that the design outputs for the PS installation and commissioning phase conform to the requirements of that phase.	i. A V&V report exists and concludes that the design outputs of the PS installation and commissioning phase conform to the requirements of the installation and commissioning phase.
4.15	Controls exist in the RSS that allow manual actuation of RT.	a. Inspections will be performed to verify the existence of controls in the RSS. b. Tests will be performed to verify the correct functionality of the controls in the RSS.	a. Controls exist in the RSS that allow manual actuation of RT. b. The correct actuation signals are present at the RT devices after the corresponding controls in the RSS are manually activated.
4.16	Electrical isolation is provided on connections between the four PS divisions.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the four PS divisions. b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the four PS divisions. c. Inspections will be performed on connections between the four PS divisions.	a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between the four PS divisions. b. A report exists and concludes that the Class 1E isolation devices used between the four PS divisions prevent the propagation of credible electrical faults. c. Class 1E electrical isolation devices exist on connections between the four PS divisions.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.22	The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.	Analysis will be performed to demonstrate that the operational availability of each input variable listed in Table 2.4.1-2 and Table 2.4.1-3 can be confirmed during reactor operation including post-accident periods by one of the following methods: • By perturbing the monitored variable. • By introducing and varying, as appropriate, a substitute input of the same nature as the measured variable. • By cross-checking between channels that bear a known relationship to each other. • By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.	A report exists and concludes that the operational availability of each input variable listed in Table 2.4.1-2 and Table 2.4.1-3 can be confirmed during reactor operation including post-accident periods by one of the following methods: • By perturbing the monitored variable. • By introducing and varying, as appropriate, a substitute input of the same nature as the measured variable. • By cross-checking between channels that bear a known relationship to each other. • By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.
4.23	The PS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods. 07.-1-19	A TELEPERM XS platform changes analysis will be performed on the PS hardware and system software to verify its conformance to the key TELEPERM XS principles, features, and quality methods. **{{DAC}}**	A report exists and concludes that the PS hardware modules and system software modules: ~~A report exists and concludes that the PS hardware and software are designed to conform to the key TELEPERM XS principles, features, and methods.~~ **~~{{DAC}}~~** a. Conform to the key TELEPERM XS design principles. **{{DAC}}** b. Conform to the key TELEPERM XS processing features. **{{DAC}}**

4.3 Electrical isolation is provided on connections between the ~~safety~~ safety-related parts of the SICS and ~~the~~ non-Class 1E equipment. ~~safety I&C systems.~~

4.4 ~~The~~ Class 1E SICS equipment ~~classified as Class 1E in Table 2.4.2-1~~ can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

4.5 The SICS ~~hardware and software~~system design and application software are developed using a ~~design~~ process composed of ~~five~~ six life cycle phases with each phase having ~~design~~ outputs which must conform to the requirements of that phase. The ~~five~~ six life cycle phases are the following:

07.01-19

1. Basic ~~design~~ Design ~~phase~~Phase.
2. Detailed ~~design~~ Design ~~phase~~Phase.
3. Manufacturing ~~phase~~Phase.
4. System Integration and Testing phase.
5. Installation and ~~commissioning~~ Commissioning ~~phase~~Phase.
6. Final Documentation Phase.

4.6 Electrical isolation is provided on connections between the RSS and the MCR for the SICS.

4.7 Electrical isolation is provided on connections between the four SICS divisions.

4.8 Communications independence is provided between the four SICS divisions.

4.9 Communications independence is provided between SICS equipment and non-Class 1E equipment.

4.10 The SICS is designed so that safety-related functions required for design basis events (DBE) are performed in the presence of the following:

- Single detectable failures within the SICS concurrent with identifiable but non-detectable failures.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the DBE requiring the safety function.

4.11 The equipment for each SICS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.

4.12 Locking mechanisms are provided on the SICS cabinet doors located outside of the MCR. Opened SICS cabinet doors are indicated in the MCR.

4.13 Key lock switches on the QDS restrict connections between the QDS and the QDS service unit.

4.14 The SICS is capable of performing its safety function when one of the SICS divisions is out of service. Out of service divisions of SICS are indicated in the MCR.

07.01-19

4.15 The SICS PI hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods.

07.01-19

4.16 The SICS QDS hardware and system software are evaluated and accepted for use in safety-related applications through a commercial grade dedication process.

5.0 Electrical Power Design Features

5.1 ~~The~~ Class 1E SICS components ~~identified as Class 1E in Table 2.4.2-1~~ are powered from ~~the~~ a Class 1E division ~~as listed in Table 2.4.2-1~~ in a normal or alternate feed condition.

6.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.2-2 lists the SICS ITAAC.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.4	~~The~~ Class 1E SICS equipment ~~listed as Class 1E in Table 2.4.2-1~~ can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	Type tests, tests, analyses or a combination of these will be performed for the Class 1E equipment listed in Table 2.4.1-1.	A report exists and concludes that the equipment ~~listed~~ identified as Class 1E in Table 2.4.2-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.
4.5	The SICS system design and application software are developed using a process composed of six life cycle phases, with each phase having outputs which must conform to the requirements of that phase. The six life cycle phases are the following: 1) Basic Design Phase. 2) Detailed Design Phase. 3) Manufacturing Phase. 4) System Integration and Testing Phase 5) Installation and Commissioning Phase. 6) Final Documentation Phase.~~The SICS hardware and software are developed using a design process composed of five life cycle phases with each phase having design outputs which must conform to the requirements of that phase. The five life cycle phases are the following:~~	a. Analyses will be performed to verify that the outputs for the SICS basic design phase conform to the requirements of that phase. **{{DAC}}**~~a. Inspections will be performed to verify that the SICS basic design phase process has design outputs.~~	a. A report exists and concludes that the outputs conform requirements of the basic design phase of the SICS. **{{DAC}}**~~a. A report exists and provides the design outputs for the basic design phase of the SICS hardware and software design process.~~
		b. Analyses will be performed to verify that the outputs for the SICS detailed design phase conform to the requirements of that phase. **{{DAC}}**~~b. Analyses will be performed to verify that the design outputs for the SICS basic design phase conform to the requirements of that phase.~~	b. A report exists and concludes that the outputs conform to requirements of the detailed design phase of the SICS. **{{DAC}}**~~b. A verification and validation (V&V) report exists and concludes that the design outputs conform to the requirements of the SICS basic design phase.~~
		c. Analyses will be performed to verify that the outputs for the SICS manufacturing phase conform to the requirements of that phase.~~c. Inspections will be performed to verify that the SICS detailed design phase process has design outputs.~~	c. A report exists and concludes that the outputs conform to the requirements of the manufacturing phase of the SICS.~~c. A report exists and provides the design outputs for the detailed design phase of the SICS hardware and software design process.~~

07.01-19

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

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
~~1) Basic design phase.~~ ~~2) Detailed design phase.~~ ~~3) Manufacturing phase.~~ ~~4) Testing phase.~~ ~~5) Installation and commissioning phase.~~	d. Analyses will be performed to verify that the outputs for the SICS system integration and testing phase conform to the requirements of that phase.~~d. Analyses will be performed to verify that the design outputs for the SICS detailed design phase conform to the requirements of that phase.~~	d. A report exists and concludes that the outputs conform to the requirements of the system integration and testing phase of the SICS.~~d. A V&V report exists and concludes that the design outputs conform to the requirements of the SICS detailed design phase.~~
	e. Analyses will be performed to verify that the outputs for the SICS installation and commissioning phase conform to the requirements of that phase..~~e. Inspections will be performed to verify that the SICS manufacturing phase process has design outputs.~~	e. A report exists and concludes that the outputs conform to the requirements of the installation and commissioning phase of the SICS.~~e. A report exists and provides the design outputs for the manufacturing phase of the SICS hardware and software design process.~~
	f. Analyses will be performed to verify that the outputs for the SICS final documentation phase conform to the requirements of that phase.~~f. Inspections will be performed to verify that the SICS testing phase process has design outputs.~~	f. A report exists and concludes that the outputs conform to the requirements of the final documentation phase of the SICS.~~f. A report exists and provides the design outputs for the testing phase of the SICS hardware and software design process.~~
	~~g. Analyses will be performed to verify that the design outputs for the SICS testing phase conform to the requirements of that phase.~~	~~g. A V&V report exists and concludes that the design outputs of the testing phase conform to the requirements of the SICS testing phase.~~
	~~h. Inspections will be performed to verify that the SICS installation and commissioning phase process has design outputs.~~	~~h. A report exists and provides the design outputs for the installation and commissioning phase of the SICS hardware and software design process.~~

07.01-19

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
	07.01-19 →	~~i. Analyses will be performed to verify that the design outputs for the SICS installation and commissioning phase conform to the requirements of that phase.~~	~~i. A V&V report exists and concludes that the design outputs of the SICS installation and commissioning phase conform to the requirements of the installation and commissioning phase.~~
4.6	Electrical isolation is provided on connections between the RSS and the MCR for the SICS.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the RSS and the MCR for the SICS.	a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between the RSS and the MCR for the SICS.
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the RSS and the MCR for the SICS.	b. A report exists and concludes that the Class 1E isolation devices used between the RSS and the MCR for the SICS prevent the propagation of credible electrical faults.
		c. Inspections will be performed on connections between the RSS and the MCR for the SICS.~~An inspection will be performed.~~	c. Class 1E electrical isolation devices exist on connections between the RSS and the MCR for the SICS.~~Electrical isolation is provided between RSS and the MCR for the SICS.~~
4.7	Electrical isolation is provided on connections between the four SICS divisions.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the four SICS divisions.	a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between the four SICS divisions.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		c. Tests and inspections will be performed to verify an indication exists in the MCR when a SICS cabinet door located outside of the MCR is in the open position.	c. Opened SICS cabinet doors located outside of the MCR are indicated in the MCR.
4.13	Key lock switches on the QDS restrict connections between the QDS and the QDS service unit.	Tests will be performed to verify that the key lock switches on the QDS restrict modifications to the SICS software.	Key lock switches on the QDS restrict modifications to the SICS software.
4.14	The SICS is capable of performing its safety function when one of the SICS divisions is out of service. Out of service divisions of SICS are indicated in the MCR.	a. A test of the SICS will be performed to verify the SICS can perform its safety function when one of the SICS divisions is out of service. b. Inspections will be performed to verify the existence of indications in the MCR when a SICS division is placed out of service.	a. The SICS can perform its safety functions when one of the SICS divisions is out of service. b. Out of service divisions of SICS are indicated in the MCR.
4.15	The SICS PI hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods. **{{DAC}}**	A TELEPERM XS platform changes analysis will be performed on the SICS hardware and system software to verify its conformance to the key TELEPERM XS principles, features, and quality methods. **{{DAC}}**	A report exists and concludes that the ~~PS~~SICS PI hardware modules and system software modules: ~~A report exists and concludes that the SICS hardware and software are designed to conform to the key TELEPERM XS principles, features, and methods.~~ ~~**{{DAC}}**~~ a. Conform to the key TELEPERM XS design principles. **{{DAC}}**

07.01-19

07.01-19

Table 2.4.2-2—Safety Information and Control System ITAAC
07.01-19
(~~4~~ 8 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.16	The SICS QDS hardware and system software are evaluated and accepted for use in safety related applications through a commercial grade dedication process.	a. Analyses will be performed to determine the critical characteristics of the QDS. **{{DAC}}** b. Analyses will be performed to determine a combination of special tests, surveys, source verifications, or performance record reviews that is sufficient to demonstrate that the QDS exhibits the required critical characteristics. **{{DAC}}** c. Inspections, tests, analyses or a combination thereof will be performed to demonstrate that the QDS exhibits the required critical characteristics.	a. A report exists and defines the critical characteristics for acceptance of the QDS. **{{DAC}}** b. A dedication acceptance plan exists and defines a combination of special tests, surveys, source verifications, or performance reviews that is sufficient to demonstrate that the QDS exhibits the required critical characteristics. **{{DAC}}** c. A dedication acceptance package exists and documents results of special tests, surveys, source verifications, or performance reviews that demonstrate the QDS exhibits the required critical characteristics.
5.1	~~The~~ Class 1E SICS components ~~identified as Class 1E in Table 2.4.2-1~~ are powered from ~~the~~ a Class 1E division ~~as listed in Table 2.4.2-1~~ in a normal or alternate feed condition.	a. Testing will be performed for components identified as Class 1E in Table 2.4.2-1 by providing a test signal in each normally aligned division. b. Testing will be performed for components identified as Class 1E in Table 2.4.2-1 by providing a test signal in each division with the alternate feed aligned to the divisional pair.	a. The test signal provided in the normally aligned division is present at the respective Class 1E components identified in Table 2.4.2-1. b. The test signal provided in each division with the alternate feed aligned to the divisional pair is present at the respective Class 1E components identified in Table 2.4.2-1.

Next File

4.5 The SAS ~~hardware~~ system design and application software are developed using a ~~design~~ process composed of ~~five~~ six life cycle phases with each phase having ~~design~~ outputs which must conform to the requirements of that phase. The ~~five~~ six life cycle phases are the following:

07.01-19

1. Basic ~~design~~ Design ~~phase~~Phase.
2. Detailed ~~design~~ Design ~~phase~~Phase.
3. Manufacturing ~~phase~~Phase.
4. System Integration and Testing ~~phase~~Phase.
5. Installation and ~~commissioning~~ Commissioning ~~phase~~Phase.
6. Final Documentation Phase.

4.6 Electrical isolation is provided on connections between the four SAS divisions.

4.7 Electrical isolation is provided on connections between SAS equipment and non-Class 1E equipment.

4.8 Communications independence is provided between the four SAS divisions.

4.9 Communications independence is provided between SAS equipment and non-Class 1E equipment.

4.10 The SAS is designed so that safety-related functions required for design basis events (DBE) are performed in the presence of the following:

- Single detectable failures within the SAS concurrent with identifiable but non-detectable failures.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the DBE requiring the safety function.

4.11 The equipment for each SAS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.

4.12 Locking mechanisms are provided on the SAS cabinet doors. Opened SAS cabinet doors are indicated in the MCR.

4.13 Key lock switches are present at the SAS cabinets to restrict modifications to the SAS software.

4.14 The SAS is capable of performing its safety function when one of the SAS divisions is out of service. Out of service divisions of SAS are indicated in the MCR.

4.15 The operational availability of each input variable listed can be confirmed during reactor operation including post-accident periods.

07.01-19

4.16 The SAS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods.

5.0 Electrical Power Design Features

5.1 ~~The~~ Class 1E SAS components ~~identified as Class 1E in Table 2.4.4-1~~ are powered from ~~the~~ a Class 1E division ~~as listed in Table 2.4.4-1~~ in a normal or alternate feed condition.

6.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.4-5 lists the SAS ITAAC.

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.5	The SAS system design and application software are developed using a process composed of six life cycle phases, with each phase having outputs which must conform to the requirements of that phase. The six life cycle phases are the following: 1) Basic Design Phase. 2) Detailed Design Phase. 3) Manufacturing Phase. 4) System Integration and Testing Phase 5) Installation and Commissioning Phase. 6) Final Documentation Phase.~~The SAS hardware and software are developed using a design process composed of five life cycle phases with each phase having design outputs which must conform to the requirements of that phase. The five life cycle phases are the following:~~ ~~1) Basic design phase.~~ ~~2) Detailed design phase.~~ ~~3) Manufacturing phase.~~	a. Analyses will be performed to verify that the outputs for the SAS basic design phase conform to the requirements of that phase. {{**DAC**}}~~a. Inspections will be performed to verify that the SAS basic design phase process has design outputs.~~ b. Analyses will be performed to verify that the outputs for the SAS detailed design phase conform to the requirements of that phase. {{**DAC**}}~~b. Analyses will be performed to verify that the design outputs for the SAS basic design phase conform to the requirements of that phase.~~ c. Analyses will be performed to verify that the outputs for the SAS manufacturing phase conform to the requirements of that phase.~~c. Inspections will be performed to verify that the SAS detailed design phase process has design outputs.~~	a. A report exists and concludes that the outputs conform requirements of the basic design phase of the SAS. {{**DAC**}}~~a. A report exists and provides the design outputs for the basic design phase of the SAS hardware and software design process.~~ b. A report exists and concludes that the outputs conform to requirements of the detailed design phase of the SAS. {{**DAC**}}~~b. A verification and validation (V&V) report exists and concludes that the design outputs conform to the requirements of the SAS basic design phase.~~ c. A report exists and concludes that the outputs conform to the requirements of the manufacturing phase of the SAS.~~c. A report exists and provides the design outputs for the detailed design phase of the SAS hardware and software design process.~~

07.01-19

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

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
~~4) Testing phase.~~ ~~5) Installation and commissioning phase.~~	d. Analyses will be performed to verify that the outputs for the SAS system integration and testing phase conform to the requirements of that phase.~~d. Analyses will be performed to verify that the design outputs for the SAS detailed design phase conform to the requirements of that phase.~~	d. A report exists and concludes that the outputs conform to the requirements of the system integration and testing phase of the SAS.~~d. A V&V report exists and concludes that the design outputs conform to the requirements of the SAS detailed design phase.~~
	e. Analyses will be performed to verify that the outputs for the SAS installation and commissioning phase conform to the requirements of that phase..~~e. Inspections will be performed to verify that the SAS manufacturing phase process has design outputs.~~	e. A report exists and concludes that the outputs conform to the requirements of the installation and commissioning phase of the SAS.~~e. A report exists and provides the design outputs for the manufacturing phase of the SAS hardware and software design process.~~
	f. Analyses will be performed to verify that the outputs for the SAS final documentation phase conform to the requirements of that phase.~~f. Inspections will be performed to verify that the SAS testing phase process has design outputs.~~	f. A report exists and concludes that the outputs conform to the requirements of the final documentation phase of the SAS.~~f. A report exists and provides the design outputs for the testing phase of the SAS hardware and software design process.~~
	~~g. Analyses will be performed to verify that the design outputs for the SAS testing phase conform to the requirements of that phase.~~	~~g. A V&V report exists and concludes that the design outputs of the testing phase conform to the requirements of the SAS testing phase.~~

07.01-19

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
	07.01-19 →	~~h. Inspections will be performed to verify that the SAS installation and commissioning phase process has design outputs.~~	~~h. A report exists and provides the design outputs for the installation and commissioning phase of the SAS hardware and software design process.~~
		~~i. Analyses will be performed to verify that the design outputs for the SAS installation and commissioning phase conform to the requirements of that phase.~~	~~i. A V&V report exists and concludes that the design outputs of the SAS installation and commissioning phase conform to the requirements of the installation and commissioning phase.~~
4.6	Electrical isolation is provided on connections between the four SAS divisions.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the four SAS divisions.	a. A test plan exists that provides the test specification for determining whether a device is capable of preventing the propagation of credible electrical faults on connections between the four SAS divisions.
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the four SAS divisions.	b. A report exists and concludes that the Class 1E isolation devices used between the four SAS divisions prevent the propagation of credible electrical faults.
		c. Inspections will be performed on connections between the four SAS divisions.	c. Class 1E electrical isolation devices exist on connections between the four SAS divisions.

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

07.01-19

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.16	The SAS hardware and system software are designed to conform to the key TELEPERM XS principles, features, and quality methods. **{{DAC}}**	A TELEPERM XS platform changes analysis will be performed on the SAS hardware and system software to verify its conformance to the key TELEPERM XS principles, features, and quality methods. **{{DAC}}**	A report exists and concludes that the ~~PS~~SAS hardware modules and system software modules: ~~A report exists and concludes that the SAS hardware and software are designed to conform to the key TELEPERM XS principles, features, and methods.~~ **~~{{DAC}}~~** a. Conform to the key TELEPERM XS design principles. **{{DAC}}** b. Conform to the key TELEPERM XS processing features. **{{DAC}}** c. Conform to the key TELEPERM XS communication independence features. **{{DAC}}** d. Do not introduce more than a minimal increase in the likelihood of occurrence of a software malfunction relative to predecessor modules. **{{DAC}}** e. Do not introduce more than a minimal increase in the consequences of a malfunction relative to predecessor modules. **{{DAC}}** f. Do not create the possibility for a malfunction with a different result relative to predecessor modules. **{{DAC}}**

07.01-19

2.4.24 Diverse Actuation System

1.0 Description

The diverse actuation system (DAS) is a non-safety related digital I&C system.

The DAS provides the following non-safety related functions:

- Automatic anticipated transient without scram (ATWS) mitigation functions.
- Automatic PS software common cause failure mitigation functions.
- Automatic station blackout (SBO) mitigation functions.

2.0 Arrangement

2.1 The DAS equipment is located as listed in Table 2.4.24-1—Diverse Actuation System Equipment.

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

3.0 I&C Design Features, Displays and Controls

3.1 The DAS system design is accomplished through a phased approach which includes the following (or equivalent) phases:

07.01-19

1. System Requirements Phase.
2. System Design Phase.
3. Software/Hardware Requirements Phase.
4. Software/Hardware Design Phase.
5. Software/Hardware Implementation Phase.
6. Software/Hardware Validation Phase.
7. System Integration Phase.
8. System Validation Phase.

3.2 The system hardware and system software in the DAS are diverse from the system hardware and system software in the protection system (PS).

3.3 The DAS generates signals for automatic actuation of the functions identified in Table 2.4.24-2—Functions Automatically Actuated by the DAS.

3.4 The DAS allows manual, system-level actuation of the functions listed in Table 2.4.24-3.

Table 2.4.24-4—Diverse Actuation System ITAAC (2 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	The DAS equipment is located as listed in Table 2.4.24-1.	Inspections will be performed of the location of the DAS equipment.	The equipment listed in Table 2.4.24-1 is located as listed in Table 2.4.24-1.
2.2	Physical separation exists between the four divisions of the DAS.	Inspections will be performed to verify that the divisions of the DAS are located in separate buildings.	The four divisions of the DAS are located in separate safeguard buildings.
3.1	The DAS system design is accomplished through a phased approach which includes the following (or equivalent) phases: 1. System Requirements Phase. 2. System Design Phase. 3. Software/Hardware Requirements Phase. 4. Software/Hardware Design Phase. 5. Software/Hardware Implementation Phase. 6. Software/Hardware Validation Phase. 7. System Integration Phase. 8. System Validation Phase.	a. Analyses will be performed to verify that the outputs for the DAS system requirements phase conform to the requirements of that phase. **{{DAC}}** b. Analyses will be performed to verify that the outputs for the DAS system design phase conform to the requirements of that phase. **{{DAC}}** c. Analyses will be performed to verify that the outputs for the DAS software/hardware requirements phase conform to the requirements of that phase. **{{DAC}}** d. Analyses will be performed to verify that the outputs for the DAS software/hardware design phase conform to the requirements of that phase. **{{DAC}}** e. Analyses will be performed to verify that the outputs for the DAS software/hardware implementation phase conform to the requirements of that phase.	a. A report exists and concludes that the outputs for the DAS system requirements phase conform to the requirements of that phase. **{{DAC}}** b. A report exists and concludes that the outputs for the DAS system design phase conform to the requirements of that phase. **{{DAC}}** c. A report exists and concludes that the outputs for the DAS software/hardware requirements phase conform to the requirements of that phase. **{{DAC}}** d. A report exists and concludes that the outputs for the DAS software/hardware design phase conform to the requirements of that phase. **{{DAC}}** e. A report exists and concludes that the outputs for the DAS software/hardware implementation phase conform to the requirements of that phase.

07.01-19

Table 2.4.24-4—Diverse Actuation System ITAAC (2 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		f. Analyses will be performed to verify that the outputs for the DAS software/hardware validation phase conform to the requirements of that phase.	f. A report exists and concludes that the outputs for the DAS software/hardware validation phase conform to the requirements of that phase.
	07.01-19 →	g. Analyses will be performed to verify that the outputs for the DAS system integration phase conform to the requirements of that phase.	g. A report exists and concludes that the outputs for the DAS system integration phase conform to the requirements of that phase.
		h. Analyses will be performed to verify that the outputs for the DAS system validation phase conform to the requirements of that phase.	h. A report exists and concludes that the outputs for the DAS system validation phase conform to the requirements of that phase.
3.2	The system hardware and system software in the DAS are diverse from the system hardware and system software in the protection system (PS).	An analysis will be performed to demonstrate that the system hardware and system software in the DAS are diverse from the system hardware and system software in the PS.	A report exists and concludes that the system hardware and system software in the DAS are diverse from the system hardware and system software in the PS.
3.3	The DAS generates signals for automatic actuation of the functions identified in Table 2.4.24-2.	Tests will be performed on the as-built DAS using test signals.	The DAS generates signals for automatic actuation of the functions identified in Table 2.4.24-2.
3.4	The DAS allows manual, system-level actuation of the functions listed in Table 2.4.24-3.	Tests will be performed on the as-built DAS using test signals.	The DAS generates signals allowing manual actuation of the functions identified in Table 2.4.24-3.
3.5	Functions of the DAS that are not tested by the self-test features are identified and included in the periodic testing procedures.	a. An analysis is performed to identify functions of the DAS that are not tested by self-test features.	a. A report exists which identifies any functions of the DAS that are not tested by self-test features.

information for display to the operator. These systems also process manual commands to operate plant equipment.

- Level 0: process interface – These I&C systems act as the coupling between the physical process and the I&C systems. They include sensing components, actuation devices, and actuated equipment such as pressure sensors, thermocouples, switchgear, pumps and valves.

7.1.1.2 Use of TELEPERM XS and Qualified Display System in the U.S. EPR

07.01-19

TELEPERM XS (TXS) is a digital I&C platform that has been specifically designed and qualified for use in nuclear safety-related applications.

The qualified display system (QDS) is a digital human machine interface (HMI) that is qualified for use in safety-related applications through a commercial grade dedication process.

7.1.1.2.1 TXS Platform Design

The TXS platform is described in the Reactor Protection System Topical Report (EMF-2110(NP)(A) (Reference 6). Because of advances in technology and rapid obsolescence of components, the various modules described in EMF-2110(NP)(A) (Reference 6) will be modified and upgraded over time, and new modules will be developed. ~~However, the principles and methods described in EMF-2110(NP)(A) (Reference 6) and summarized below apply to the application of the TXS platform for the U.S. EPR.~~

The aspects of the TXS platform discussed in EMF-2110(NP)(A) can be classified in three broad categories:

1. Hardware design and qualification.
2. System software design and qualification.
3. Various configurations and arrangements of hardware and software to form a project-specific system architecture.

Modified, upgraded or new TXS hardware modules and system software modules will be used in the U.S. EPR without further NRC review provided they conform to the key TXS principles, features, and methods described in EMF-2110(NP)(A) and identified in ANP-10272. The U.S. EPR FSAR Tier 1, Chapter 2 sections for the PS, and SAS contain commitments that those systems' "hardware modules and system software modules conform to the key TELEPERM XS principles, features and quality methods." The criteria and evaluation process specified in TELEPERM XS Software Program Manual (ANP-10272) (Reference 8) Sections 4.1.1 through 4.1.4 is used to satisfy these Tier 1 commitments by determining that modified, upgraded or new

07.01-19

hardware modules and system software modules conform to the key TXS principles, features, and methods.

7.1.1.2.2 QDS Platform Design

The QDS was not included in the scope of EMF-2110NP(A), but is designed to interface with the standard TXS hardware and system software. The QDS hardware and system software are different from the standard TXS platform because the QDS performs video display functionality as opposed to system automation functionality. The QDS is qualified for use in safety-related applications through a commercial grade dedication process that conforms to the guidance of EPRI TR-106439, "Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (Reference 43).

07.01-19

The U.S. EPR-specific I&C system architectures that will be implemented using the TXS and QDS platforms are described in Section 7.1 for NRC review against the current regulations and guidance. The U.S EPR-specific system architectures supersede the example system architectures that were included in EMF-2110(NP)(A) to provide context for the review of the generic TXS platform.

- ~~Platform design using four building blocks, which include:~~
  - ~~System hardware.~~
  - ~~System software.~~
  - ~~Application software.~~
  - ~~Engineering tools to configure the application.~~
- ~~System hardware, system software, and engineering tools development processes that meet the quality requirements of 10 CFR 50.55a(a)(1) and GDC 1. This includes software verification and validation (V&V) methods.~~
- ~~Processing principles that provide for system integrity, which include:~~
  - ~~Real-time, static operating system.~~
  - ~~Cyclic processing.~~
  - ~~Interference-free communications.~~
  - ~~Self-monitoring and diagnostics.~~
  - ~~Fail-safe design.~~
- ~~Control of access principles, including service unit (SU) maintenance interfaces.~~

~~The TXS product family also extends to other modules and components outside of those described in EMF-2110(NP)(A) (Reference 6). Examples include the priority module described in AV42 Topical Report (ANP-10273P) (Reference 7), and the qualified display system (QDS). The QDS is a video display unit designed for use in nuclear safety-related applications. Modules and components that are developed for use in I&C systems design shall be consistent with the requirements described in this chapter.~~

7.1.1.2.3 Application of the TXS ~~Platform~~and QDS Platforms

07.01-19

TELEPERM XS Software Topical Report (ANP-10272) (Reference 8) describes the lifecycle processes for application software development used in safety-related applications of the TXS and QDS platforms for the U.S. EPR, as well as software V&V processes. These phases are listed below along with the primary activities included in ~~documentation generated at the end of~~ each phase:

- Basic design:
  - System requirements.
  - System design.
  - Software requirements.
  - Initiate software requirements traceability.
  - Summary reports for V&V activities (i.e., acquisition support, planning, concept, and requirements).
- Detailed design:
  - Software design.
  - Automatic code generation.
  - Application software integration validation test planning (using an NRC-approved simulation test tool).
  - Application software integration validation test execution (using an NRC-approved simulation test tool).
  - Application software integration validation test reporting (using an NRC-approved simulation test tool).
  - Software safety analyses.
  - Continue software requirements traceability.
  - Hardware design.

07.01-19

- Summary reports for V&V activities (i.e., design and implementation.

- Manufacturing:
  - Hardware manufacturing.
  - Approval of supplier manufactured, tested hardware, and required supplier hardware documentation.
  - Cabinet design.
  - Cabinet internal wiring design.
- System integration and testing:
  - Integration of hardware and software.
  - Software integration, system and acceptance validation test planning.
  - Software integration, system and acceptance validation test execution.
  - Software integration, system and acceptance validation test reporting.
  - Continue software requirements traceability.
  - Summary reports for V&V activities.
- Installation and commissioning:
  - Installation and commissioning test planning.
  - Installation and commissioning test execution.
  - Installation and commissioning test reporting.
  - Summary reports for V&V activities.
- Final Documentation:
  - Generation of final documentation before system is placed in service.

The primary documentation generated as outputs of each of these phases is described in ANP-10272 (Reference 8), Section 4.5. While the development of the QDS application software is performed in accordance with the lifecycle and configuration controls defined in ANP-10272 for the standard TXS platform, there is one difference: the development tools to create the application software (i.e., SPACE) described in ANP-10272 are not used to create QDS application software. The QDS-specific tools are qualified as part of the commercial grade dedication process described in Section 7.1.1.2.2. Once qualified, these tools will be controlled under configuration management as required by IEEE 7-4.3.2-2003, Section 5.3.2.

07.01-19

- ~~Basic design phase:~~
  - ~~Functional requirements specification.~~
  - ~~Software requirement specification.~~
  - ~~Hardware requirement specification.~~
  - ~~Concept activity V&V summary report.~~
  - ~~Requirements activity V&V summary report.~~
- ~~Detailed design phase:~~
  - ~~Software design description.~~
  - ~~Cabinet design and layout.~~
  - ~~Code generation and documentation.~~
  - ~~Software test plan.~~
  - ~~Software test report.~~
  - ~~Design activity V&V summary report.~~
  - ~~Implementation activity V&V summary report.~~
- ~~Manufacturing Phase.~~
- ~~Testing Phase:~~
  - ~~Factory acceptance test plan.~~
  - ~~Factory acceptance test report.~~
  - ~~Test activity V&V summary report.~~
- ~~Installation and Commissioning Phases:~~
  - ~~Site acceptance test plan.~~
  - ~~Site acceptance test report.~~
  - ~~Installation and checkout activity V&V summary report if required for any changes following testing phase.~~

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

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

GWs are provided to interface to the plant data network.

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

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

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

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

SUs are provided for configuration and maintenance of the SICS. The PIs are serviced by the SUs of the safety automation system (SAS) via the monitoring and service interface (MSI) of the SAS. The QDSs have dedicated non-safety-related SUs that are only connected to the QDS when the QDS is out of service. They are normally isolated through a key lock switch. The number and location of SUs is determined based on the number and layout of QDSs.

Equipment

07.01-19

The SICS is implemented with the TXS digital I&C platform, the QDS platform, and hardwired I&C equipment.

The PIs utilize the TXS platform and generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. The QDS consists of a computer, video display with touch screen capabilities, and input devices such as a keyboard and trackball. The hardwired I&C consists of conventional HMI devices such as buttons, switches, and analog and digital indicators that are hardwired from the various I&C systems. Fiber optic and copper cable are used for the various data and hardwired connections.

Qualification Requirements

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

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

07.01-19

Quality for the QDS platform is described in Section 7.1.1.2.2.

The application software used in the safety-related portion of the SICS is developed using the lifecycle processes described in Section 7.1.1.2.~~3~~2. 07.01-19

Diversity Requirements

The SICS is credited in the defense-in-depth and diversity analysis described in Section 7.8.2. The manual reactor trip actuation is implemented from the SICS using a hardwired path that is not affected by a software common cause failure (CCF) of the SICS or PS.

Data Communications

Data communications implemented in the safety-related portion of the SICS include:

- PS-SICS (Control) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Control) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- PS-SICS (Monitoring) – uni-directional (PS to SICS), point-to-point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Monitoring) – uni-directional (SAS to SICS), point-to-point data connections implemented with the TXS Profibus protocol.
- PI-QDS (Control) – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- PI-QDS (Monitoring) – uni-directional (PI to QDS), point-to-point data connections implemented with the TXS Ethernet protocol.
- PI-PI (Monitoring) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. This network is provided to allow the display of redundant divisional information on a single QDS for optimization of the human

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

Details on these functional units, along with details of the PS architecture, are described in Digital Protection System ~~Topical~~Technical Report (ANP-~~10281~~10309P) (Reference 9).

Equipment

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

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

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

Qualification Requirements

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

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

The application software used in the PS is developed using the lifecycle processes described in Section 7.1.1.2.3~~2~~. ← 07.01-19

Qualification Requirements

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

Quality Requirements

Quality for the TXS platform is described inSection 7.1.1.2.1.

The application software used in the SAS is developed using the lifecycle processes described in Section 7.1.1.2.32. 07.01-19

Diversity Requirements

There are no equipment diversity requirements for the SAS.

Data Communications

Data communications implemented in the SAS are:

- CU-CU (A or B) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. This network is provided to implement signal selection algorithms using redundant sensors for improved reliability in the control of safety-related processes. Separate connections are used for redundancies A and B. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4.

- CU-MSI – bi-directional, point to point data connections implemented with the TXS Profibus protocol.

- SAS-SICS (Control) – refer to Section 7.1.1.3.1.

- SAS-SICS (Monitoring) – refer to Section 7.1.1.3.1.

- MSI-GW – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol. This network is provided to allow monitoring and control of the SAS from the PICS. The design features that provide for independence between safety-related and non-safety-related systems are described in Section 7.1.1.6.4.

- MSI-SU – 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 design features that provide for independence between safety-related and non-safety-related systems are described in Section 7.1.1.6.4.

- GW-Plant Data Network – non-safety-related, divisional, bi-directional, networked communications.

37. BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

38. BTP 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

39. BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

40. BTP 7-21, "Guidance on Digital Computer Real-Time Performance," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

41. BTP 5-2, "Overpressurization Protection of Pressurized-Water Reactors While Operating at Low Temperatures," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

42. EMF-2341(P), Revision 1, "Generic Strategy for Periodic Surveillance Testing of TELEPERM™ XS Systems in U.S. Nuclear Generating Stations," Siemens Power Corporation, March 2000.

07.01-19

43. ERPI TR-106439, "Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, October 1996.