ArevaEPRDCPEm Resource

From: WELLS Russell D (AREVA NP INC) [Russell.Wells@areva.com]
Sent: Friday, June 12, 2009 5:33 PM
To: Tesfaye, Getachew
Cc: Pederson Ronda M (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 78, FSAR Ch 14, Supplement 2
Attachments: RAI 78 Supplement 2 Response US EPR DC.pdf

Getachew,

AREVA NP Inc. (AREVA NP) provided responses to 4 of the 6 questions of RAI No. 78 on November 3, 2008. AREVA NP informed NRC on March 26, 2009 that technically correct and complete responses could not be provided as scheduled for RAI No. 78, Questions 14.03.05-3 and 14.03.05-4. AREVA NP indicated that technically correct and complete responses for these questions would be provided by June 12, 2009. The attached file, "RAI 78 Supplement 2 US EPR DC.pdf," provides technically correct and complete responses to the remaining 2 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 78 Questions 14.03.05-3 and 14.03.05-4.

The following table indicates the respective pages in the response document, "RAI 78 Supplement 2 US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 78 — 14.03.05-3	2	2
RAI 78 — 14.03.05-4	3	48

This concludes the formal AREVA NP response to RAI 78, and there are no questions from this RAI for which AREVA NP has not provided responses.

Sincerely,

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

From: Pederson Ronda M (AREVA NP INC)
Sent: Thursday, March 26, 2009 5:28 PM
To: 'Getachew Tesfaye'
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); DUNCAN Leslie E (AREVA NP INC)
Subject: RE: Response to U.S. EPR Design Certification Application RAI No. 78, FSAR Ch 14

Getachew,

Based upon feedback from the NRC staff, AREVA NP is modifying the I&C architecture and rewriting I&C digital control system ITAAC. Therefore, AREVA NP is unable to provide technically correct and complete responses to the questions that were scheduled to be completed by March 27, 2009.

The schedule for technically correct and complete responses to the remaining two questions has been revised as provided below.

Question #	Response Date
RAI 78 — 14.03.05-3	June 12, 2009
RAI 78 — 14.03.05-4	June 12, 2009

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: WELLS Russell D (AREVA NP INC)
Sent: Monday, November 03, 2008 5:59 PM
To: 'Getachew Tesfaye'
Cc: 'John Rycyna'; Pederson Ronda M (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 78, FSAR Ch 14

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 78 Response US EPR DC.pdf" provides technically correct and complete responses to 4 of the 6 questions.

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 78 Questions 14.03.05-5 and 14.03.05-6.

The following table indicates the respective pages in the response document "RAI 78 Response US EPR DC.pdf" that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 78 — 14.03.05-1	2	2
RAI 78 — 14.03.05-2	3	3
RAI 78 — 14.03.05-3	4	4
RAI 78 — 14.03.05-4	5	5
RAI 78 — 14.03.05-5	6	6
RAI 78 — 14.03.05-6	7	8

A complete answer is not provided for 2 of the 6 questions. The schedule for a technically correct and complete response to this question is provided below.

Question #	Response Date
RAI 78 — 14.03.05-3	March 27, 2009
RAI 78 — 14.03.05-4	March 27, 2009

Sincerely,

(Russ Wells on behalf of)

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

From: Getachew Tesfaye [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Friday, October 03, 2008 6:28 PM
To: ZZ-DL-A-USEPR-DL
Cc: Joseph Ashcraft; Michael Miernicki; Terry Jackson; Joseph Colaccino; John Rycyna
Subject: U.S. EPR Design Certification Application RAI No. 78 (958), FSAR Ch14

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on September 12, 2008, and discussed with your staff on September 25, 2008. Draft RAI Questions 14.03.05-1 and 14.03.05-4 were modified 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: 574

Mail Envelope Properties (1F1CC1BBDC66B842A46CAC03D6B1CD410195306F)

Subject: Response to U.S. EPR Design Certification Application RAI No. 78, FSAR Ch 14, Supplement 2
Sent Date: 6/12/2009 5:32:58 PM
Received Date: 6/12/2009 5:33:06 PM
From: WELLS Russell D (AREVA NP INC)

Created By: Russell.Wells@areva.com

Recipients:
"Pederson Ronda M (AREVA NP INC)" <Ronda.Pederson@areva.com>
Tracking Status: None
"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen V (AREVA NP INC)" <Karen.Delano@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	5764	6/12/2009 5:33:06 PM
RAI 78 Supplement 2 Response US EPR DC.pdf	605255	

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

Response to

Request for Additional Information No. 78, Supplement 2

10/3/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 14.03.05 - Instrumentation and Controls - Inspections, Tests, Analyses, and Acceptance Criteria
Application Section: 14.3
ICE1 Branch

Question 14.03.05-3:

Demonstrate how ITAAC addresses the digital safety system security guidance provided in Rev. 2 of Regulatory Guide (RG) 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants."

ITAAC should verify that the application conforms with Regulatory Positions 2.1-2.9 in RG 1.152. How is ITAAC addressing security as described in above RG and cyber security in general?

Response to Question 14.03.05-3:

AREVA NP believes that the waterfall lifecycle phases described in Regulatory Guide (RG) 1.152, Revision 2, Regulatory Positions 2.1 through 2.9 for the protection of digital safety systems are intended to be controlled through the cyber security program required by 10 CFR 73.54(d). This consideration is consistent with the provisions in RG 5.71, Revision 0, January 2009, Section 3.4.1.1.1, Life Cycle Phases Activities. RG 5.71 states: "The licensees bears sole responsibility for ensuring that the potential for adverse effects on safety, security, and emergency preparedness is assessed and managed to provide a high assurance that critical functions are adequately protected from cyber attacks." Thus, U.S. EPR FSAR Tier 1 ITAAC does not explicitly address the cyber security design.

To incorporate the requirements of 10 CFR 73.54 (74 FR 13970, March 27, 2009), U.S. EPR FSAR Tier 2, Table 1.8-2 and Section 13.6 will be revised to include a new combined License Information Item (13.6-4) incorporating a new operational program: "A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54." U.S. EPR FSAR Tier 2, Section 13.4 will also be revised to include the new operational program.

Information regarding how the U.S. EPR FSAR implements RG 1.152 for systems within the scope of the design certification is also available in ANP-10295, "U.S. EPR Security Design Features" (Safeguards Information), Table B-1—TXS System Alignment with Regulatory Guide 1.152. This technical report was submitted in the Response to RAI 42, Question 14.03.12-1.

FSAR Impact:

U.S. EPR FSAR Tier 2, Table 1.8-2, Section 13.4, and Section 13.6 will be revised as described in the response and indicated on the enclosed markup.

Question 14.03.05-4:

Identify which Inspection, Tests, Analysis, and Acceptance Criteria (ITAAC) address the following aspects of safety systems identified in Tier 1, Section 2.4 and describe how the ITAAC address these aspects:

1. Environmental Qualification of equipment (temperature, humidity, etc.)
2. Not only the existence, but proper operation of equipment used to transfer control from the main control room to the remote shutdown station.
3. Not only the existence, but proper operation of permissive and bypass functions, including automatic removal of bypasses
4. Physical and cyber access controls are present and functional
5. Proper identification of instrumentation and control (I&C) components

10 CFR 52.47(b)(1) requires, in part, that ITAAC are necessary and sufficient to provide reasonable assurance that if the ITAAC are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. One of the regulations affecting safety-related I&C systems is 10 CFR 50.55a(h), which endorses IEEE Std. 603-1991. IEEE Std. 603 provides criteria for safety systems, including equipment qualification, manual control, operating bypasses, and identification of equipment. The staff could not identify ITAAC that addressed the above mentioned aspects of IEEE Std. 603 criteria. For example, the staff identified ITAAC addressing seismic and electromagnetic interference qualification of equipment, but not environmental aspects such as temperature. Also, some ITAAC addressed the existence of equipment and features, but not their proper operation. Completion of the ITAAC should provide assurance that the criteria in 10 CFR 50.55a(h) are met for the installed instrumentation and control system.

Response to Question 14.03.05-4:

The response to this question has six parts. The first five parts address the five points made in the first paragraph of the question. The last part of this response demonstrates how safety-related I&C systems ITAAC addresses the requirements discussed in the second paragraph of the question.

1. In cases where Class 1E I&C equipment will be located in a harsh environment, ITAAC is provided to verify qualification of such equipment. For example, U.S. EPR FSAR Tier 1, Table 2.4.19-2, Item 5.1 provides verification that the Class 1E equipment located in a harsh environment will perform their safety function in the environments that exist before and during the time required to perform their safety function.

   ITAAC are not required, however, for equipment that will be located in a mild environment. AREVA NP considers equipment qualification to mild environments to be less safety-significant than equipment qualification to harsh environments. AREVA NP established a graded approach to the development of U.S. EPR FSAR Tier 1 as described in Standard Review Plan (SRP) 14.3. SRP 14.3, page 14.3-2 provides a general discussion on the graded approach to ITAAC:

"The type of information and the level of detail in Tier 1 are based on a graded approach commensurate with the safety significance of the structures, systems, and components (SSCs) for the design. The top-level information selected should include the principal performance characteristics and safety functions of the SSCs and should be verified appropriately by ITAAC. Design-specific and unique features of the facility should be considered carefully for inclusion in Tier 1. The SRP Section 14.3 subsections provide specific review area guidance."

2. The Response to RAI 123, Supplement 2, Question 14.03.05-14 provided ITAAC items that verify the capability to transfer control from the main control room (MCR) to the remote shutdown station (RSS).
3. U.S. EPR FSAR Tier 1, Table 2.4.1-7—Protection System ITAAC , Item 4.3 verifies the existence of the operating bypasses and tests the proper operation of operating bypasses associated with the protection system (PS).
4. ITAAC will be added to U.S. EPR FSAR Tier 1, Section 2.4.1 to address physical and cyber access controls that are present and functional. Similar ITAAC will be added to U.S. EPR FSAR Tier 1, Section 2.4.2, Section 2.4.4, and Section 2.4.5 for the safety information and control system (SICS), safety automation system (SAS), and priority and actuator control system (PACS), respectively.
5. ITAAC will be added to U.S. EPR FSAR Tier 1, Section 2.4.1 to address the proper identification of I&C components in the PS. Similar ITAAC will be added to U.S. EPR FSAR Tier 1, Section 2.4.2, Section 2.4.4, and Section 2.4.5 for the SICS, SAS, and PACS, respectively.
6. This item presents an ITAAC map for the list of safety-related I&C requirements provided in SRP Section 14.3, Appendix C. The ITAAC map is presented in Table 14.03.05-1—ITAAC Mapping of I&C System Requirements. The ITAAC provided in U.S. EPR FSAR Tier 1, Section 2.4.1 (Protection System), Section 2.4.2 (Safety Information and Control System), Section 2.4.4 (Safety Automation System), and Section 2.4.5 (Priority and Actuator Control System) are mapped to the list of requirements in SRP Section 14.3, Appendix C, Part II under the Instrumentation and Control Systems Review Checklist. Requirements justification tables are provided for the above sections in Table 14.03.05-2—Requirements Justification for Protection System, Table 14.03.05-3—Requirements Justification for Safety Information and Control System, Table 14.03.05-4—Requirements Justification for Safety Automation System, and Table 14.03.05-5—Requirements Justification for Priority and Actuator Control System. The requirements justification tables explain how each ITAAC addresses the requirements listed in SRP Section 14.3, Appendix C.

FSAR Impact:

U.S. EPR FSAR Tier 1, Table 1.3-1, Section 2.4.1, Section 2.4.2, Section 2.4.4, Section 2.4.5, and Section 2.4.10 will be revised as described in the response and indicated on the enclosed markup.

Table 14.03.05-1—ITAAC Mapping of I&C System Requirements (5 Sheets)

Requirement	Description	PS (Tier 1, Section 2.4.1, ITAAC #)	SICS (Tier 1 Section 2.4.2, ITAAC #)	SAS (Tier 1 Section 2.4.4, ITAAC #)	PACS (Tier 1 Section 2.4.5, ITAAC #)
Safety System Designation					
IEEE 603 Clause 4.1	Applicable Design Basis Events	4.14	4.5	4.5	See Note 11
IEEE 603 Clause 4.4	Variables/ Analytical Limits	4.6; 4.7; 4.14	4.5	4.2; 4.5	See Note 1
IEEE 603 Clause 4.5	Criteria for Manual Action	4.14; See Note 10	4.5; See Note 10	4.5; See Note 10	See Note 2
IEEE 603 Clause 4.6	Number and Location of Sensors for Variables with Spatial Dependence	4.14	4.5	4.5	See Note 1
IEEE 603 Clause 4.7	Range of Conditions	4.14	4.5	4.5	See Note 16
IEEE 603 Clause 4.8	Conditions having the potential for functional degradation	4.14	4.5	4.5	See Note 16
IEEE 603 Clause 4.9	Methods to be used to determine reliability	4.14	4.5	4.5	See Note 16
Safety System Criteria					
IEEE 603 Clause 5.1	Single Failure Criterion	4.18	4.10	4.10	See Note 3
IEEE 603 Clause 5.2	Completion of Protective Action	See Note 4	See Note 4	See Note 4	See Note 4
IEEE 603 Clause 5.3	Quality	4.8; 4.10; 4.14; 4.17	4.3; 4.4; 4.5; 4.8	4.1; 4.5; 4.6; 4.8	4.2; 4.3
IEEE 603 Clause 5.4	Equipment Qualification	3.1; 4.8; 4.17	3.1; 4.3; 4.8	3.1; 4.6; 4.8	3.1; 4.2
IEEE 603 Clause 5.5	System Integrity	3.1; 4.10	3.1; 4.4	3.1; 4.1	3.1; 4.3
IEEE 603 Clause 5.6	Independence	2.1; 2.2; 4.4; 4.8; 4.16; 4.17	2.1; 4.3; 4.7; 4.8; 4.9; See Note 20	2.1; 2.2; 4.6; 4.7; 4.8; 4.9	2.1; 2.2; 4.2
IEEE 603 Clause 5.7	Capability for Test and Calibration	4.5	4.14	4.14	4.5
IEEE 603 Clause 5.8	Information Displays	4.5; See Note 10	4.14; See Note 10	4.14; See Note 10	See Note 10

Table 14.03.05-1—ITAAC Mapping of I&C System Requirements (5 Sheets)

Requirement	Description	PS (Tier 1, Section 2.4.1, ITAAC #)	SICS (Tier 1 Section 2.4.2, ITAAC #)	SAS (Tier 1 Section 2.4.4, ITAAC #)	PACS (Tier 1 Section 2.4.5, ITAAC #)
IEEE 603 Clause 5.9	Control of Access	4.20; 4.21	4.12; 4.13	4.12; 4.13	4.6
IEEE 603 Clause 5.10	Repair	4.5	4.14	4.14	See Note 7
IEEE 603 Clause 5.11	Identification	4.19	4.11	4.11	4.7
IEEE 603 Clause 5.12	Auxiliary Features	4.8; 4.16; See Note 9	4.3; 4.7; See Note 9	4.8; 4.9; See Note 9	See Note 9
IEEE 603 Clause 5.13	Multi- Unit Stations	See Note 8	See Note 8	See Note 8	See Note 8
IEEE 603 Clause 5.14	Human Factors Considerations	See Note 10	See Note 10	See Note 10	See Note 10
IEEE 603 Clause 5.15	Reliability	4.18	4.10	4.10	See Note 3
Sense and Command Features					
IEEE 603 Clause 6.1	Automatic Control	4.1; 4.2	See Note 12	4.3; 4.4	4.1
IEEE 603 Clause 6.2	Manual Control	4.11; 4.12; 4.15	See Note 13	See Note 13	See Note 13
IEEE 603 Clause 6.3	Interaction Between the Sense and Command and Other Systems	2.2; 4.8; 4.16	4.7	2.2; 4.8; 4.9	2.2; 4.2
IEEE 603 Clause 6.4	Derivation of System Inputs	4.7	See Note 17	4.2	See Note 1
IEEE 603 Clause 6.5	Capability for Testing and Calibration	4.22	See Note 18	4.15	See Note 1
IEEE 603 Clause 6.6	Operating Bypasses	4.3	See Note 14	See Note 14	See Note 14
IEEE 603 Clause 6.7	Maintenance Bypass	4.5	4.14	4.14	See Note 19
IEEE 603 Clause 6.8	Setpoints	4.6	See Note 15	See Note 15	See Note 15
Executive Features					
IEEE 603 Clause 7.3	Completion of Protective Action	See Note 4	See Note 4	See Note 4	See Note 4
Power Source Requirements					
IEEE 603 Clause 8	Electrical Power Sources	5.1	5.1	5.1	5.1
General Design Criteria					
GDC 1	Quality Standards and Records	3.1; 4.14	3.1; 4.4; 4.5	3.1; 4.1; 4.5	3.1; 4.3

Table 14.03.05-1—ITAAC Mapping of I&C System Requirements (5 Sheets)

Requirement	Description	PS (Tier 1, Section 2.4.1, ITAAC #)	SICS (Tier 1 Section 2.4.2, ITAAC #)	SAS (Tier 1 Section 2.4.4, ITAAC #)	PACS (Tier 1 Section 2.4.5, ITAAC #)
GDC 2	Design Bases for Protection Against Natural Phenomena	2.1; 3.1	2.1; 3.1	2.1; 3.1	2.1; 3.1
GDC 4	Environmental and Dynamic Effects Design Bases	2.1	2.1; 4.4	2.1; 4.1	2.1; 4.3
GDC 13	Instrumentation and Control	4.11; See Note 10	See Note 10	See Note 10	See Note 10
GDC 19	Control Room	4.15; See Note 10	4.1; See Note 10	See Note 10	See Note 10
GDC 20	Protection System Functions	4.1; 4.2	See Note 5	See Note 5	See Note 5
GDC 21	Protection System Reliability and Testability	3.1; 4.5; 4.10	See Note 5	See Note 5	See Note 5
GDC 22	Protection System Independence	4.17	See Note 5	See Note 5	See Note 5
GDC 23	Protection System Failure Modes	4.18	See Note 5	See Note 5	See Note 5
GDC 24	Separation of Protection and Control Systems	4.8	See Note 5	See Note 5	See Note 5
GDC 25	Protection System Requirements for Reactivity Control Malfunctions	4.1	See Note 5	See Note 5	See Note 5
GDC 29	Protection Against Anticipated Operational Occurrences	4.1; 4.2; 4.14	See Note 5	See Note 5	See Note 5
Branch Technical Position					
BTP 7-14	Guidance on Software in Digital Computer Based I&C	4.14	4.5	4.5	See Note 6

Notes:

1. The PACS does not receive plant variable inputs from sensors. Inputs to PACS are from the other I&C systems.
2. The criteria for manual control of safety functions is provided by the safety I&C systems that generate the manual control signals.
3. Single failure and reliability analyses on the PACS is bounded by mechanical system single failure and reliability analyses.
4. Completion of protective action is verified by several ITAAC. ITAAC item 4.2 in section 2.4.1 verifies that an ESF actuation signal remains as long as conditions that represent the completion of the function do not exist and requires deliberate operator action to be returned to normal. ITAAC item 4.4 in section 2.4.5 verifies proper connections from the other I&C systems to the PACS. Various mechanical system PACS ITAAC is provided that verifies that the actuator responds to the state requested by the test signal sent to the PACS. Examples of this ITAAC can be found in Tier 1, sections 2.2.1, 2.2.3, 2.2.4, 2.2.7, 2.6.1, 2.6.6, 2.7.1, 2.7.2, 2.7.11. All ITAAC items mentioned above provide verification that completion of protective action requirement is satisfied.
5. GDC 20, 21, 22, 23, 24, 25, and 29 apply only to the Protection System.
6. The PACS does not contain a software lifecycle because the PACS does not contain software.
7. Repair of PACS is facilitated by the mechanical safety systems capability to remove a train from service and still provide their safety function.
8. Sharing of SSCs between units at multi generating stations does not exist, therefore no ITAAC exists for this requirement.
9. Examples of ITAAC verifying that auxiliary supporting features meet the requirements can be found in Tier 1, section 2.5.1 ,item 5.2 (EPSS); section 2.5.2, item 5.1 (EUPS); section 2.5.4, item 3.14 (EDG lubricating oil system); section 2.6.7, item 6.1(SG Building ventilation).
10. The Human Factors Engineering (HFE) ITAAC in Tier 1, section 3.4 address this requirement.
11. Documentation of applicable design basis events is addressed by ITAAC item 4.14 in Section 2.4.1 and by ITAAC item 4.5 in Section 2.4.4.
12. Automatic initiation and control of protective actions is covered by ITAAC in Sections 2.4.1 (PS), 2.4.4 (SAS) and 2.4.5 (PACS).
13. Means for manual control are addressed by ITAAC items 4.11, 4.12, and 4.15 in Section 2.4.1. Portions of Clause 6.2 concerning the availability of operator controls and displays will be addressed by HFE ITAAC in Section 3.4.
14. The proper operation of automatic bypasses is addressed by ITAAC item 4.3 in Section 2.4.1.
15. ITAAC item 4.6 in section 2.4.1 addresses the determination of setpoints associated with analytical limits.
16. Documentation of Clauses 4.7, 4.8 and 4.9 are addressed by ITAAC item 4.14 in Section 2.4.1.

17. The SICS does not receive sense and command feature input signals. These signals are received by the PS and SAS. ITAAC item 4.7 in section 2.4.1 and ITAAC item 4.2 in Section 2.4.4 address sense and command feature inputs.
18. The capability for testing the operational availability of each sense and command feature input is provided in ITAAC item 4.22 in Section 2.4.1 and ITAAC item 4.15 in Section 2.4.4.
19. Maintenance bypass of PACS occurs when its associated individual safety related equipment is removed from service. The removal of safety related equipment from service is administratively controlled such that safety functions remain operable.
20. ITAAC item 2.2 in Section 3.6 provides physical separation of cabling between Class 1E cabling of different divisions and between Class 1E and non class 1E cabling in the MCR and RSS (locations of SICS).

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
2.1	PS equipment is located as listed in Table 2.4.1-1.	GDC 2 – Design Bases for protection against natural phenomena	GDC 2- The verification that the redundant portions of the system are located in separate safeguards buildings demonstrates protection against natural phenomena.
		GDC 4 – Environmental and dynamic effects design bases.	GDC 4- The fact that the safeguards building structures are designed to provide protection from environmental and design bases effects, the location of the PS equipment in these buildings demonstrates the equipment can withstand such effects.
		IEEE 603, Clause 5.6.2 – Independence between safety systems and effects of design bases event.	IEEE 603, Clause 5.6.2 – This ITAAC verifies that the PS equipment resides in buildings that provide protection from the effects of a design basis event (DBE). The safeguards buildings are designed to protect the equipment from the effects of a DBE.
2.2	Physical separation exists between the four divisions of the PS.	IEEE 603, Clause 5.6.1 – Independence between redundant portions of a safety system.	IEEE 603, Clause 5.6.1- This ITAAC verifies that physical separation of redundant portions of the PS exists.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – Physical separation of redundant divisions prevents a single credible event from preventing protective action.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
3.1	Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.	GDC 1 – Quality standards and records.	GDC 1- This ITAAC verifies that components important to safety are tested to quality standards.
		GDC 2 – Design Bases for protection against natural phenomena.	GDC 2 – This ITAAC verifies that components important to safety are designed to withstand the effects of natural phenomena such as earthquakes.
		GDC 21 – Protection system reliability and testability.	GDC 21- This ITAAC demonstrates the PS is designed for high functional reliability.
		IEEE 603, Clause 5.4 – Equipment Qualification.	IEEE 603, Clause 5.4- This ITAAC verifies that safety system equipment is qualified through testing and analyses to be capable of meeting the seismic performance requirements.
		IEEE 603 , Clause 5.5- System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the PS equipment is capable of accomplishing its safety functions during a design basis earthquake.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.1	The PS generates automatic RT signals.	GDC 20 – Protection system functions.	GDC 20- This ITAAC verifies that the PS is designed to initiate automatically the operation of the reactivity control systems (control rods and boron injection) to ensure the fuel design limits are not exceeded.
		GDC 25 – Protection system requirements for reactivity control malfunctions.	GDC 25 - This ITAAC verifies that the PS provides function(s) that protects against an accidental withdrawal of controls rods. (From chapter 15 , Table 15.0-10, the following RTs protect against accidental rod withdrawal accidents: • Low DNBR • High Flux Rate • High Linear Power Density • High core power
		GDC 29 – Protection against anticipated operational occurrences.	GDC 29 - The PS automatic RT functions provide protection against the effects of anticipated operational occurrences (AOO). See Table 15.0-10— Plant Systems Used in the Accident.
		IEEE 603, Clause 6.1 – Automatic Control	IEEE 603, Clause 6.1 – This ITAAC verifies that means are provided to automatically initiate protective actions.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.2	The PS generates automatic ESF signals.	GDC 20 – Protection system functions.	GDC 20- This ITAAC verifies that the PS is designed to initiate automatically the operation of the engineered safety features (ESF) to protect against the effects of DBEs and AOOs.
		GDC 29 – Protection against anticipated operational occurrences.	GDC29 – The PS automatically actuates ESF functions provide protection against the effects of anticipated operational occurrences.
		IEEE 603, Clause 5.2 – Completion of Protective Action.	IEEE 603, Clause 5.2 - The ITAAC verifies that ESF signals remain until the signals that represent the completion of the safety function are present.
		IEEE 603, Clause 6.1 – Automatic Control	IEEE 603, Clause 6.1 – This ITAAC verifies that means are provided to automatically initiate protective actions
4.3	The permissives provide operating bypass capability for the corresponding PS functions.	IEEE 603, Clause 6.6 – Operating Bypasses	IEEE 603, Clause 6.6 - This ITAAC verifies the permissive conditions that provide an operating bypass of PS functions.
4.4	Communication independence is provided between the four PS divisions.	IEEE 603, Clause 5.6.1 – Independence Between Redundant Portions of a Safety System	IEEE 603, Clause 5.6- This ITAAC verifies communications independence exists between redundant portions of the PS.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
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.	GDC 21 – Protection system reliability and testability.	GDC 21- This ITAAC satisfies GDC 21 in that removal from service of any component or channel does not result in the loss of the required minimum redundancy.
		IEEE 603, Clause 5.7- Capability for Test and Calibration	IEEE 603, Clause 5.7 – This ITAAC verifies that a division of the PS can be placed in maintenance bypass to perform testing and calibration while retaining the capability of the PS to accomplish its safety functions
		IEEE 603, Clause 5.8 – Information Displays.	IEEE 603, Clause 5.8– The second part of this ITAAC verifies that an indication of bypass is provided in the MCR.
		IEEE 603, Clause 5.10- Repair	IEEE 603, Clause 5.10- This ITAAC verifies that the PS is designed to facilitate replacement, repair, and adjustment of malfunctioning PS equipment, by providing the capability of placing a PS division in maintenance bypass while maintaining the PS safety functions. This allows the repair of equipment in the bypassed division.
		IEEE 603, Clause 6.7 – Maintenance Bypass.	IEEE 603, Clause 6.7 – The first part of this ITAAC verifies that the PS can perform its safety function when a division is placed in maintenance bypass.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.6	Setpoints associated with the automatic RT signals and the automatic ESF signals 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.	IEEE 603, Clause 4.4- Variables and analytical limits.	IEEE 603, Clause 4.4- This ITAAC documents the analytical limits associated with each variable.
		IEEE 603, Clause 6.8 - Setpoints	IEEE 603, Clause 6.8- This ITAAC verifies that the PS setpoints are determined using a documented methodology that allows for uncertainties between the process analytical limits and the device setpoint.
4.7	Input variables provide the inputs for generating RT signals and ESF signals.	IEEE 603, Clause 4.4- Variables.	IEEE 603, Clause 4.4- This ITAAC verifies the correct input variables are used in the PS design.
		IEEE 603, Clause 6.4- Derivation of System Inputs.	IEEE 603, Clause 6.4 – This ITAAC verifies the sense and command feature inputs are derived from signals that are direct measures of the desired variable as specified in the design basis.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.8	Electrical isolation is provided on connections between PS equipment and non-Class 1E equipment.	GDC 24 – Separation of protection and control systems.	GDC 24- This ITAAC assures that an electrical surge originating from the non safety I&C system will not effect the PS, therefore providing a form a separation.
		IEEE 603, Clause 5.3- Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the PS (electrical isolation devices) are designed to a high degree of quality.
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4 – This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).
		IEEE 603, Clause 5.6.3 – Independence between safety systems and other systems.	IEEE 603, Clause 5.6.3 – This ITAAC provides verification that the safety systems are electrically isolated from the non-safety systems, thus providing a form of electrical independence.
		IEEE 603, Clause 5.12- Auxiliary Features	IEEE 603, Clause 5.12 – This ITAAC verifies that the auxiliary features of the PS such as the test equipment located at the service unit (SU) does not degrade the PS equipment through the use of electrical isolation devices.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – By providing electrical isolation between the PS and other non safety system, interactions between the PS and other non safety systems is minimized.
4.9	Deleted.	Deleted.	Deleted.
4.10	Class 1E PS equipment can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	GDC 1 – Quality standards and records	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 4 –Environmental and dynamic effects design bases	GDC 4- This ITAAC verifies the PS is designed to accommodate the effects of and to be compatible with the environmental conditions (EMI, RFI) associated with normal operation, maintenance, testing, and postulated accidents.
		GDC 21 – Protection System reliability and testability	GDC 21- This ITAAC demonstrates the PS is designed for high functional reliability.
		IEEE 603-, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the PS are designed to a high degree of quality (EMI, RFI, and ESD and power surge resistance).

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.5 - System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the PS equipment is capable of accomplishing its safety functions under the full range of applicable conditions (EMI, RFI, ESD and power surges).
4.11	Controls exist in the MCR that allow manual actuation at the system level.	GDC 13 – Instrumentation and Control IEEE 603, Clause 6.2 – Manual Control	GDC 13- This ITAAC demonstrates controls exist in the control room to assure adequate safety. IEEE 603, Clause 6.2 – This ITAAC verifies that manual controls exist for the actuation of protective functions.
4.12	Controls exist in the MCR and RSS to allow validation or inhibition of manual permissives.	GDC 13 – Instrumentation and Control IEEE 603, Clause 6.2 – Manual Control	GDC 13- This ITAAC demonstrates controls exist in the control room to assure adequate safety IEEE 603, Clause 6.2 – This ITAAC verifies means of manual control.
4.13	The PS interlocks exist as listed in Table 2.4.1-6.	IEEE 603, Clause 6.1 – Automatic Control	IEEE 603, Clause 6.1 -This ITAAC provides means for automatic initiation of protective actions.
4.14	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 following:	Branch Technical Position (BTP 7-14) – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.	BTP 7-14 – This ITAAC verifies that the hardware and application software development process (as described in the SPM) was followed and that the process produces acceptable design outputs as identified by V&V reports.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
	1) Basic design phase. 2) Detailed design phase. 3) Manufacturing phase. 4) Testing phase. 5) Installation and commissioning phase.	GDC 1 – Quality standards and records.	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 29 – Protection against anticipated operational occurrences.	GDC 29 – This ITAAC verifies the use of a high quality design process that assures an extremely high probability that the PS can accomplish its safety functions in the event of an AOO.
		IEEE 603, Clause 4.1- Applicable Design Basis Events	IEEE 603, Clause 4.1- This ITAAC will document the design basis for the PS through reports, including the design basis events that the PS software design will be based on.
		IEEE 603, Clause 4.4- Variables	IEEE 603, Clause 4.4- This ITAAC will document the variables that are to be monitored to manually or automatically or both control the protective actions.
		IEEE 603, Clause 4.6- Number and Location of Variable	IEEE 603, Clause 4.6 – This ITAAC will document the minimum number and locations of sensors for those variables in IEEE 603, Clause 4.4 that have a spatial dependence

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 4.7- Range of Conditions	IEEE 603, Clause 4.7 – This ITAAC will document the range of transient and steady state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the PS shall perform.
		IEEE 603, Clause 4.8- Conditions having the potential for functional degradation.	IEEE 603, Clause 4.8- This ITAAC will document the conditions having the potential for functional degradation for safety systems performance and for which provisions shall be incorporated to retain the capability for performing the safety functions.
		IEEE 603, Clause 4.9- Methods to be used to determine reliability	IEEE 603, Clause 4.9, This ITAAC will document the method to be used to determine that the reliability of the PS design is appropriate and any reliability goals that may be imposed on the PS design.
		IEEE 603, Clause 5.3- Quality	IEEE 603, Clause 5.3 – This ITAAC verifies that the application software is designed in accordance with a prescribed quality assurance program.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.15	Controls exist in the RSS that allow manual actuation of RT.	GDC 13- Instrumentation and Control.	GDC 13- This ITAAC demonstrates controls exist in the RSS to assure adequate safety.
		GDC 19- Control Room	GDC 19- The ITAAC verifies the RT feature in the RSS which allows the capability to shutdown the reactor using controls out side the control room.
		IEEE 603, Clause 6.2- Manual Control.	IEEE 603, Clause 6.2 – This ITAAC verifies means of manual actuation of RT.
4.16	Electrical isolation is provided on connections between the four PS divisions.	IEEE 603, Clause 5.6.3 – Independence between Safety Systems and Other Systems.	IEEE 603, Clause 5.6.3 – This ITAAC verifies communication independence with other non safety systems. Communication independence prevents a failure in the non safety systems from affecting the PS in performing its required safety functions.
		IEEE 603, Clause 5.12- Auxiliary Features	IEEE 603, Clause 5.12 – This ITAAC verifies that the auxiliary features of the PS such as the test equipment located at the service unit (SU) does not degrade the PS equipment by demonstrating communication independence between the PS class 1E equipment and the non class 1E SU equipment.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – By providing communication independence between the PS and other non safety system, interactions between the PS and other non safety systems is minimized.
4.17	Communications independence is provided between PS equipment and non-Class 1E equipment.	GDC 22 – Protection System Independence	GDC 22- This ITAAC assures that an electrical surge originating from one PS division will not effect the other redundant divisions, preventing the loss of protective functions.
		IEEE 603, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the PS (electrical isolation devices) are designed to a high degree of quality.
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4- This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).
		IEEE 603, Clause 5.6.1 – Independence between redundant portions of a safety system	IEEE 603, Clause 5.6.1- This ITAAC serves to verify that redundant portions of the PS are independent. The use of electrical isolation between redundant portions provides a sense of independence in that an electrical fault in one redundant portion does not affect another redundant portion.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.18	The PS is designed so that safety-related functions required for DBE are performed in the presence of the following:	GDC 23 – Protection System Failure Modes	GDC 23- This ITAAC verifies through a failure modes and effects analysis that the PS is designed to fail in to a safe state.
	• Single detectable failures within the PS concurrent with identifiable but non-detectable failures. • Failures caused by the single failure.	IEEE 603, Clause 5.1- Single Failure Criterion.	IEEE 603, Clause 5.1 – This ITAAC verifies through a failure mode and effects analysis that the PS can perform its safety functions in the presence of a single failure.
	• Failures and spurious system actions that cause or are caused by the DBE requiring the safety function.	IEEE 603, Clause 5.15- Reliability	IEEE 603, Clause 5.15 – This ITAAC confirms through analysis that the PS reliability goals have been achieved.
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.	IEEE 603, Clause 5.11- Identification of Equipment	IEEE 603, Clause 5.11 – This ITAAC verifies that the PS equipment is distinctly identified for each redundant portion of the PS.
4.20	Locking mechanisms are provided on the PS cabinet doors. Opened PS cabinet doors are indicated in the MCR.	IEEE 603, Clause 5.9 - Control of Access.	IEEE 603, Clause 5.9 – This ITAAC verifies that access to the PS equipment is controlled through the use of locking devices.
4.21	Key lock switches are provided at the PS cabinets to restrict modifications to the PS software.	IEEE 603, Clause 6.5 – Capability	IEEE 603, Clause 6.5 – This ITAAC verifies that the operational availability of PS inputs can be confirmed during reactor operation and post-accident periods by one of the approved methods.

Table 14.03.05-2—Requirements Justification for Protection System ITAAC (15 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.22	The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.	IEEE 603, Clause 6.5 – Capability for Testing and Calibration	IEEE 603, Clause 6.5 – This ITAAC verifies that the operational availability of PS inputs can be confirmed during reactor operation and post-accident periods by one of the approved methods.
5.1	Class1E PS components are powered from a Class 1E division in a normal or alternate feed condition.	IEEE 603, Clause 8.1- Electrical Power Sources	IEEE 603, Clause 8.1- This ITAAC verifies that the PS equipment is powered from a Class 1E source of power. ITAAC associated with the Class 1E power system is addressed in Tier 1, Section 2.5.1.

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
2.1	SICS equipment is located as listed in Table 2.4.2-1.	GDC 2 – Design Bases for protection against natural phenomena	GDC 2- The verification that the redundant portions of the system are located in separate safeguards buildings demonstrates protection against natural phenomena.
		GDC 4 – Environmental and dynamic effects design bases	GDC 4- The fact that the safeguards building structures are designed to provide protection from environmental and design bases effects, the location of the SAS equipment in these buildings demonstrates the equipment can withstand such effects.
		IEEE 603, Clause 5.6.2 – Independence between safety systems and effects of design bases event.	IEEE 603, Clause 5.6.2 – This ITAAC verifies that the SAS equipment resides in buildings that provide protection from the effects of a design basis event (DBE). The safeguards buildings are designed to protect the equipment from the effects of a DBE.
3.1	Equipment identified as Seismic Category I can withstand seismic design basis loads without loss of safety function.	GDC 1 – Quality standards and records.	GDC 1- This ITAAC verifies that components important to safety are tested to quality standards.
		GDC 2 – Design Bases for protection against natural phenomena.	GDC 2 – This ITAAC verifies that components important to safety are designed to withstand the effects of natural phenomena such as earthquakes.

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.4 – Equipment Qualification	IEEE 603, Clause 5.4- This ITAAC verifies that safety system equipment is qualified through testing and analyses to be capable of meeting the seismic performance requirements.
		IEEE 603 , Clause 5.5- System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the SAS equipment is capable of accomplishing its safety functions during a design basis earthquake.
4.1	The capability to transfer control of the SICS from the MCR to the RSS exists.	GDC 19 – Control Room	GDC 19 – This ITAAC verifies that the equipment and procedures are in place to allow control outside the control room.
4.3	Electrical isolation is provided on connections between the safety-related parts of the SICS and non-Class 1E equipment.	IEEE 603, Clause 5.3- Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the PS (electrical isolation devices) are designed to a high degree of quality.
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4 – This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).
		IEEE 603, Clause 5.6.3 – Independence between safety systems and other systems.	IEEE 603, Clause 5.6.3 – This ITAAC provides verification that the safety systems are electrically isolated from the non-safety systems, thus providing a form of electrical independence.

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.12-Auxiliary Features	IEEE 603, Clause 5.12 – This ITAAC verifies that the auxiliary features of the SICS such as the test equipment located at the service unit (SU) does not degrade the SICS equipment through the use of electrical isolation devices.
4.4	Class 1E SICS equipment can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	GDC 1 – Quality standards and records	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 4 –Environmental and dynamic effects design bases	GDC 4- This ITAAC verifies the SAS is designed to accommodate the effects of and to be compatible with the environmental conditions (EMI, RFI) associated with normal operation, maintenance, testing, and postulated accidents.
		IEEE 603-, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the SAS are designed to a high degree of quality (EMI, RFI, and ESD and power surge resistance).
		IEEE 603, Clause 5.5 - System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the SAS equipment is capable of accomplishing its safety functions under the full range of applicable conditions (EMI, RFI, ESD and power surges).

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.5	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: 1) Basic design phase. 2) Detailed design phase. 3) Manufacturing phase. 4) Testing phase. 5) Installation and commissioning phase.	Branch Technical Position (BTP 7-14) – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.	BTP 7-14 – This ITAAC verifies that the hardware and application software development process (as described in the SPM) was followed and that the process produces acceptable design outputs as identified by V&V reports.
		GDC 1 – Quality standards and records.	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 29 – Protection against anticipated operational occurrences.	GDC 29 – This ITAAC verifies the use of a high quality design process that assures an extremely high probability that the SICS can accomplish its safety functions in the event of an AOO.
		IEEE 603, Clause 4.1- Applicable Design Basis Events	IEEE 603, Clause 4.1- This ITAAC will document the design basis for the SICS through reports, including the design basis events that the SICS software design will be based on.
		IEEE 603, Clause 4.4- Variables	IEEE 603, Clause 4.4- This ITAAC will document the variables that are to be monitored to manually or automatically or both control the protective actions.
		IEEE 603, Clause 4.6- Number and Location of Variable	IEEE 603, Clause 4.6 – This ITAAC will document the minimum number and locations of sensors for those variables in IEEE 603, Clause 4.4 that have a spatial dependence

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 4.7- Range of Conditions	IEEE 603, Clause 4.7 – This ITAAC will document the range of transient and steady state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the SICS shall perform.
		IEEE 603, Clause 4.8- Conditions having the potential for functional degradation.	IEEE 603, Clause 4.8- This ITAAC will document the conditions having the potential for functional degradation for safety systems performance and for which provisions shall be incorporated to retain the capability for performing the safety functions.
		IEEE 603, Clause 4.9- Methods to be used to determine reliability	IEEE 603, Clause 4.9, This ITAAC will document the method to be used to determine that the reliability of the SICS design is appropriate and any reliability goals that may be imposed on the SICS design.
		IEEE 603, Clause 5.3- Quality	IEEE 603, Clause 5.3 – This ITAAC verifies that the application software is designed in accordance with a prescribed quality assurance program.
4.6	Electrical isolation is provided on connections between the RSS and the MCR for the SICS.	RG 1.189 – Fire Protection for Nuclear Power Plants	RG 1.189 - This ITAAC verifies electrical isolation between the MCR and the RSS to meet the guidance of RG 1.189

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.7	Electrical isolation is provided on connections between the four SICS divisions.	IEEE 603, Clause 5.6.3 – Independence between Safety Systems and Other Systems.	IEEE 603, Clause 5.6.3 – This ITAAC verifies communication independence with other non safety systems. Communication independence prevents a failure in the non safety systems from allowing the SICS to perform its required safety functions.
		IEEE 603, Clause 5.12-Auxiliary Features	IEEE 603, Clause 5.12 – This ITAAC verifies that the auxiliary features of the SICS such as the test equipment located at the service unit (SU) does not degrade the SICS equipment by demonstrating communication independence between the SICS class 1E equipment and the non class 1E SU equipment.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – By providing communication independence between the SICS and other non safety system, interactions between the SICS and other non safety systems is minimized.

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.8	Communications independence is provided between the four SICS divisions.	IEEE 603, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the SICS (electrical isolation devices) are designed to a high degree of quality.
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4- This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).
		IEEE 603, Clause 5.6.1 – Independence between redundant portions of a safety system	IEEE 603, Clause 5.6.1- This ITAAC serves to verify that redundant portions of the SICS are independent. The use of electrical isolation between redundant portions provides a sense of independence in that an electrical fault in one redundant portion does not affect another redundant portion.
4.9	Communications independence is provided between SICS equipment and non-Class 1E equipment.	IEEE 603, Clause 5.6.1 – Independence Between Redundant Portions of a Safety System	IEEE 603, Clause 5.6- This ITAAC verifies communications independence exists between redundant portions of the SICS.

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.10	The SICS is designed so that safety-related functions required for 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.	IEEE 603, Clause 5.1-Single Failure Criterion. IEEE 603, Clause 5.15-Reliability	IEEE 603, Clause 5.1 – This ITAAC verifies through a failure mode and effects analysis that the SICS can perform its safety functions in the presence of a single failure. IEEE 603, Clause 5.15 – This ITAAC confirms through analysis that the SICS reliability goals have been achieved.
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.	IEEE 603, Clause 5.11-Identification of Equipment	IEEE 603, Clause 5.11 – This ITAAC verifies that the SICS equipment is distinctly identified for each redundant portion of the SICS.
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.	IEEE 603, Clause 5.9 - Control of Access.	IEEE 603, Clause 5.9 – This ITAAC verifies that access to the SICS equipment is controlled through the use of locking devices
4.13	Key lock switches are present at the SICS cabinets located outside of the MCR to restrict modifications to the SICS software.	IEEE 603, Clause 5.9 - Control of Access.	IEEE 603, Clause 5.9 – This ITAAC verifies that access to the SICS software is restricted.

Table 14.03.05-3—Requirements Justification for Safety Information and Control System ITAAC (9 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
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.	IEEE 603, Clause 5.7-Capability for Test and Calibration	IEEE 603, Clause 5.7 – This ITAAC verifies that a division of the SICS can be placed out of service to perform testing and calibration while retaining the capability of the SICS to accomplish its safety functions
		IEEE 603, Clause 5.8 – Information Displays.	IEEE 603, Clause 5.8– The second part of this ITAAC verifies that an indication of a division out of service is provided in the MCR.
		IEEE 603, Clause 5.10-Repair	IEEE 603, Clause 5.10- This ITAAC verifies that the SICS is designed to facilitate replacement, repair, and adjustment of malfunctioning SICS equipment, by providing the capability of placing a SICS division out of service while maintaining the SICS safety functions. This allows the repair of equipment in the out of service division.
		IEEE 603, Clause 6.7 – Maintenance Bypass.	IEEE 603, Clause 6.7 – The first part of this ITAAC verifies that the SICS can perform its safety function when a division is placed out of service for maintenance, testing, or repair.
5.1	Class 1E SICS components are powered from a Class 1E division in a normal or alternate feed condition.	IEEE 603, Clause 8.1-Electrical Power Sources	IEEE 603, Clause 8.1- This ITAAC verifies that the SICS equipment is powered from a Class 1E source of power. ITAAC associated with the Class 1E power system is addressed in Tier 1, Section 2.5.1.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
2.1	SAS equipment is located as listed in Table 2.4.4-1.	GDC 2 – Design Bases for protection against natural phenomena	GDC 2- The verification that the redundant portions of the system are located in separate safeguards buildings demonstrates protection against natural phenomena.
		GDC 4 – Environmental and dynamic effects design bases	GDC 4- The fact that the safeguards building structures are designed to provide protection from environmental and design bases effects, the location of the SAS equipment in these buildings demonstrates the equipment can withstand such effects.
		IEEE 603, Clause 5.6.2 – Independence between safety systems and effects of design bases event.	IEEE 603, Clause 5.6.2 – This ITAAC verifies that the SAS equipment resides in buildings that provide protection from the effects of a design basis event (DBE). The safeguards buildings are designed to protect the equipment from the effects of a DBE.
2.2	Physical separation exists between the four divisions of the SAS.	IEEE 603, Clause 5.6.1 – Independence between redundant portions of a safety system	IEEE 603, Clause 5.6.1- This ITAAC verifies that physical separation of redundant portions of the SAS exists.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – Physical separation of redundant divisions prevents a single credible event from preventing a safety function.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
3.1	Equipment identified as Seismic Category I can withstand seismic design basis loads without loss of safety function.	GDC 1 – Quality standards and records.	GDC 1- This ITAAC verifies that components important to safety are tested to quality standards.
		GDC 2 – Design Bases for protection against natural phenomena	GDC 2 – This ITAAC verifies that components important to safety are designed to withstand the effects of natural phenomena such as earthquakes.
		IEEE 603, Clause 5.4 – Equipment Qualification	IEEE 603, Clause 5.4- This ITAAC verifies that safety system equipment is qualified through testing and analyses to be capable of meeting the seismic performance requirements.
		IEEE 603 , Clause 5.5- System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the SAS equipment is capable of accomplishing its safety functions during a design basis earthquake.
4.1	Class 1E SAS equipment can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	GDC 1 – Quality standards and records	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 4 –Environmental and dynamic effects design bases	GDC 4- This ITAAC verifies the SAS is designed to accommodate the effects of and to be compatible with the environmental conditions (EMI, RFI) associated with normal operation, maintenance, testing, and postulated accidents.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603-, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the SAS are designed to a high degree of quality (EMI, RFI, and ESD and power surge resistance).
		IEEE 603, Clause 5.5 - System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the SAS equipment is capable of accomplishing its safety functions under the full range of applicable conditions (EMI, RFI, ESD and power surges).
4.2	The SAS receives input signals from the sources listed in Table 2.4.4-2.	IEEE 603, Clause 4.4- Variables.	IEEE 603, Clause 4.4- This ITAAC verifies the correct input variables are used in the SAS design.
		IEEE 603, Clause 6.4- Derivation of System Inputs.	IEEE 603, Clause 6.4 – This ITAAC verifies the sense and command feature inputs are derived from signals that are direct measures of the desired variable as specified in the design basis.
4.3	The SAS provides the output signals listed in Table 2.4.4-3.	IEEE 603, Clause 6.1 – Automatic Control	IEEE 603, Clause 6.1 – This ITAAC verifies that means are provided to automatically initiate protective actions.
4.4	The SAS provides the interlocks listed in Table 2.4.4-4.	IEEE 603, Clause 6.1 – Automatic Control	IEEE 603, Clause 6.1 – This ITAAC verifies that means are provided to automatically initiate protective actions.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.5	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. 4) Testing phase. 5) Installation and commissioning phase.	Branch Technical Position (BTP 7-14) – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems.	BTP 7-14 – This ITAAC verifies that the hardware and application software development process (as described in the SPM) was followed and that the process produces acceptable design outputs as identified by V&V reports.
		GDC 1 – Quality standards and records.	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 29 – Protection against anticipated operational occurrences.	GDC 29 – This ITAAC verifies the use of a high quality design process that assures an extremely high probability that the SAS can accomplish its safety functions in the event of an AOO.
		IEEE 603, Clause 4.1- Applicable Design Basis Events	IEEE 603, Clause 4.1- This ITAAC will document the design basis for the SAS through reports, including the design basis events that the SAS software design will be based on.
		IEEE 603, Clause 4.4- Variables	IEEE 603, Clause 4.4- This ITAAC will document the variables that are to be monitored to manually or automatically or both control the protective actions.
		IEEE 603, Clause 4.6- Number and Location of Variable	IEEE 603, Clause 4.6 – This ITAAC will document the minimum number and locations of sensors for those variables in IEEE 603, Clause 4.4 that have a spatial dependence

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 4.7-Range of Conditions	IEEE 603, Clause 4.7 – This ITAAC will document the range of transient and steady state conditions of both motive and control power and the environment during normal, abnormal, and accident circumstances throughout which the SAS shall perform.
		IEEE 603, Clause 4.8-Conditions having the potential for functional degradation.	IEEE 603, Clause 4.8- This ITAAC will document the conditions having the potential for functional degradation for safety systems performance and for which provisions shall be incorporated to retain the capability for performing the safety functions.
		IEEE 603, Clause 4.9-Methods to be used to determine reliability	IEEE 603, Clause 4.9, This ITAAC will document the method to be used to determine that the reliability of the SAS design is appropriate and any reliability goals that may be imposed on the SAS design.
		IEEE 603, Clause 5.3-Quality	IEEE 603, Clause 5.3 – This ITAAC verifies that the application software is designed in accordance with a prescribed quality assurance program.
4.6	Electrical isolation is provided on connections between the four SAS divisions.	IEEE 603, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the SAS (electrical isolation devices) are designed to a high degree of quality.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4- This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).
		IEEE 603, Clause 5.6.1 – Independence between redundant portions of a safety system	IEEE 603, Clause 5.6.1- This ITAAC serves to verify that redundant portions of the SAS are independent. The use of electrical isolation between redundant portions provides a sense of independence in that an electrical fault in one redundant portion does not affect another redundant portion.
4.7	Electrical isolation is provided on connections between SAS equipment and non-Class 1E equipment.	IEEE 603, Clause 5.6.1 – Independence Between Redundant Portions of a Safety System	IEEE 603, Clause 5.6- This ITAAC verifies communications independence exists between redundant portions of the SAS.
4.8	Communications independence is provided between the four SAS divisions.	IEEE 603, Clause 5.3- Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the SAS (electrical isolation devices) are designed to a high degree of quality.
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4 – This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.6.3 – Independence between safety systems and other systems.	IEEE 603, Clause 5.6.3 – This ITAAC provides verification that the safety systems are electrically isolated from the non-safety systems, thus providing a form of electrical independence.
		IEEE 603, Clause 5.12-Auxiliary Features	IEEE 603, Clause 5.12 – This ITAAC verifies that the auxiliary features of the SAS such as the test equipment located at the service unit (SU) does not degrade the SAS equipment through the use of electrical isolation devices.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – By providing electrical isolation between the SAS and other non safety system, interactions between the SAS and other non safety systems is minimized.
4.9	Communications independence is provided between SAS equipment and non-Class 1E equipment.	IEEE 603, Clause 5.6.3 – Independence between Safety Systems and Other Systems.	IEEE 603, Clause 5.6.3 – This ITAAC verifies communication independence with other non safety systems. Communication independence prevents a failure in the non safety systems from allowing the SAS to perform its required safety functions.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.12-Auxiliary Features	IEEE 603, Clause 5.12 – This ITAAC verifies that the auxiliary features of the SAS such as the test equipment located at the service unit (SU) does not degrade the SAS equipment by demonstrating communication independence between the SAS class 1E equipment and the non class 1E SU equipment.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – By providing communication independence between the SAS and other non safety system, interactions between the SAS and other non safety systems is minimized.
4.10	The SAS is designed so that safety-related functions required for 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.	IEEE 603, Clause 5.1-Single Failure Criterion.	IEEE 603, Clause 5.1 – This ITAAC verifies through a failure mode and effects analysis that the SAS can perform its safety functions in the presence of a single failure.
		IEEE 603, Clause 5.15-Reliability	IEEE 603, Clause 5.15 – This ITAAC confirms through analysis that the SAS reliability goals have been achieved.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
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.	IEEE 603, Clause 5.11- Identification of Equipment	IEEE 603, Clause 5.11 – This ITAAC verifies that the SAS equipment is distinctly identified for each redundant portion of the SAS.
4.12	Locking mechanisms are provided on the SAS cabinet doors. Opened SAS cabinet doors are indicated in the MCR.	IEEE 603, Clause 5.9 - Control of Access.	IEEE 603, Clause 5.9 – This ITAAC verifies that access to the SAS equipment is controlled through the use of locking devices
4.13	Key lock switches are present at the SAS cabinets to restrict modifications to the SAS software.	IEEE 603, Clause 5.9 - Control of Access.	IEEE 603, Clause 5.9 – This ITAAC verifies that access to the SAS software is restricted.
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.	IEEE 603, Clause 5.7- Capability for Test and Calibration	IEEE 603, Clause 5.7 – This ITAAC verifies that a division of the SAS can be placed out of service to perform testing and calibration while retaining the capability of the SAS to accomplish its safety functions
		IEEE 603, Clause 5.8 – Information Displays.	IEEE 603, Clause 5.8– The second part of this ITAAC verifies that an indication of a division out of service is provided in the MCR.

Table 14.03.05-4—Requirements Justification for Safety Automation System ITAAC (10 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.10-Repair	IEEE 603, Clause 5.10- This ITAAC verifies that the SAS is designed to facilitate replacement, repair, and adjustment of malfunctioning SAS equipment, by providing the capability of placing a SAS division out of service while maintaining the SAS safety functions. This allows the repair of equipment in the out of service division.
		IEEE 603, Clause 6.7 – Maintenance Bypass.	IEEE 603, Clause 6.7 – The first part of this ITAAC verifies that the SAS can perform its safety function when a division is placed out of service for maintenance, testing, or repair.
4.15	The operational availability of each input variable can be confirmed during reactor operation including post-accident periods.	IEEE 603, Clause 6.5 – Capability	IEEE 603 Clause 6.5 – This ITAAC verifies that the operational availability of SAS inputs can be confirmed during reactor operation and post-accident periods by one of the approved methods.
5.1	Class 1E SAS components are powered from a Class 1E division in a normal or alternate feed condition.	IEEE 603, Clause 8.1-Electrical Power Sources	IEEE 603, Clause 8.1- This ITAAC verifies that the SAS equipment is powered from a Class 1E source of power. ITAAC associated with the Class 1E power system is addressed in Tier 1, Section 2.5.1.

Table 14.03.05-5—Requirements Justification for Priority and Actuator Control System ITAAC (5 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
2.1	PACS equipment is located as listed in Table 2.4.5-1.	GDC 2 – Design Bases for protection against natural phenomena	GDC 2- The verification that the redundant portions of the system are located in separate safeguards buildings demonstrates protection against natural phenomena.
		GDC 4 – Environmental and dynamic effects design bases	GDC 4- The fact that the safeguards building structures are designed to provide protection from environmental and design bases effects, the location of the PACS equipment in these buildings demonstrates the equipment can withstand such effects.
		IEEE 603, Clause 5.6.2 – Independence between safety systems and effects of design bases event.	IEEE 603, Clause 5.6.2 – This ITAAC verifies that the PACS equipment resides in buildings that provide protection from the effects of a design basis event (DBE). The safeguards buildings are designed to protect the equipment from the effects of a DBE.
2.2	Physical separation exists between the four divisions of the PACS.	IEEE 603, Clause 5.6.1 – Independence between redundant portions of a safety system.	IEEE 603, Clause 5.6.1- This ITAAC verifies that physical separation of redundant portions of the PACS exists.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – Physical separation of redundant divisions prevents a single credible event from preventing protective action.

Table 14.03.05-5—Requirements Justification for Priority and Actuator Control System ITAAC (5 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
3.1	Equipment identified as Seismic Category I can withstand seismic design basis loads without loss of safety function.	GDC 1 – Quality standards and records.	GDC 1- This ITAAC verifies that components important to safety are tested to quality standards.
		GDC 2 – Design Bases for protection against natural phenomena.	GDC 2 – This ITAAC verifies that components important to safety are designed to withstand the effects of natural phenomena such as earthquakes.
		IEEE 603, Clause 5.4 – Equipment Qualification	IEEE 603, Clause 5.4- This ITAAC verifies that safety system equipment is qualified through testing and analyses to be capable of meeting the seismic performance requirements.
		IEEE 603 , Clause 5.5- System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the PACS equipment is capable of accomplishing its safety functions during a design basis earthquake.
4.1	The order of priority of automatic functions performed by PACS is listed from highest to lowest: • Safety-related I&C functions. • Non-safety-related I&C functions.	IEEE 603, Clause 6.1- Automatic Control	IEEE 603, Clause 6.1- This ITAAC verifies means are provided to automatically initiate and control protective action.
4.2	Electrical isolation is provided on connections between PACS equipment and non-Class 1E equipment.	IEEE 603, Clause 5.3- Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the PACS (electrical isolation devices) are designed to a high degree of quality.

Table 14.03.05-5—Requirements Justification for Priority and Actuator Control System ITAAC (5 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603, Clause 5.4 – System Integrity	IEEE 603, Clause 5.4 – This ITAAC serves to verify that the electrical isolation devices are capable of meeting the performance requirements (maximum credible fault determined per analysis).
		IEEE 603, Clause 5.6.3 – Independence between safety systems and other systems.	IEEE 603, Clause 5.6.3 – This ITAAC provides verification that the safety systems are electrically isolated from the non-safety systems, thus providing a form of electrical independence.
		IEEE 603, Clause 6.3 – Interaction between the sense and command features and other systems	IEEE 603, Clause 6.3 – By providing electrical isolation between the PACS and other non safety system, interactions between the PACS and other non safety systems is minimized.
4.3	Class 1E PACS equipment can perform its safety function when subjected to EMI, RFI, ESD, and power surges.	GDC 1 – Quality standards and records	GDC 1- This ITAAC provides quality design records for components important to safety.
		GDC 4 –Environmental and dynamic effects design bases	GDC 4- This ITAAC verifies the PACS is designed to accommodate the effects of and to be compatible with the environmental conditions (EMI, RFI) associated with normal operation, maintenance, testing, and postulated accidents.

Table 14.03.05-5—Requirements Justification for Priority and Actuator Control System ITAAC (5 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
		IEEE 603-, Clause 5.3 – Quality	IEEE 603, Clause 5.3- This ITAAC serves to verify that components of the PACS are designed to a high degree of quality (EMI, RFI, and ESD and power surge resistance).
		IEEE 603, Clause 5.5 - System Integrity	IEEE 603, Clause 5.5 – This ITAAC serves to verify that the PACS equipment is capable of accomplishing its safety functions under the full range of applicable conditions (EMI, RFI, ESD and power surges).
4.4	The input wiring from other I&C systems to the PACS is properly connected.	IEEE 603, Clause 5.2 – Completion of Protective Action	IEEE 603, Clause 5.2 – ITAAC item 4.2 in section 2.4.1 verifies the feature of maintaining a PS engineered safety feature (ESF) signal until the protective action is complete. However, ITAAC item 4.2 in section 2.4.1 does not verify the continuity of the signal path from the PS to the PACS. This ITAAC verifies the continuity of the ESF signal from the PS to the PACS by verifying the input wiring to the PACS.
4.5	The capability for testing of the PACS is provided while retaining the capability of the PACS to accomplish its safety function. PACS divisions in test are indicated in the MCR.	IEEE 603, Clause 5.7 – Capability for Test and Calibration	IEEE 603, Clause 5.7 – This ITAAC verifies that the PACS have the capability for testing and calibration while retaining its capability to accomplish its safety function.
4.6	Locking mechanisms are provided on the PACS cabinet doors. Opened PACS cabinet doors are indicated in the MCR.	IEEE 603, Clause 5.9 - Control of Access.	IEEE 603, Clause 5.9 – This ITAAC verifies that access to the PACS equipment is controlled through the use of locking devices.

Table 14.03.05-5—Requirements Justification for Priority and Actuator Control System ITAAC (5 Sheets)

ITAAC No.	Commitment Wording	Requirements Addressed	Justification
4.7	The equipment for each PACS 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.	IEEE 603, Clause 5.11- Identification of Equipment	IEEE 603, Clause 5.11 – This ITAAC verifies that the PACS equipment is distinctly identified for each redundant portion of the PACS.
5.1	Class 1E PACS components are powered from a Class 1E division in a normal or alternate feed condition.	IEEE 603, Clause 8.1- Electrical Power Sources	IEEE 603, Clause 8.1- This ITAAC verifies that the PACS equipment is powered from a Class 1E source of power. ITAAC associated with the Class 1E power system is addressed in Tier 1, Section 2.5.1.

U.S. EPR Final Safety Analysis Report Markups

Table 1.3-1—Abbreviations and Acronyms List (6 Sheets)

Term	Definition
3/4_EPGB	Divisions 3 and 4 Emergency Power Generating Building
10CFR	Title 10, Code of Federal Regulations
12UPS	12-Hour Uninterruptible Power Supply System
AAC	Alternate AC Source
AC_or_ac	Alternating Current
ALU	Actuation Logic Unit
AMI	Accident Monitoring Instrumentation
AOO	Anticipated Operational Occurrence
ASME	American Society of Mechanical Engineers
ATWS	Anticipated Transient Without Scram
AVS	Annulus Ventilation System
AWG	American Wire Gauge
BCMS	Boron Concentration Measurement System
BDBE	Beyond Design Basis Event
BPV	Boiler and Pressure Vessel
BTU	British Thermal Unit
CAV	Cumulative Absolute Velocity
CBVS	Containment Building Ventilation System
CCWS	Component Cooling Water System
CGCS	Combustible Gas Control System
CIS	Containment Isolation Signal
CL	Cold Leg
CMSS	Core Melt Stabilization System
COL	Combined License
COMS	Communication System
CRACS	Control Room Air Conditioning System
CRDCS	Control Rod Drive Control System
CRDM	Control Rod Drive Mechanism
CRE	Control Room Envelope
CVCS	Chemical and Volume Control System
DAC	Design Acceptance Criteria
DAS	Diverse Actuation System
DBA	Design Basis Accident
DBE	Design Basis Event

14.03.05-4

14.03.05-4

Table 1.3-1—Abbreviations and Acronyms List (6 Sheets)

Term	Definition
MFW	Main Feedwater
MFWCKV	Main Feedwater Check Valves
MFWFLCV	Main Feedwater Full Load Control Valve
MFWFLIV	Main Feedwater Full Load Isolation Valve
MFWIV	Main Feedwater Isolation Valve
MFWLLCV	Main Feedwater Low Load Control Valve
MFWLLIV	Main Feedwater Low Load Isolation Valve
MFWVLLCV	Main Feedwater Very Low Load Control Valve
MFWS	Main Feedwater System
MFWSVS	Main Feedwater System Valve Station
MHSI	Medium Head Safety Injection
MS or MSS	Main Steam System
MSI	Monitoring and Service Interface
MSIV	Main Steam Isolation Valve
MSRT	Main Steam Relief Train
MSSV	Main Steam Safety Valve
MSV	Main Steam Valve
MSVS	Main Steam Valve Station
MSU	Main Setup Transformer
MW	Megawatt
MWt	Megawatts Thermal
N/A	Not Applicable
NAB	Nuclear Auxiliary Building
NABVS	Nuclear Auxiliary Building Ventilation System
NAT	Normal Auxiliary Transformer
NDE	Nondestructive Examination
NI	Nuclear Island
NPSH	Net Positive Suction Head
NPSHA	Net Positive Suction Head Available
NPSS	Normal Power Supply System
NR	Narrow Range
NSSS	Nuclear Steam Supply System
NUPS	Non-Class 1E Uninterruptible Power Supply System
OER	Operating Experience Review

14.03.05-4

14.03.05-4

Table 1.3-1—Abbreviations and Acronyms List (6 Sheets)

Term	Definition
PACS	Priority and Actuator Control System ← 14.03.05-4
PAM	Post-Accident Monitoring
PAR	Passive Autocatalytic Recombiner
PAS	Process Automation System
PDS	Primary Depressurization System
PFAS	Plant Fire Alarm System
PICS	Process Information and Control System
PPS	Preferred Power Supply
PRA	Probabilistic Risk Assessment
PRD	Power Range Detector
PRT	Pressurizer Relief Tank
PS	Protection System
psf	Pounds per Square Foot
psia	Pounds per Square Inch Absolute
psig	Pounds per Square Inch Gauge
PSRV	Pressurizer Safety Relief Valve
PSWS	Plant Service Water System
PWR	Pressurized Water Reactor
PZR	Pressurizer
QA	Quality Assurance
QDS	Qualified Display System
RAP	Reliability Assurance Program
RB	Reactor Building
RBA	Reactor Building Annulus
RCB	Reactor Containment Building
RCP	Reactor Coolant Pump
RCPB	Reactor Coolant Pressure Boundary
RCS	Reactor Coolant System
RCSL	Reactor Control Surveillance and Limitation
RFI	Radio Frequency Interference
RG	Regulatory Guide
RHRS	Residual Heat Removal System
RPV	Reactor Pressure Vessel
RPVL	Reactor Pressure Vessel Level

Table 1.3-1—Abbreviations and Acronyms List (6 Sheets)

Term	Definition
RSB	Reactor Shield Building
RSS	Remote Shutdown Station
RT	Reactor Trip
RV	Reactor Vessel
RWB	Radioactive Waste Building
RWSS	Raw Water Supply System
SAHRS	Severe Accident Heat Removal System
SAS	Safety Automation System
SB	Safeguard Building
SBO	Station Blackout
SBODG	Station Blackout Diesel Generator
SBVS	Safeguard Building Controlled-Area Ventilation System
SBVSE	Electrical Division of Safeguard Building Ventilation System
SCWS	Safety Chilled Water System
SFP	Spent Fuel Pool
SFSP	Spent Fuel Storage Pool
SG	Steam Generator
SGI	Safeguards Information
SGBS	Steam Generator Blowdown System
SICS	Safety Information and Control System
SIS	Safety Injection System
SMS	Seismic Monitoring System
SOV	Solenoid Operated Valve
SPND	Self Powered Neutron Detector
SRP	Standard Review Plan
SSC	Structures, Systems, and Components
SSE	Safe Shutdown Earthquake
SSS	Startup and Shutdown System
SSSS	Standstill Seal System
TA	Task Analysis
TSC	Technical Support Center
TSP	Trisodium Phosphate
UHS	Ultimate Heat Sink
UL	Underwriter's Laboratories Inc

14.03.05-4

Table 1.3-1—Abbreviations and Acronyms List (6 Sheets)

Term	Definition
UPS	Uninterruptible Power Supply
U.S. EPR	United States Evolutionary Power Reactor
V	Volt
V&V	Verification and Validation 14.03.05-4
Vac	Volts Alternating Current
Vdc	Volts Direct Current
WR	Wide Range

Next File

2.4 Instrumentation and Control Systems

2.4.1 Protection System

1.0 Description

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

The PS provides the following safety related functions:

- Performs automatic initiation of reactor trip (RT) functions.
- Performs automatic initiation of engineered safety feature (ESF) functions.
- Provides for manual initiation of RT functions. ← 14.03.05-4
- Provides for manual actuation of ESF functions.
- Generates permissive signals that authorize the activation or deactivation of certain protective actions according to current plant conditions.
- Generates permissive signals that maintain safety related interlocks.

2.0 Arrangement

14.03.05-4 ↓

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

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

3.0 Mechanical Design Features

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

4.0 I&C Design Features, Displays and Controls

14.03.05-4 ↓

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

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

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

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

14.03.05-4

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 interlocks exist as ~~provided~~ listed in Table 2.4.1-6~~8~~—Protection System Interlocks.

4.14 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 following:

1. Basic design phase.
2. Detailed design phase.
3. Manufacturing phase.
4. Testing phase.
5. Installation and commissioning phase.

14.03.05-4

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.

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

14.03.05-4

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

Table 2.4.1-1—Protection System Equipment

14.03.05-4

Equipment Description	Equipment Tag Number (1)	Equipment Location	Seismic Category I	IEEE Class 1E(2)
PS Cabinets, Division 1	30CLE	Safeguard Building 1	I~~Yes~~	1^N 2^A
PS Cabinets, Division 2	30CLF	Safeguard Building 2	I~~Yes~~	2^N 1^A
PS Cabinets, Division 3	30CLG	Safeguard Building 3	I~~Yes~~	3^N 4^A
PS Cabinets, Division 4	30CLH	Safeguard Building 4	I~~Yes~~	4^N 3^A

1) Equipment Tag numbers are provided for information and are not part of the design certification.

2) ^{N} denotes the division the component is normally powered from. ^{A} denotes the division the component is powered from when alternate feed is implemented.

14.03.05-4

Table 2.4.1-2—Protection System Automatic Reactor Trip Signals and Input Variables

Reactor Trip Signal	Input Variable
High Linear Power Density (HLPD)	Neutron Flux - Self Powered Neutron Detectors
Low Departure from Nucleate Boiling Ratio (DNBR)	Neutron Flux - Self Powered Neutron Detectors
	Cold Leg Temperature (NR)
	Reactor Coolant Pump (RCP) Speed
	Rod Control Cluster Assembly Position
	Pressurizer Pressure
High Neutron Flux Rate of Change	Neutron Flux - Power Range Detectors
High Core Power Level	Cold Leg Temperature (WR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (NR)
Low RCP Speed	RCP Speed
Low Loop Flow Rate (two loops)	RCS Loop Flow
Low–Low Loop Flow Rate (one loop)	RCS Loop Flow
Low Doubling Time	Neutron Flux - Intermediate Range Detectors
High Neutron Flux	Neutron Flux - Intermediate Range Detectors
Low Pressurizer Pressure	Pressurizer Pressure (NR)
High Pressurizer Pressure	Pressurizer Pressure (NR)
High Pressurizer Level	Pressurizer Level (NR)
Low Hot Leg Pressure	Hot Leg Pressure (WR)
Steam Generator (SG) Pressure Drop	SG Pressure
Low Steam Generator Pressure	SG Pressure
High Steam Generator Pressure	SG Pressure
Low Steam Generator Level	SG Level (NR)
High Steam Generator Level	SG Level (NR)
High Containment Pressure	Containment Service Compartment Pressure (NR)
	Containment Equipment Compartment Pressure
Low Saturation Margin	Cold Leg Temperature (WR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (NR)
On Safety Injection System (SIS) Actuation	SIS Actuation Signal
On Emergency Feedwater System (EFWS) Actuation	EFWS Actuation Signal

14.03.05-4

Table 2.4.1-2—Protection System Input Signals (2 Sheets)

Item #	Signal	Source	# Divisions	IEEE Class 1E
1	Neutron Flux from Self Powered Neutron Detectors (SPND)	JKS	4	Yes
2	Neutron Flux from Power Range Detector (PRD)	JKT	4	Yes
3	Neutron Flux from Intermediate Range Detector (IRD)	JKT	4	Yes
4	Rod Control Cluster Assembly (RCCA) positions	JDA	4	Yes
5	Pressurizer (PZR) Pressure-Narrow Range (NR)	JEF	4	Yes
6	PZR Level	JEF	4	Yes
7	Cold Leg Temperature (NR)	JEC	4	Yes
8	Cold Leg Temperature Wide Range (WR)	JEC	4	Yes
9	Hot Leg (HL) Temperature (NR)	JEC	4	Yes
10	Hot Leg Temperature (WR)	JEC	4	Yes
11	Hot Leg Pressure (WR)	JNA	4	Yes
12	Reactor Coolant Pump (RCP) Speed Sensor	JEB	4	Yes
13	RCP power supply current	JEB	4	Yes
14	RCS (Reactor Coolant System) Loop Flow Rate	JEC	4	Yes
15	RCS Loop Level	JEC	4	Yes
16	Chemical and Volume Control System (CVCS) Boron Concentration Measurement	KBA	4	Yes
17	CVCS Charging Flow	KBD	4	Yes
18	Steam Generator (SG) Pressure	LBA	4	Yes
19	SG Level (NR)	JEA	4	Yes
20	SG Level (WR)	JEA	4	Yes
21	Containment Equipment Compartments Pressure	KLA	4	Yes
22	Containment Service Compartments Pressure (NR)	KLA	4	Yes

14.03.05-4

Table 2.4.1-2—Protection System Input Signals (2 Sheets)

Item #	Signal	Source	# Divisions	IEEE Class 1E
23	Containment Service Compartments Pressure (WR)	KLA	4	Yes
24	Differential Pressure Across RCP	JEC	4	Yes
25	6.9 kV Bus Voltage	BD	4	Yes
26	Reactor Trip Breaker Position	BU	4	Yes
27	Main Steam Line Activity	LBA	4	Yes
28	Main Control Room (MCR) Air Intake Activity	KLK	4	Yes
29	Containment High Range Activity	JYK	4	Yes
30	Manual Reactor Trip	CWY	4	Yes
31	Manual Partial Cooldown Actuation	CWY	4	Yes
32	Manual Main Steam Relief Train (MSRT) Actuation	CWY	4	Yes
33	Manual MSRT Isolation	CWY	4	Yes
34	Manual MSIV Isolation	CWY	4	Yes
35	Manual MFW Isolation	CWY	4	Yes
36	Manual Containment Isolation	CWY	4	Yes
37	Manual SG Isolation	CWY	4	Yes
38	Manual MCR Air Intake Isolation and Filtering	CWY	4	Yes
39	Manual EDG Actuation	CWY	4	Yes
40	Manual Safety Injection System (SIS) Actuation	CWY	4	Yes
41	Manual EFWS Isolation	CWY	4	Yes
42	Manual EFWS System Actuation	CWY	4	Yes

14.03.05-4

Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Signals and Input Variables (2 Sheets)

Engineered Safety Feature Signal	Input Variable
Safety Injection System Actuation	Pressurizer Pressure (NR)
	Hot Leg Pressure (WR)
	Hot Leg Temperature (WR)
	RCS Loop Level
Emergency Feedwater System Actuation	SG Level (WR)
	LOOP Signal
	SIS Actuation signal
Emergency Feedwater System Isolation	SG Level (WR)
	SG Isolation Signal
Partial Cooldown Actuation	SIS Actuation signal
Main Steam Relief Train (MSRT) Opening	SG Pressure
MSRT Isolation	SG Pressure
Main Steam Isolation	SG Pressure
	SG Isolation Signal
Main Feedwater Isolation	SG Level (NR)
	SG Pressure
	RT Breaker Position
	SG Isolation Signal
Containment Isolation Stage 1	Containment Service Compartment Pressure (NR)
	Containment Service Compartment Pressure (WR)
	Containment Equipment Compartment Pressure
	Containment High Range Activity
	SIS Actuation Signal
Containment Isolation Stage 2	Containment Service Compartment Pressure (WR)
CVCS Charging Isolation	Pressurizer Level (NR)
CVCS Isolation for Anti-Dilution	Boron Concentration
	CVCS Charging Flow
	Cold Leg Temperature (WR)
Emergency Diesel Generator Actuation	LOOP Signal
	SIS Actuation Signal

14.03.05-4

Table 2.4.1-3—Protection System Automatic Engineered Safety Feature Signals and Input Variables (2 Sheets)

Engineered Safety Feature Signal	Input Variable
PSRV Opening	Hot Leg Pressure (NR)
SG Isolation	Main Steam Line Activity
	SG Level (NR)
	Partial cooldown actuated signal
Reactor Coolant Pump Trip	RCP Differential Pressure
	RCP current measurement
	Containment Isolation Stage 2 Signal
Main Control Room Air Conditioning System (CRACS) Isolation and Filtering	MCR Air Intake Duct Activity
Turbine Trip	RT Breaker Position
Loss of Offsite Power (LOOP)	Bus loss of voltage
	Bus degraded voltage

14.03.05-4

~~Table 2.4.1-3—Protection System Automatic Reactor Trips~~

~~RT on Low PZR Pressure~~
~~RT on High PZR Pressure~~
~~RT on High PZR Level~~
~~RT on Low Hot Leg Pressure~~
~~RT on Low SG Pressure~~
~~RT on High SG Pressure~~
~~RT on High SG Pressure Drop~~
~~RT on Low SG Level~~
~~RT on High SG Level~~
~~RT on High Containment Pressure~~
~~RT on High Linear Power Density (HLPD)~~
~~RT on Low Departure from Nucleate Boiling Ratio (DNBR)~~
~~RT on Low DNBR and (Imbalance or Rod Drop)~~
~~RT on Low DNBR and Rod Drop~~
~~RT on Low DNBR- High Quality~~
~~RT on Low DNBR-High Quality and (Imbalance or Rod Drop)~~
~~RT on High Neutron Flux Rate of Change~~
~~RT on High Core Power Level (HCPL)~~
~~RT on Low Reactor Coolant System (RCS) Loop Flow Rate (Two Loops)~~
~~RT on Low-Low RCS Loop Flow Rate (One Loop)~~
~~RT on Low RCP Speed in Two Loops~~
~~RT on High Neutron Flux- Intermediate Range (IR)~~
~~RT on Low Doubling Time Intermediate Range(IR)~~
~~RT on Low Saturation Margin~~
~~RT on SIS Actuation~~
~~RT on Emergency Feedwater System (EFWS) Actuation~~

14.03.05-4

Table 2.4.1-4—Protection System Automatically Actuated Engineered Safety Features (2 Sheets)

SIS Actuation on Low PZR Pressure
SIS Actuation on Low ΔPSat
SIS Actuation on Low RCS Loop Level
RCP Trip on Low ΔP Over RCP and SIS Signal
RCP Trip on Containment Isolation Stage 2 Signal
Partial Cooldown Actuation on SIS Signal
LOOP Signal on a Bus Loss of Voltage
LOOP Signal on a Bus Degraded Voltage
EFWS Actuation on Low SG Level
EFWS Actuation on LOOP and SIS Actuation
EFWS Isolation on High SG Level
EFWS Isolation on SG Isolation Signal
Main Steam Relief Train (MSRT) Opening on High SG Pressure
MSRT Isolation (MSRIV, MSRCV) on Low SG Pressure
MSRT Setpoint Increase on SG Isolation Signal
Main Steam Isolation Valve (MSIV) Closure on High SG Pressure Drop
MSIV Closure on Low SG Pressure
MSIV Closure on SG Isolation Signal
Main Feedwater (MFW) Full Load Closure on High SG Level
MFW Full Load Closure on RT Confirmation
MFW Full Load and Startup Shutdown Isolation on SG Isolation Signal
MFW Startup and Shutdown Isolation on High SG Pressure Drop
MFW Startup and Shutdown Isolation on Low SG Pressure
MFW Startup and Shutdown Isolation on High SG Level for period of time following RT
Containment Isolation Stage 1 on High Containment Pressure
Containment Isolation Stage 1 on SIS Actuation
Containment Isolation Stage 2 on High Containment Pressure
Containment Isolation on High Containment Activity
EDG Actuation on LOOP Signal
EDG Actuation on SIS Actuation
First PSV Opening on High HL Pressure
Second PSV Opening on High HL Pressure
CVCS Charging Line Shutdown on High PZR Level (two stages)
CVCS Isolation on Anti-Dilution (Shutdown state with no RCP running)

14.03.05-4

~~Table 2.4.1-4—Protection System Automatically Actuated Engineered Safety Features (2 Sheets)~~

~~CVCS Isolation on Anti-Dilution (Standard shutdown state)~~
~~CVCS Isolation on Anti-Dilution (at power)~~
~~SG Isolation on Partial Cooldown signal and High SG Level~~
~~SG Isolation on Partial Cooldown signal and High Main Steam Activity~~
~~Control Room Heating Ventilation Air Conditioning (HVAC) Isolation and Filtering on High Intake Activity~~
~~Turbine Trip on RT Confirmation~~

14.03.05-4

Table 2.4.1-45 Protection System Manually Actuated Functions

Reactor Trip
SIS Actuation
Partial Cooldown Actuation
MSRT Actuation
MSRT Isolation
Main Steam ~~MSIV~~ Isolation
Main Feedwater (MFW) Isolation
Containment Isolation
SG Isolation
CRACS~~Control Room HVAC~~ Isolation and Filtering
EDG Actuation
EFWS Isolation
EFWS Actuation

14.03.05-4

14.03.05-4

Table 2.4.1-5—Protection System Permissives and Operating Bypasses (2 Sheets)

Permissive	Inhibit	Validate	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P2	Automatic	Automatic	Low DNBR RT	
			HLPD RT	
			Low RCS Loop Flow RT	
			Low RCP Speed RT	
			Low Pressurizer Pressure RT	
P3	Automatic	Automatic	Low-Low RCS Loop RT	
P5	Automatic	Automatic	High Core Power Level RT	
			Low Saturation Margin RT	
P6	Automatic	Manual		High Neutron Flux RT
				Low Doubling Time RT
P12	Automatic	Manual		High Pressurizer Level RT
				Low Hot Leg Pressure RT
				Low SG Pressure RT
				MSRT Isolation (manual)
				MSRT Isolation (low SG pressure)
				Main Steam Isolation (low SG pressure)
				MFW Startup and Shutdown System (SSS) Isolation (low SG pressure)
P13	Automatic	Manual		Low SG Level RT
				High SG Level RT
				EFWS Actuation (low SG level)
				EFWS Actuation (SIS + LOOP)
				EFWS Actuation (manual)
				EFWS Isolation (high SG level)

14.03.05-4

Table 2.4.1-5—Protection System Permissives and Operating Bypasses (2 Sheets)

Permissive	Inhibit	Validate	Function Bypassed by Inhibited Permissive	Function Bypassed by Validated Permissive
P13	Automatic	Manual		EFWS Isolation (manual)
				MFW Full Load Isolation (high SG level)
				MFW SSS Isolation (high SG level for period of time + RT)
				SG Isolation
P14	Manual	Manual		Partial Cooldown Actuation
P17	Automatic	Manual	PSRV Opening	CVCS Charging Isolation (high Pressurizer level)

14.03.05-4

Table 2.4.1-6—Protection System Operating Bypasses
(2 Sheets)

RT Functions:
RT on High Linear Power Density (HLPD)
RT on Low DNBR
RT on Low DNBR and Imbalance or Rod Drop
RT on Low DNBR and Rod Drop
RT on Variable Low DNBR and Insertion Signal
RT on Low DNBR- High Quality
RT on Low DNBR-High Quality and (Imbalance or Rod Drop)
RT on Low Loop Flow Rate (Two Loops)
RT on Low-Low Loop Flow Rate (One Loop)
RT on Low RCP Speed in Two Loops
RT on Low PZR Pressure
RT on HCPL
RT on Low Saturation Margin
RT on High Neutron Flux- Intermediate Range
RT on Low Doubling Time Intermediate Range
RT on Low HL Pressure
RT on Low SG Pressure
RT on Low SG Level
RT on High SG Level
RT on EFWS Actuation
RT on High PZR Level
Engineered Safeguard Functions:
SIS Actuation on Low PZR Pressure
SIS Actuation on Low ΔPSat
SIS Actuation on Low RCS Loop Level
CVCS Charging Isolation on High PZR Level
CVCS Isolation on Anti-Dilution (Shutdown state with no RCP running)
CVCS Isolation on Anti-Dilution (Standard shutdown state)
CVCS Isolation on Anti-Dilution (at power)
Partial Cooldown Actuation on SIS Signal
EFWS Actuation on Low SG Level
EFWS Actuation on LOOP and SIS Signals
EFWS Isolation on High SG Level

14.03.05-4

~~**Table 2.4.1-6—Protection System Operating Bypasses**~~
~~**(2 Sheets)**~~

~~MSRT Isolation on Low SG Pressure~~
~~Main Feedwater (MFW) Full Load Closure on High SG Level~~
~~MFW Startup and Shutdown Isolation on High SG Level for period of time following RT~~
~~MFW Startup and Shutdown Isolation on Low SG Pressure~~
~~MSIV Closure on Low SG Pressure~~
~~First PSV Opening on High HL Pressure~~
~~Second PSV Opening on High HL Pressure~~
~~SG Isolation~~

14.03.05-4

Table 2.4.1-7—Protection System Permissives

Permissive	Validation (Manual / Automatic)	Inhibition (Manual / Automatic)
P2	Automatic	Automatic
P3	Automatic	Automatic
P5	Automatic	Automatic
P6	Manual	Automatic
P7	Automatic	Automatic
P8	Automatic	Automatic
P12	Manual	Automatic
P13	Manual	Automatic
P14	Manual	Manual
P15	Manual	Automatic
P16	Manual	Automatic
P17	Manual	Automatic

14.03.05-4

Table 2.4.1-6~~8~~—Protection System Interlocks

RHR Suction Valves
MHSI Large Miniflow Line Valves
Safety Injection Accumulator Valves

14.03.05-4

Table 2.4.1-~~7~~9—Protection System ITAAC (~~5~~ 12 Sheets)

Commitment Wording		Inspections, Tests, Analyses 14.03.05-4	Acceptance Criteria
2.1	PS equipment is located as listed in Table 2.4.1-1.	Inspections will be performed of the location of the PS equipment.	The PS equipment listed in Table 2.4.1-1 is located as listed in Table 2.4.1-1.
2.2	Physical separation exists between the four divisions of the PS.	Inspections will be performed to verify that the divisions of the PS are located in separate safeguard buildings	The four divisions of the PS are located in separate safeguard buildings.
3.1	Equipment identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment listed as Seismic Category I in Table 2.4.1-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements.	a. Tests/analysis reports exist and conclude that the equipment listed as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.
		b. Inspections will be performed of the as-installed Seismic Category I equipment listed in Table 2.4.1-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	b. Inspection reports exist and conclude that the as-installed Seismic Category I equipment listed in Table 2.4.1-1 including anchorage is installed as specified on the construction drawings.
4.1	The PS generates ~~an~~ automatic RT signals. ~~for each of the parameters identified in Table 2.4.1-3.~~	a. Tests will be performed on the as-installed PS using test signals to verify that the RT breakers open when a trip limit in the PS is reached	a. The RT breakers open after a test signal reaches the trip limit in the PS for one RT function.
		b. Tests will be performed on the as-installed PS using test signals to verify that a RT signal is generated for the input variables listed in Table 2.4.1-2 when a test signal reaches the trip limit.~~Tests will be performed on the as- built PS using test signals to simulate the RT functions listed in Table 2.4.1-3~~.	b. The PS generates a RT signal after the test signal reaches the trip limit for the input variables listed in Table 2.4.1-2.~~The PS generates an automatic RT signal for each of the parameters identified in Table 2.4.1-3.~~

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.2	The PS generates automatically actuated engineered safety featureESF signals., as identified in Table 2.4.1-4.	Tests will be performed on the as-installed PS using test signals to verify that a ESF signal is generated for the input variables listed in Table 2.4.1-3 when a test signal reaches the trip limit.Tests will be performed on the as- built PS using test signals to simulate the engineered safety feature functions listed in Table 2.4.1-4.	The PS generates a ESF signal after the test signal reaches the trip limit for the input variables listed in Table 2.4.1-3. The ESF signals remain following removal of the test signal. The ESF signals are removed when test signals that represent the completion of the ESF function are present. Deliberate operator action is required to return the PS to normal.The PS generates automatic actuation of engineered safety feature signals, as identified in Table 2.4.1-4.
4.3	The permissives provide operating bypass capability for the corresponding PS functions.The PS provides operating bypasses for the functions identified in Table 2.4.1-6.	a. For each function listed as being bypassed by an inhibited permissive in Table 2.4.1-5, tests will be performed to verify that each function is bypassed when test signals representing the corresponding inhibited permissive signal are present. For each function listed as being bypassed by an inhibited permissive in Table 2.4.1-5, tests will be performed to verify the automatic removal of the bypass when test signals representing the corresponding inhibited permissive are removed.	a. The functions listed as being bypassed by inhibited permissives in Table 2.4.1-5 are bypassed when test signals representing the corresponding inhibited permissive are present and the bypasses are automatically removed when test signals representing the corresponding inhibited permissive are removed.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		b. For each function listed as being bypassed by a validated permissive in Table 2.4.1-5, tests will be performed to verify that each function is bypassed when test signals representing the corresponding validated permissive signal are present. For each function listed as being bypassed by a validated permissive in Table 2.4.1-5, tests will be performed to verify the automatic removal of the bypass when test signals representing the corresponding validated permissive are removed. ~~Tests will be performed on the as- built PS using test signals.~~	b. The functions listed as being bypassed by validated permissives in Table 2.4.1-5 are bypassed when test signals representing the corresponding validated permissive are present and the bypasses are automatically removed when test signals representing the corresponding validated permissive are removed. ~~The PS provides operating bypasses for the functions identified in Table 2.4.1-6.~~

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.4	Communication independence is provided in between the inter- four PS divisions. communication paths within the PS.	Tests, analyses, or a combination of tests and analyses will be performed on the as-installed PS equipment. Type tests, tests ,analyses or a combination of tests and analyses will be performed on components that establish communication independence in the inter-division communication paths within the PS	A report exists and concludes that: • The PS function processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor and the PS function processor. • The PS function processors operate in a strictly cyclic manner. • The PS function processors operate asynchronously from the PS communications processors.A verification and validation (V&V) report exists and concludes that communication independence exists in the inter-division communications 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.	a. A test of the as-installed PS will be performed to verify the maintenance bypass functionality. b. Tests will be performed to verify the existence of indications in the MCR when PS equipment is in maintenance bypass (inoperable).A test of the as built PS will be performed.	a. The PS can perform its safety functions when PS equipment is in maintenance bypass (inoperable). b. Bypassed PS equipment is indicated in the MCR.Bypassed or inoperable PS channels status information is retrievable in the MCR.

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.6	Setpoints associated with the automatic RT signals ~~reactor trips listed in Table 2.4.1-3~~ and the automatic ESF signals ~~ally actuated engineered safety features 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.	a. An inspection will be performed to verify the existence of an established methodology for determining the PS setpoints. b. An analysis will be performed to verify that the PS setpoints for the functions listed in Table 2.4.1-2 and Table 2.4.1-3 are determined using the documented methodology.	a. An established methodology for determining PS setpoints exists. b. A report exists and concludes that the PS setpoints associated with the automatic ~~reactor trips~~RT signals listed in Table 2.4.1-~~3~~ 2 and the automatic ESF signals ~~ally actuated engineered safety features~~ listed in Table 2.4.1-~~3~~4 are determined using a documented methodology: (1) For the determination of applicable contributors to instrument loop error. (2) For combining instrument loop errors. (3) For 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.~~	a. An analysis will be performed on the PS software design to verify that the input variables listed in Table 2.4.1-2 and Table 2.4.1-3 provide the inputs for generating the RT signals in Table 2.4.1-2 and the ESF signals in Table 2.4.1-3.	a. A report exists and concludes that each RT signal listed in Table 2.4.1-2 and each ESF signal listed in Table 2.4.1-3, the input variables associated with the signals are used in the PS software design for generating each signal

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
		b. Inspections, tests, or combinations of inspections and tests will be performed on the as-installed PS equipment to verify that the sensors that provide the input variables listed in Table 2.4.1-2 and Table 2.4.1-3 are connected to the correct input terminals of the PS as specified in the construction drawings. ~~Tests will be performed using simulated signals.~~	b. The sensors that provide the input variables listed in Table 2.4.1-2 and Table 2.4.1-3 are connected to the correct input terminals of the PS as specified in the construction drawings. ~~The PS receives the input signals listed in Table 2.4.1-2.~~
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.~~	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between PS equipment and non-Class 1E equipment.	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 PS equipment and non-Class 1E equipment.
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between PS equipment and non-Class 1E equipment.	b. A report exists and concludes that the Class 1E isolation devices used between PS equipment and non-Class 1E equipment prevent the propagation of credible electrical faults.
		c. Inspections will be performed on connections between PS equipment and non-Class 1E equipment. ~~Inspections will be performed on the existence of the electrical isolation devices.~~	c. Class 1E electrical isolation devices exist on connections between PS equipment and non-Class 1E equipment.~~Electrical isolation devices exist in the signal path from the PS to the non safety related control systems.~~

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.9	Deleted. Electrical isolation devices exist in the data communication paths between the PS and the non safety related displays and controls.	Deleted. Inspections will be performed on the existence of the electrical isolation devices.	Deleted. Electrical isolations 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 EMI, RFI, ESD, and power surges.	Type tests, tests, analyses or a combination of these will be performed on 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 2.4.1-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.
4.11	Controls exist in the MCR that allow manual actuation, at the system level., of the functions identified in Table 2.4.1-5.	a. Inspections will be performed to verify the existence of controls in the MCR . b. Tests will be performed to verify the correct functionality of the controls in the MCR.	a. Controls exist in the MCR that allow manual actuation at the system level of the functions listed in Table 2.4.1-5. b. For each function in Table 2.4.1-54, the correct actuation signals are present at the output of the PS actuation logic units (ALU) after the corresponding controls in the MCR are manually activated.
4.12	Controls exist in the MCR and RSS to allow validation or inhibition of manual permissives listed in Table 2.4.1-7.	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 MCR and RSS.	a. Controls exist in the MCR and RSS to allow validation or inhibition of manual permissives listed in Table 2.4.1-7. b. For each of the manual permissives in Table 2.4.1-57, the correct permissive status is present in the PS actuation logic units (ALU) after the corresponding controls in the MCR and RSS are manually activated.
4.13	The PS interlocks exist as provided listed in Table 2.4.1-68.	Tests will be performed on the operation of the interlocks listed in Table 2.4.1-86.	The PS interlocks exist as provided listed in Table 2.4.1-86.

14.03.05-4

Table 2.4.1-~~7~~9—Protection System ITAAC (~~5~~ 12 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		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.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.17	Communications independence is provided between PS equipment and non-Class 1E equipment.	Tests, analyses, or a combination of tests and analyses will be performed on the as-installed PS equipment.	A report exists and concludes that: • Data communications between PS function processors and non-Class 1E equipment is through a Monitoring and Service Interface (MSI). • The MSI processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor and the MSI processor. • The MSI processors operate in a strictly cyclic manner. • The MSI processors operate asynchronously from the communications processors.
4.18	The PS is designed so that safety-related functions required for 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.	A failure modes and effects analysis will be performed on the PS.	A report exists and concludes that the PS is designed so that safety-related functions required for 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.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
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.	Inspections will be performed on the PS equipment to verify that the equipment for each PS division is distinctly identified and distinguishable from other markings placed on the equipment and that the identifications do not require frequent use of reference material.	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.	a. Inspections will be performed to verify the existence of locking mechanisms on the PS cabinet doors. b. Tests will be performed to verify the proper operation of the locking mechanisms on the PS cabinet doors. c. Tests will be performed to verify an indication exists in the MCR when a PS cabinet door is in the open position.	a. Locking mechanisms exist on the PS cabinet doors. b. The locking mechanisms on the PS cabinet doors operate properly. c. 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.	a. Inspections will be performed to verify the existence of key lock switches that restrict modifications to the PS software. b. Tests will be performed to verify that the key lock switches restrict modifications to the PS software	a. Key lock switches are provided at the PS cabinets. b. Key lock switches at the PS cabinets restrict modifications to the PS software.

14.03.05-4

Table 2.4.1-~~7~~9—Protection System ITAAC (~~5~~ 12 Sheets)

14.03.05-4

	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.
5.1	~~The~~ Class1E 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.	a. Testing will be performed for components identified as Class 1E in Table 2.4.1-1 by providing a test signal in each normally aligned division. b. Testing will be performed for components identified as Class 1E in Table 2.4.1-1 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 2.4.1-1. 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 2.4.1-1.

14.03.05-4

Next File

2.4.2 Safety Information and Control System

1.0 Description

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

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

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

2.0 Arrangement

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

2.2 Deleted.

14.03.05-4

3.0 Mechanical Design Features

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

4.0 I&C Design Features, Displays and Controls

4.1 The capability to transfer control of the SICS from the MCR to the RSS exists.

14.03.05-4

4.2 Deleted.

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 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.
4. Testing phase.
5. Installation and commissioning phase.

14.03.05-4

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 are present at the SICS cabinets located outside of the MCR to 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.

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.

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

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

14.03.05-4

14.03.05-4

Table 2.4.2-2—Safety Information and Control System ITAAC
(~~4~~ 8 Sheets) ← 14.03.05-4

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	~~The location of the~~ SICS equipment is located as listed in Table 2.4.2-1.	Inspection will be performed of the location of the SICS equipment.	The SICS equipment listed in Table 2.4.2-1 is located as listed in Table 2.4.2-1.
2.2	Deleted.	Deleted.	Deleted..
3.1	Equipment identified as Seismic Category I ~~in Table 2.4.2-1~~can withstand seismic design basis loads without loss of safety function. ↑ 14.03.05-4	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment ~~listed~~ identified as Seismic Category I in Table 2.4.1-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements.	a. Tests/analysis reports exist and conclude that the equipment ~~listed~~ identified as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function.
		b. Inspections will be performed of the as-installed Seismic Category I equipment listed in Table 2.4.2-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	b. Inspection reports exist and conclude that the as-installed Seismic Category I equipment listed in Table 2.4.2-1 including anchorage is installed as specified on the construction drawings.
4.1	The capability to transfer control of the SICS from the MCR to the RSS exists.	a. Inspections will be performed to verify the existence of procedures.	a. A report exists and concludes that procedures exist for transfer of control of the SICS from the MCR to the RSS.
		b. Tests will be performed to verify that control of the SICS can be transferred from the MCR to the RSS.	b. A report exists and concludes that the test results confirm that control of the SICS can be transferred from the MCR to the RSS.
4.2	Deleted.	Deleted.	Deleted.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.3	Electrical isolation is provided on connections between the ~~safety~~ safety-related parts of the SICS and non-Class 1E equipment.~~and the non safety I&C systems.~~	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the ~~safety~~ safety-related parts of the SICS and ~~the~~ non-Class 1E equipment. ~~safety I&C systems.~~	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 ~~safety~~ safety-related parts of the SICS and ~~the~~ non-Class 1E equipment. ~~safety I&C systems.~~
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the ~~safety~~ safety-related parts of the SICS and ~~the~~ non-Class 1E equipment. ~~safety I&C systems.~~	b. A report exists and concludes that the Class 1E isolation devices used between the ~~safety~~ safety-related parts of the SICS and ~~the~~ non-Class 1E equipment. ~~safety I&C systems~~ prevent the propagation of credible electrical faults.
		c. Inspections will be performed on ~~all~~ connections between the ~~safety~~ safety-related parts of the SICS and ~~the~~ non-Class 1E equipment. ~~safety I&C systems.~~	c. Class 1E electrical isolation devices exist on ~~all~~ 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 ~~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 hardware and software are developed using a design process composed of five life cycle phases with each	a. Inspections will be performed to verify that the SICS basic design phase process has design outputs.	a. A report exists and provides the design outputs for the basic design phase of the SICS hardware and software design process.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		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.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between the four SICS divisions. c. Inspections will be performed on connections between the four SICS divisions.	b. A report exists and concludes that the Class 1E isolation devices used between the four SICS divisions prevent the propagation of credible electrical faults. c. Class 1E electrical isolation devices exist on connections between the four SICS divisions.
4.8	Communications independence is provided between the four SICS divisions.	Tests, analyses, or a combination of tests and analyses will be performed on the as-installed SICS equipment.	A report exists and concludes that: • The SICS function processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor and the SICS function processor. • The SICS function processors operate in a strictly cyclic manner. • The SICS function processors operate asynchronously from the SICS communications processors.
4.9	Communications independence is provided between SICS equipment and non-Class 1E equipment.	Tests, analyses, or a combination of tests and analyses will be performed on the as-installed SICS equipment.	A report exists and concludes that communications independence is provided between SICS equipment and non-Class 1E equipment.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.10	The SICS is designed so that safety-related functions required for 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.	A failure modes and effects analysis will be performed on the SICS.	A report exists and concludes that the SICS is designed so that safety-related functions required for 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.	Inspections will be performed on the SICS equipment to verify that the equipment for each SICS division is distinctly identified and distinguishable from other markings placed on the equipment and that the identifications do not require frequent use of reference material.	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.	a. Inspections will be performed to verify the existence locking mechanisms on the SICS cabinet doors located outside the MCR. b. Tests will be performed to verify the proper operation of the locking mechanisms on the SICS cabinet doors located outside of the MCR.	a. Locking mechanisms exist on the SICS cabinet doors located outside of the MCR. b. The locking mechanisms on the SICS cabinet doors located outside of the MCR operate properly.

14.03.05-4

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 are present at the SICS cabinets located outside of the MCR to restrict modifications to the SICS software.	a. Inspections will be performed to verify the existence of key lock switches that restrict modifications to the SICS software at the SICS cabinets located outside the MCR.	a. Key lock switches are provided at the SICS cabinets located outside the MCR.
		b. Tests will be performed to verify that the key lock switches at the SICS cabinets located outside the MCR restrict modifications to the SICS software.	b. Key lock switches at the SICS cabinets located outside the MCR 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 as-installed SICS will be performed to verify the SICS can perform its safety function when one of the SICS divisions is out of service.	a. The SICS can perform its safety functions 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.	b. Out of service divisions of SICS are indicated in the MCR.

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
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. 14.03.05-4	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

2.4.4 Safety Automation System

1.0 Description

14.03.05-4

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

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

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

14.03.05-4

2.0 Arrangement

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

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

3.0 Mechanical Design Features

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

4.0 I&C Design Features, Displays and Controls

14.03.05-4

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

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

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

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

4.5 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.
4. Testing phase.
5. Installation and commissioning phase. 14.03.05-4

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.

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.

14.03.05-4

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

14.03.05-4

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	~~The location of the~~ SAS equipment is located as listed in Table 2.4.4-1.	~~An i~~Inspections will be performed of the location of the SAS equipment ~~listed in Table 2.4.4-1~~.	The SAS equipment listed in Table 2.4.4-1 is located as listed in Table 2.4.4-1.
2.2	Physical ~~Separation~~ separation exists between the four divisions of the SAS.	Inspections will be performed to verify that ~~redundant~~ the divisions of the SAS are located in separate safeguard buildings.	The four divisions of the SAS are located in separate safeguard buildings.
3.1	Equipment identified as Seismic Category I ~~in Table 2.4.4-1~~ can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the equipment ~~listed~~ identified as Seismic Category I in Table 2.4.4-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements.	a. Tests/analysis reports exist and conclude that the equipment ~~listed~~ identified as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without loss of safety function.
		b. Inspections will be performed of the as-installed Seismic Category I equipment ~~listed~~ identified in Table 2.4.4-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	b. Inspection reports exist and conclude that the as-installed Seismic Category I equipment ~~listed~~ identified in Table 2.4.4-1 including anchorage is installed as specified on the construction drawings.
4.1	~~Equipment~~ Class 1E SAS equipment ~~listed as Class 1E in Table 2.4.4-1~~ can perform its safety function when subjected to ~~electromagnetic interference~~ 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 2.4.4-1.	A report exists and concludes that the equipment ~~listed~~ identified as Class 1E in Table 2.4.4-1 can perform its safety function when subjected to electromagnetic interference EMI, RFI, ESD, and power surges.
4.2	The SAS receives input signals from the sources listed in Table 2.4.4-2.	Tests will be performed to verify the existence of input signals.	The SAS receives input signals from the sources listed in Table 2.4.4-2.
4.3	The SAS provides the output signals listed in Table 2.4.4-3.	Tests will be performed to verify the existence of output signals.	The SAS provides output signals to the recipients listed in Table 2.4.4-3.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
		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.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.7	Electrical isolation is provided on connections between SAS equipment and non-Class 1E equipment.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between SAS equipment and non-Class 1E equipment.	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 SAS equipment and non-Class 1E equipment.
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between SAS equipment and non-Class 1E equipment.	b. A report exists and concludes that the Class 1E isolation devices used between SAS equipment and non-Class 1E equipment prevent the propagation of credible electrical faults.
		c. Inspections will be performed on connections between SAS equipment and non-Class 1E equipment.	c. Class 1E electrical isolation devices exist on connections between SAS equipment and non-Class 1E equipment.

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.8	Communications independence is provided between the four SAS divisions.	Tests, analyses, or a combination of tests and analyses will be performed on the as-installed SAS equipment.	A report exists and concludes that: • The SAS function processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor and the SAS function processor. • The SAS function processors operate in a strictly cyclic manner. • The SAS function processors operate asynchronously from the SAS communications processors.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.9	Communications independence is provided between SAS equipment and non-Class 1E equipment.	Tests, analyses, or a combination of tests and analyses will be performed on the as-installed SAS equipment.	A report exists and concludes that: • Data communications between SAS function processors and non-Class 1E equipment is through a Monitoring and Service Interface (MSI). • The MSI processors do not interface directly with a network. Separate communication processors interface directly with the network. • Separate send and receive data channels are used in both the communications processor and the MSI function processor. • The MSI processors operate in a strictly cyclic manner. • The MSI processors operate asynchronously from the communications processors.
4.10	The SAS is designed so that safety-related functions required for 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.	A failure modes and effects analysis will be performed on the SAS.	A report exists and concludes that the SAS is designed so that safety-related functions required for 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.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
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.	Inspections will be performed on the SAS equipment to verify that the equipment for each SAS division is distinctly identified and distinguishable from other markings placed on the equipment and that the identifications do not require frequent use of reference material.	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.	a. Inspections will be performed to verify the existence of locking mechanisms on the SAS cabinet doors. b. Tests will be performed to verify the proper operation of the locking mechanisms on the SAS cabinet doors. c. Tests and inspections will be performed to verify an indication exists in the MCR when a SAS cabinet door is in the open position.	a. Locking mechanisms exist on the SAS cabinet doors. b. The locking mechanisms on the SAS cabinet doors operate properly. c. 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.	a. Inspections will be performed to verify the existence of key lock switches that restrict modifications to the SAS software. b. Tests will be performed to verify that the key lock switches restrict modifications to the SAS software.	a. Key lock switches are provided at the SAS cabinets. b. Key lock switches at the SAS cabinets restrict modifications to the SAS software.

14.03.05-4

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
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.	a. A test of the as-installed SAS will be performed to verify the SAS can perform its safety function when one of the SAS divisions is out of service. b. Inspections will be performed to verify the existence of indication in the MCR when a SAS division is placed out of service.	a. The SAS can perform its safety functions when one of the SAS divisions is out of service. b. Out of service divisions of SAS are indicated in the MCR.
4.15	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 2.4.4-2 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 2.4.4-2 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.

14.03.05-4

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

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
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. 14.03.05-4	a. Testing will be performed for components identified as Class 1E in Table 2.4.4-1 by providing a test signal in each normally aligned division. b. Testing will be performed for components identified as Class 1E in Table 2.4.4-1 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 2.4.4-1. 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 2.4.4-1.

Next File

2.4.5 Priority and Actuator Control System

1.0 Description

14.03.05-4

The priority and actuator control system (PACS) is a safety-related system.

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

- Prioritizes actuation requests from I&C systems.
- Performs essential equipment protection.
- Performs drive actuation.
- Performs drive monitoring.

14.03.05-4

2.0 Arrangement

2.1 ~~The~~ PACS equipment is located as listed in Table 2.4.5-1—Priority and Actuator Control System Equipment.

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

14.03.05-4

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I ~~in Table 2.4.5-1~~ can withstand seismic design basis loads without loss of safety function.

4.0 I&C Design Features, Displays and Controls

4.1 The order of priority of automatic functions performed by PACS is listed from highest to lowest:

- Safety-related I&C functions.
- Non-~~safety~~ safety-related I&C functions.

4.2 Electrical isolation is provided on connections between ~~the~~ PACS equipment and non-Class 1E equipment.~~the non-safety I&C systems.~~

4.3 ~~The~~ Class 1E PACS equipment ~~classified as Class 1E in Table 2.4.5-1~~ can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

4.4 The input wiring from other I&C systems to the PACS is properly connected.

4.5 The capability for testing of the PACS is provided while retaining the capability of the PACS to accomplish its safety function. PACS divisions in test are indicated in the MCR.

14.03.05-4

14.03.05-4

4.6 Locking mechanisms are provided on the PACS cabinet doors. Opened PACS cabinet doors are indicated in the MCR.

4.7 The equipment for each PACS 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.

5.0 Electrical Power Design Features

5.1 ~~The~~ Class 1E PACS components ~~identified as Class 1E in Table 2.4.5-1~~ are powered from ~~the~~ a Class 1E division ~~as listed in Table 2.4.5-1~~ in a normal or alternate feed condition.

14.03.05-4

6.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.5-2 lists the PACS ITAAC.

14.03.05-4

Table 2.4.5-1—Priority and Actuator Control System Equipment

Equipment Description	Equipment Tag Number (1)	Equipment Location	Seismic ~~Class~~ Category	IEEE Class 1E(2)
~~Priority and Actuator Control System~~ PACS Cabinets, Division 1 ~~Cabinets~~	30CLE6	Safeguard Building 1	I	1^N 2^A
~~Priority and Actuator Control System~~PACS Cabinets, Division 2 ~~Cabinets~~	30CLF6	Safeguard Building 2	I	2^N 1^A
~~Priority and Actuator Control System~~PACS Cabinets, Division 3 ~~Cabinets~~	30CLG6	Safeguard Building 3	I	3^N 4^A
~~Priority and Actuator Control System~~ PACS Cabinets, Division 4 ~~Cabinets~~	30CLH6	Safeguard Building 4	I	4^N 3^A

14.03.05-4

1) Equipment Tag numbers are provided for information and are not part of the design certification.

2) ^{N} denotes the division the component is normally powered from. ^{A} denotes the division the component is powered from when alternate feed is implemented.

Table 2.4.5-2—Priority and Actuator Control System ITAAC
(~~2~~ 4 Sheets) ← 14.03.05-4

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	~~The~~ PACS equipment is located as listed in Table 2.4.5-1.	Inspections will be performed of the location of the PACS equipment.	The PACS equipment listed in Table 2.4.5-1 is located as listed in Table 2.4.5-1.
2.2	Physical separation exists between the four divisions of the PACS.	Inspections will be performed to verify that the divisions of the PACS are located in separate ~~Safeguard~~ safeguard ~~Buildings~~buildings.	The four divisions of the PACS are located in separate safeguard buildings.
3.1	Equipment identified as Seismic Category I ~~in Table 2.4.5-1~~ can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment ~~listed~~ identified as Seismic Category I in Table 2.4.5-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements. b. Inspections will be performed of the as-installed Seismic Category I equipment ~~listed~~ identified in Table 2.4.5-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	a. Tests/analysis reports exist and conclude that the equipment ~~listed~~ identified as Seismic Category I in Table 2.4.5-1 can withstand seismic design basis loads without loss of safety function. b. Inspection reports exist and conclude that the as-installed Seismic Category I equipment ~~listed~~ identified in Table 2.4.5-1 including anchorage is installed as specified on the construction drawings.
4.1	The order of priority of automatic functions performed by PACS is listed from highest to lowest: • ~~Safety~~ Safety-related I&C functions. • Non-~~safety~~ safety-related I&C functions.	Operational tests will be performed using test signals to verify the order of priority of automatic functions performed by PACS.	The order of priority of automatic functions performed by PACS is listed from highest to lowest: Safety related I&C functions Non-safety related I&C functions

↑ 14.03.05-4

Table 2.4.5-2—Priority and Actuator Control System ITAAC
(~~2~~ 4 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.2	Electrical isolation is provided on connections between ~~the~~ PACS equipment and non-Class 1E equipment.~~the non-safety I&C systems.~~	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between ~~the~~ PACS equipment and non-Class 1E equipment.~~the non safety I&C systems.~~	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~~ PACS equipment and non-Class 1E equipmen. ~~the non safety I&C systems.~~
		b. Type tests, analyses, or a combination of type tests and analyses will be performed on the electrical isolation devices between ~~the~~ PACS equipment and non-Class 1E equipment.~~the non safety I&C systems.~~	b. A report exists and concludes that the Class 1E isolation devices used between ~~the~~ PACS equipment and non-Class 1E equipment ~~the non safety I&C systems~~ prevent the propagation of credible electrical faults.
		c. Inspections will be performed on ~~all~~ connections between ~~the~~ PACS equipment and non-Class 1E equipment. ~~the non safety I&C systems.~~	c. Class 1E electrical isolation devices exist on ~~all~~ connections between ~~the~~ PACS and non-Class 1E equipment.~~the non safety I&C systems.~~
4.3	~~The~~ Class 1E PACS equipment ~~classified as Class 1E in Table 2.4.5-1~~ 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 2.4.5-1.	A report exists and concludes that the equipment ~~listed~~ identified as Class 1E in Table 2.4.5-1 can perform its safety function when subjected to EMI, RFI, ESD, and power surges.
4.4	The input wiring from other I&C systems to the PACS is properly connected.	Inspections will be performed to verify that the input wiring from other I&C systems to the PACS is properly connected.	The input wiring from the other I&C systems to the PACS is properly connected.

14.03.05-4

Table 2.4.5-2—Priority and Actuator Control System ITAAC
(~~2~~ 4 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.5	The capability for testing of the PACS is provided while retaining the capability of the PACS to accomplish its safety function. PACS divisions in test are indicated in the MCR.	a. Testing will be performed to verify the capability for testing of the PACs is provided while retaining the capability to accomplish its safety function. b. Inspections will be performed to verify the existence of indication in the MCR when a division of the PACS is placed in test.	a. The capability for testing of the PACS is provided while retaining the capability of the PACS to accomplish its safety functions. b. PACS divisions in test are indicated in the MCR.
4.6	Locking mechanisms are provided on the PACS cabinet doors. Opened PACS cabinet doors are indicated in the MCR.	a. Inspections will be performed to verify the existence of locking mechanisms on the PACS cabinet doors. b. Tests will be performed to verify the proper operation of the locking mechanisms on the PACS cabinet doors. c. Tests and inspections will be performed to verify an indication exists in the MCR when a PACS cabinet door is in the open position.	a. Locking mechanisms exist on the PACS cabinet doors. b. The locking mechanisms on the PACS cabinet doors operate properly. c. Opened PACS cabinet doors are indicated in the MCR.
4.7	The equipment for each PACS 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.	Inspections will be performed on the PACS equipment to verify that the equipment for each PACS division is distinctly identified and distinguishable from other markings placed on the equipment and that the identifications do not require frequent use of reference material.	The equipment for each PACS 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.

14.03.05-4

Table 2.4.5-2—Priority and Actuator Control System ITAAC
(~~2~~ 4 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
5.1	~~The~~ Class 1E PACS components ~~identified as Class 1E in Table 2.4.5-1~~ are powered from ~~the~~ a Class 1E division ~~as listed in Table 2.4.5-1~~ in a normal or alternate feed condition. 14.03.05-4	a. Testing will be performed for components identified as Class 1E in Table 2.4.5-1 by providing a test signal in each normally aligned division. b. Testing will be performed for components identified as Class 1E in Table 2.4.5-1 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 2.4.5-1. 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 2.4.5-1.

Next File

2.4.10 Process Information and Control System

1.0 Description

The process information and control system (PICS) is a digital human machine interface (HMI). It provides monitoring and control of plant systems. The PICS is non-~~safety~~ safety-related and is provided in both the main control room (MCR) and the remote shutdown station (RSS).

14.03.05-4

2.0 I&C Design Features

2.1 The system hardware and software in the PICS is diverse from the safety-related system hardware and software in the Safety Information and Control System (SICS).

2.2 Deleted.

14.03.05-4

2.3 Deleted.

2.4 Electrical isolation is provided on PICS connections between the RSS and the MCR ~~for the PICS~~.

2.5 The capability to transfer control of the PICS from the MCR to the RSS exists.

3.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.10-1 lists the PICS ITAAC.

Table 2.4.10-1—Process Information and Control System ITAAC (2 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	The system hardware and software in the PICS is diverse from the safety-related system hardware and software in the SICS.	An analysis will be performed to demonstrate that the system hardware and software in the PICS is diverse from the safety-related system hardware and software in the SICS.	A report exists and concludes that the system hardware and software in the PICS is diverse from the safety-related system hardware and software in the SICS.
2.2	Deleted.	Deleted.	Deleted.
2.3	Deleted.	Deleted.	Deleted.
2.4	Electrical ~~Isolation~~ isolation is provided on PICS connections between the RSS and the MCR ~~for the PICS~~.	a. Analyses will be performed to determine the test specification for electrical isolation devices on connections between the RSS and the MCR for the PICS. 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 PICS. c. Inspections will be performed on connections between the RSS and the MCR for the PICS. ~~An inspection will be performed.~~	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 PICS. b. A report exists and concludes that the isolation devices used between the RSS and the MCR for the PICS prevent the propagation of credible electrical faults. c. Electrical isolation devices exist on connections between the RSS and the MCR for the PICS. ~~Electrical isolation is provided between RSS and the MCR for the PICS.~~

14.03.05-4

Table 1.8-2—U.S. EPR Combined License Information Items
Sheet 38 of 45

Item No.	Description	Section	Action Required by COL Applicant	Action Required by COL Holder
13.4-1	A COL applicant that references the U.S. EPR design certification will provide site-specific information for operational programs and schedule for implementation.	13.4	Y	
13.5-1	A COL applicant that references the U.S. EPR design certification will provide site-specific information for administrative, operating, emergency, maintenance, and other operating procedures.	13.5	Y	
13.6-1	A COL applicant that references the U.S. EPR design certification will provide a site-specific security assessment that adequately demonstrates how the performance requirements of 10 CFR 73.55(a) are met for the initial implementation of the security program.	13.6	Y	
13.6-2	A COL applicant that references the U.S. EPR design certification will provide a security plan to the NRC to fulfill the requirements of 10 CFR 52.79(a)(35).	13.6	Y	
13.6-3	A COL applicant that references the U.S. EPR design certification will provide a security program, through the PSP and supporting documents such as the vital equipment list and the vital areas list, that incorporates the security features listed in the U.S. EPR FSAR Tier 2, Section 13.6	13.6 14.03.05-3	Y	
13.6-4	A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54.	13.6	Y	
13.7-1	A COL applicant that references the U.S. EPR design certification will submit a physical security plan to the NRC to fulfill the fitness for duty requirements of 10 CFR 26.	13.7	Y	
14.2-1	A COL applicant that references the U.S. EPR certified design will provide site specific information that describes the organizational units that manage, supervise, or execute any phase of the test program.	14.2.2	Y	

13.4 Operational Program Implementation

A COL applicant that references the U.S. EPR design certification will provide site-specific information for operational programs and schedule for implementation.

The following operational programs are described in the FSAR, and the COL applicant will verify or provide the implementation schedule:

- Inservice inspection program (refer to Section 5.2.4 and Section 6.6).
- Inservice testing program (refer to Section 3.9.6 and Section 5.2.4).
- Environmental qualification program (refer to Section 3.11).
- Preservice inspection program (refer to Section 5.2.4 and Section 6.6).
- Reactor vessel material surveillance program (refer to Section 5.3.1).
- Preservice testing program (refer to Section 3.9.6 and Section 5.2.4).
- Containment leakage rate testing program (refer to Section 6.2.6).
- Fire protection program (refer to Section 9.5.1).
- Process and effluent monitoring and sampling program (refer to Section 11.5).
- Motor-operated valve testing (refer to Section 3.9.6).
- Initial Test Program (refer to Section 14.2).

The following operational programs are described by the COL applicant, and the COL applicant will provide the implementation schedule:

- Non-licensed plant staff training program (refer to Section 13.2).
- Reactor operator training program (refer to Section 13.2).
- Reactor operator requalification program (refer to Section 13.2).
- Emergency planning (refer to Section 13.3).
- Security program (refer to Section 13.6).
- Quality assurance program–operation (refer to Section 17.5).
- Radiation protection program (refer to Section 12.5).
- Maintenance rule (refer to Section 17.6).
- Cyber security plan (refer to Section 13.6). ← 14.03.05-3

Next File

13.6 Security

The physical security program provides physical features to detect, delay, assist response to, and defend against the design basis threat (DBT) for radiological sabotage. The standard design features of the U.S. EPR that enhance security can be found in Technical Report ANP-10296, "U.S. EPR Design Features that Enhance Security."

A COL applicant that references the U.S. EPR design certification will provide a site-specific security assessment that adequately demonstrates how the performance requirements of 10 CFR 73.55(a) are met for the initial implementation of the security program. The Security Assessment is Safeguards Information (SGI) and therefore is restricted from public release under 10 CFR 73.21. The site specific Security Assessment addresses identification of vital equipment, development of target sets, vulnerability assessments, defensive analyses, design features to enhance security, the portions of the NRC orders to the current operating plants that impact U.S. EPR design, and the other security features of the U.S. EPR that establish the security system design.

A COL applicant that references the U.S. EPR design certification will provide a security plan to the NRC to fulfill the requirements of 10 CFR 52.79(a)(35). The security plan consists of the Physical Security Plan (PSP), the guard force training and qualification (T&Q) plan, and the safeguards contingency plan. The security plan is SGI and therefore is restricted from public release under 10 CFR 73.21.

14.03.05-3 → A COL applicant that references the U.S. EPR design certification will provide a cyber security plan consistent with 10 CFR 73.54.

A COL applicant that references the US EPR design certification will provide a security program, through the PSP and supporting documents such as the Vital Equipment List and the Vital Areas list, that incorporates the following security features:

13.6.1 Protected Area and Vital Areas

1. Vital equipment is located only within a Vital Area. Vital Areas boundaries are physical barriers with access controls provided for each of the points of entry.

2. Locations of vital equipment have been identified in the Vital Equipment List as found in Appendix A of Technical Report ANP-10295, "U.S. EPR Security Features." This document is Safeguards Information (SGI) and therefore is restricted from public release under 10 CFR 73.21.

3. Access to vital equipment requires passage through at least two physical barriers as defined in 10 CFR 73.2(a). The first substantial barrier between an adversary and a Vital Area is the Protected Area boundary which is described by the COL applicant in the site-specific PSP. The second substantial boundary is the Vital