ArevaEPRDCPEm Resource

From: WELLS Russell D (AREVA NP INC) [Russell.Wells@areva.com]
Sent: Thursday, December 17, 2009 1:26 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. 285, FSAR Ch 7, Supplement 1
Attachments: RAI 285 Supplement 1 Response US EPR DC.pdf

Getachew,

AREVA NP Inc. provided responses to 4 of the 20 questions of RAI No. 285 on November 11, 2009. The attached file, “RAI 285 Supplement 1 Response US EPR DC.pdf” provides technically correct and complete responses to 6 of the remaining 16 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which supports the response to RAI 285 Questions 07.02-31 and 07.03-23.

The following table indicates the respective pages in the response document, “RAI 285 Supplement 1 Response US EPR DC.pdf,” that contain AREVA NP’s response to the subject questions.

Question #	Start Page	End Page
RAI 285 — 07.01-12	2	2
RAI 285 — 07.02-31	3	3
RAI 285 — 07.03-22	4	5
RAI 285 — 07.03-23	6	6
RAI 285 — 07.03-24	7	8
RAI 285 — 07.05-9	9	9

The schedule for a technically correct and complete response to the remaining questions is unchanged and provided below.

Question #	Response Date
RAI 285 — 07.01-13	January 22, 2010
RAI 285 — 07.01-15	January 22, 2010
RAI 285 — 07.01-16	January 22, 2010
RAI 285 — 07.01-17	January 22, 2010
RAI 285 — 07.03-21	January 22, 2010
RAI 285 — 07.03-25	February 26, 2010
RAI 285 — 07.03-26	January 22, 2010
RAI 285 — 07.03-27	January 22, 2010
RAI 285 — 07.04-11	January 22, 2010
RAI 285 — 07.04-13	January 22, 2010

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: Wednesday, November 11, 2009 6:11 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 285, FSAR Ch. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information RAI 285. The attached file, "RAI 285 Response US EPR DC.pdf" provides technically correct and complete responses to 4 of the 20 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 285 Questions 07.01-14 and 07.04-12.

The following table indicates the respective page(s) in the response document, "RAI 285 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	**Start Page**	**End Page**
RAI 285 — 07.01-12	2	2
RAI 285 — 07.01-13	3	3
RAI 285 — 07.01-14	4	4
RAI 285 — 07.01-15	5	5
RAI 285 — 07.01-16	6	6
RAI 285 — 07.01-17	7	8
RAI 285 — 07.02-30	9	10
RAI 285 — 07.02-31	11	11
RAI 285 — 07.03-21	12	12
RAI 285 — 07.03-22	13	13
RAI 285 — 07.03-23	14	14
RAI 285 — 07.03-24	15	15
RAI 285 — 07.03-25	16	16
RAI 285 — 07.03-26	17	17
RAI 285 — 07.03-27	18	18
RAI 285 — 07.04-10	19	19
RAI 285 — 07.04-11	20	20
RAI 285 — 07.04-12	21	21
RAI 285 — 07.04-13	22	23
RAI 285 — 07.05-9	24	24

A complete answer is not provided for 16 of the 20 questions. The schedule for a technically correct and complete response to these questions is provided below.

Question #	Response Date
RAI 285 — 07.01-12	December 18, 2009
RAI 285 — 07.01-13	January 22, 2010
RAI 285 — 07.01-15	January 22, 2010
RAI 285 — 07.01-16	January 22, 2010
RAI 285 — 07.01-17	January 22, 2010
RAI 285 — 07.02-31	December 18, 2009
RAI 285 — 07.03-21	January 22, 2010
RAI 285 — 07.03-22	December 18, 2009
RAI 285 — 07.03-23	December 18, 2009
RAI 285 — 07.03-24	December 18, 2009
RAI 285 — 07.03-25	February 26, 2010
RAI 285 — 07.03-26	January 22, 2010
RAI 285 — 07.03-27	January 22, 2010
RAI 285 — 07.04-11	January 22, 2010
RAI 285 — 07.04-13	January 22, 2010
RAI 285 — 07.05-9	December 18, 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: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Tuesday, October 13, 2009 4:49 PM
To: ZZ-DL-A-USEPR-DL
Cc: Spaulding, Deirdre; Truong, Tung; Morton, Wendell; Cheung, Calvin; Jackson, Terry; Canova, Michael; Guardiola, Maria; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 285(3560,3507,3552,3564,3565), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 25, 2009, and discussed with your staff on September 3, 2009. Draft RAI Question 07-01-13 was 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: 1056

Mail Envelope Properties (1F1CC1BBDC66B842A46CAC03D6B1CD410251CDDF)

Subject: Response to U.S. EPR Design Certification Application RAI No. 285, FSAR Ch 7, Supplement 1
Sent Date: 12/17/2009 1:25:34 PM
Received Date: 12/17/2009 1:25:37 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	5907	12/17/2009 1:25:37 PM
RAI 285 Supplement 1 Response US EPR DC.pdf		133691

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

Response to

Request for Additional Information No. 285, Supplement 1 (3560, 3507, 3552, 3564, 3565), Revision 1

10/13/2009

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.01 - Instrumentation and Controls - Introduction
SRP Section: 07.02 - Reactor Trip System
SRP Section: 07.03 - Engineered Safety Features Systems
SRP Section: 07.04 - Safe Shutdown Systems
SRP Section: 07.05 - Information Systems Important to Safety

Application Section: FSAR Ch. 7

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

Question 07.01-12:

Follow-up to RAI Question 07.01-3

In the U.S. EPR DC-FSAR, provide additional detail in Figure 7.1-2, "U.S. EPR I&C Architecture," to show the interfaces from Level 2 to Level 3, and show all of the systems that are categorized at Level 0. Additionally, provide corresponding updates to the U.S. EPR FSAR.

The staff reviewed the AREVA NP response to RAI 07.01-3, and found that a supplemental RAI is necessary. 10 CFR 52.47 states that a description shall be sufficient to permit understanding of the system designs. Although FSAR Section 7.1.1.1 states in part "… The U.S. EPR I&C architecture is represented in Figure 7.1-2 - U.S. EPR I&C Architecture. The overall I&C architecture is categorized into four levels … Other than interfaces provided from Level 2, these systems are not within the scope of this document and are not shown on Figure 7.1-2." The staff found that the interfaces from Level 2 to Level 3, which are within the scope, are not shown in Figure 7.1-2. Detail is needed in Figure 7.1-2, "U.S. EPR I&C Architecture," that shows the interfaces from Level 2 to Level 3. Additionally, the staff found that there are systems described in Section 7.1 that are categorized as Level 0, but are not shown in Figure7.1-2. Additional detail is needed in Figure 7.1-2 U.S. EPR I&C Architecture that shows all of the systems that are categorized at Level 0.

Response to Question 07.01-12:

U.S. EPR FSAR Tier 2, Figure 7.1-2—U.S. EPR I&C Architecture was revised in Reference 1 to show the systems that are categorized as Level 0.

Level 3 systems are not within the scope of the U.S. EPR FSAR, as indicated in U.S. EPR FSAR Tier 2, Section 7.1.1, but the interfaces between Level 2 and Level 3 systems are within the scope. Interfaces between the process information and control system (PICS) and Level 3 systems are shown on U.S. EPR FSAR Tier 2, Figure 7.1-2 and Figure 7.1-5—Process Information and Control System Architecture.

References for Question 07.01-12:

1. Letter, Sandra Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Conversion of ANP-10281P, 'U.S. EPR Digital Protection System Topical Report' to ANP-10309P, 'U.S. EPR Digital Protection System Technical Report'," NRC:09:119, November 24, 2009.

FSAR Impact:

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

Question 07.02-31:

Follow-up to RAI Questions No. 07.02-13 and 07.02-23.

For FSAR Tier 1,Table 2.4.1-7, ITAAC 4.2 is worded only for automatically-initiated actions. What about manually-initiated engineered safety features (ESF) actions?

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 5.2 of IEEE Std. 603-1991 states, in part, that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Table 2.4.1-7, ITAAC 4.2 states that "the PS generates automatic ESF signals. 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. The PS generates a ESF signal after the test signal reaches the trip limit for 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." To satisfy IEEE 603-1991, Clauses 5.2, the staff requires a Completion of Protection Action ITAAC for manually-initiated ESF actions.

Response to Question 07.02-31:

Manual functions processed by the protection system (PS) are listed in U.S. EPR FSAR Tier 1, Table 2.4.1-4—Protection System Manually Actuated Functions. U.S. EPR FSAR Tier 2, Table 2.4.1-7—Protection System ITAAC, Item 4.11 provides acceptance criteria for these functions and will be revised to clarify that the manually-initiated ESF actions continue until deliberate operator action is taken to return the PS to normal.

U.S. EPR FSAR Tier 1, Table 2.4.1-4 will also be revised to be consistent with recent design changes that result in additional manual functions being processed by the PS, chemical and volume control system (CVCS) isolation, anti-dilution isolation, and pressurizer safety relief valve (PSRV) opening. These design changes were discussed with the NRC staff during public meetings held in March and August of 2009, and have been incorporated into ANP-10309P, “U.S. EPR Digital Protection System Technical Report”.

FSAR Impact:

U.S. EPR FSAR Tier 1, Table 2.4.1-4 and Table 2.4.1-7 will be revised as described in the response and indicated on the enclosed markup.

Question 07.03-22:

Follow-up to RAI No. 07.03-6

Provide additional detail and or design documentation on the 'failure states' for the Engineered Safety Features Actuation System (ESFAS) design. Also, address the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 23 in the development of the failure modes and effects analysis (FMEA) tables and its associated write-up in U.S. EPR DC-FSAR Section 7.3. Addressing how a system manages a single failure in a power supply is one aspect of the question. However, AREVA NP did not fully address GDC 23 which asks for the failure state of safety equipment and why is that acceptable (whether single failure or not). Additionally, the assumptions given in AREVA's original response to this question cannot be gained from reading Section 7.3.

1. Will there be ITAAC to verify the response of the system to failures listed in GDC 23? Loss of electrical power is one scenario in GDC 23. GDC 23 requires design in terms of postulated adverse environments such as extreme heat.
2. Page 28 of the Teleperm XS Digital Protection System Manual States:

   > "The TXS system automatically detects failures in the subracks, the function processors, the I/O modules, and the communication functions. Failures that affect the subrack internal power supplies or control of the backplane bus will cause a transition to predefined fault conditions (e.g., reset) on the function computers, which results in a nonresponsive state in relationship to other subracks. Additionally, the TXS system monitors cabinet temperatures and cabinet cooling fan speed and provides the plant operators with an alarm if setpoints are exceeded."

   How is the failure of a subrack due to temperature bounded by the FMEA? What failure state would the system enter into?
3. How does the FMEA documented in Section 7.3 bound all the potential failure vectors such as those listed in GDC 23?

Response to Question 07.03-22:

While there are features in the Teleperm XS (TXS) platform that accommodate specific failure mechanisms and can place system outputs into a predefined failure state, the U.S. EPR protection system (PS) does not need to credit these features to demonstrate compliance with GDC 23 or the single failure criteria. A more conservative FMEA approach was utilized to simplify the analysis and more clearly bound the potential failure mechanisms.

A failure can appear at the output of the PS in one of two ways:

1. The failure results in non-actuation when actuation is required (blocking failure).
2. The failure results in actuation when actuation is not required (spurious failure).

These failure modes are bounding despite which phenomenon or mechanism causes the failure. As described in U.S. EPR FSAR Tier 2, Section 7.3.2.2, for the equipment analyzed in the PS FMEA, both blocking failures and spurious failures are considered, and the effects of these failures are acceptable with respect to plant safety.

This approach to the PS system-level FMEA bound potential failure vectors, including those listed in GDC 23. Regarding direct compliance to GDC 23, the PS FMEA demonstrates that any state a PS division fails to (i.e., spurious or blocking) is acceptable because plant safety is maintained in both cases.

As indicated in the Response to RAI 78, Supplement 2, Table 14.03.05-1—ITAAC Mapping of I&C System Requirements, PS compliance with GDC 23 is verified by U.S. EPR FSAR Tier 1, Section 2.4.1, Item 4.18.

FSAR Impact:

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

Question 07.03-23:

Follow-up to RAI Question 07.03-7

Provide clarification on the response to RAI Question 07.03-7 concerning compliance with IEEE Std. 603-1991, Clause 5.1.

In the response to RAI Question 07.03-7, AREVA NP provided an ITAAC Mapping of I&C system requirements to its associated IEEE Std. 603-1991 requirement, located in RAI 78, Supplement 2, Question 14.03.05-4 for U.S. EPR DC-FSAR, Section 2.4.1, ITAAC Item 4.18. However, upon reviewing the revised ITAAC (Item 4.18), the staff requires more clarification. Specifically, AREVA NP provided a summary failure modes and effects analysis (FMEA) as part of Chapter 7 of the U.S. EPR DC-FSAR. The summary FMEA goes the level of detail of the Protection System sub-components (i.e., acquisition and processing unit (APU), actuation logic unit (ALU), etc.). Will the FMEA described in Item 4.18 go to a further depth of detail to verify that single failure assumptions in the summary FMEA still hold. For example, a hardware/software analysis of the Network APU-ALU would show that it is not be susceptible to a single hardware device failure within the Network APU-ALU that would prevent signals from that APU being marked as invalid. Clarify within Item 4.18 the scope of the FMEA proposed.

Response to Question 07.03-23:

Topical Report ANP-10272, “Software Program Manual for TELEPERM XS Safety Systems,” Section 10.3.6 describes the FMEA to be performed on Teleperm XS (TXS)-based systems during the detailed design phase. This section states that the FMEA is “conducted at the replaceable module and component level.” The “Inspections, Tests, Analyses” column of U.S. EPR FSAR Tier 1, Table 2.4.1-7—Protection System ITAAC, Item 4.18 will be modified to clarify the scope of the analysis that will satisfy the commitment, consistent with the description in Topical Report ANP-10272.

For consistency, this clarification will also be made in U.S. EPR FSAR Tier 1, Table 2.4.2-2—Safety Information and Control System ITAAC and Table 2.4.4-5—Safety Automation System ITAAC.

FSAR Impact:

U.S. EPR FSAR Tier 1, Table 2.4.1-7, Table 2.4.2-2, and Table 2.4.4-5 will be revised as described in the response and indicated on the enclosed markup.

Question 07.03-24:

Follow-up to RAI Question 07.03-8

Provide clarification on bypassed or inoperable status indication in terms of the power systems supplying the Protection System (PS) to satisfy the requirements of IEEE Std. 603-1991, Clauses 5.7 and 6.7.

The PS ITAAC shown in RAI 78, Supplement 2, Question 14.03.05-4, Table 2.4.1-7, was modified to demonstrate a test for PS actuation in the presence of a maintenance bypass/inoperable status indication in the main control room to fulfill the requirements of IEEE Std. 603-1991, Clauses 5.7 and 6.7. Further clarification of AREVA NP's response is needed. Specifically, AREVA NP states, "The U.S. EPR has sufficient redundancy that a power system redundancy configuration of zero is unlikely; therefore, bypassed and inoperable status indication for power systems supporting digital I&C, as described in Clause 8.3 of IEEE 603-1991, is unnecessary."

1. How are the power systems configured such that a redundancy configuration of zero is unlikely?
2. What is meant by , ". . . power systems supporting digital I&C. . ."? Are these power systems that supply power to the PS and its supporting components, or is it power supplies within the PS cabinets themselves?
3. What power source indication or statuses are available on any PS console? By what means does an operator know if any power source is bypassed and/or inoperable?

Response to Question 07.03-24:

AREVA NP provided an inaccurate statement in the Response to RAI 60, Supplement 4, Question 07.03-8, which resulted in this question. Specifically, even though a redundancy configuration of zero is unlikely, a bypassed and inoperable status indication (BISI) of a safety-related system should still be provided. A BISI is provided for the Class 1E power supply systems as described in U.S. EPR FSAR Tier 2, Section 8.3.1.2.5 and Section 8.3.2.2.5.

This response answers the three specific questions requested. However, the questions are not related to demonstrating compliance with IEEE Std. 603-1991, Clause 5.7 and Clause 6.7.

1. Each of the four PS divisions is supplied by an independent division of electrical power. The unavailability of one division of power does not prevent the other three PS divisions from performing their safety-related functions. On the plant level, a redundancy configuration of zero is unlikely due to maintenance bypass. Within each electrical division, power to the PS cabinets is provided by the Class 1E uninterruptible power supply (EUPS) system. The Class 1E 24 Vdc I&C power supply is supplied via redundant AC/DC converters and DC/DC converters. The AC/DC converter is supplied via the EUPS vital AC distribution inverter while the DC/DC converter is supplied via the DC distribution panel. Both the AC/DC converter and DC/DC converter are sized to supply the entire I&C cabinet group so that on failure of one of the converters, or with a converter out of service, the other converter can supply the power demand of the entire group of 24 Vdc I&C cabinets, including margin.
2. The "power systems supporting digital I&C" refers to the 24 Vdc input power to the I&C cabinets supplied by the AC/DC and DC/DC converter cabinets.

This power supply is from the output of 480 Vac to 24 Vdc converters and 250 Vdc to 24 Vdc converters and it is not the power supply in the PS cabinets themselves. The AC/DC converter takes 480 Vac input power from the associated EUPS vital AC distribution motor control center (MCC) of its division. The DC/DC converter takes 250 Vdc input power from the associated EUPS DC distribution of its division. The AC/DC and DC/DC converters are operated in parallel, in an auctioneer arrangement so both power supplies are available to supply the I&C cabinet loads. Each converter cabinet is sized to supply the assigned load if the other converter cabinet fails or is out of service.

3. There is a converter trouble alarm associated with each of the AC/DC and DC/DC converters. The trouble alarm will alert the operator in the main control room (MCR) of abnormal conditions, such as out of tolerance output voltage, converter module failure, converter module removal, and trip of protective devices. There is also MCR indication of the 24 Vdc power supply bus for each AC/DC and DC/DC converter.

   The converter component parameters are provided at the local equipment. Indication of a trouble alarm will require local monitoring to verify the specific failure condition. The voltage indication and trouble alarm provide sufficient indication to the MCR operator to indicate potential failures, and if the power source is bypassed and/or inoperable. Bypassed and inoperable status indication of the electrical power supply systems is discussed in U.S. EPR FSAR Tier 2, Section 8.3.1.2.5 and Section 8.3.2.2.5.

FSAR Impact:

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

Question 07.05-9:

Follow-up to RAI Question No. 07.05-3.

The ITAAC identified in the RAI response to Question 07.05-3 are considered design acceptance criteria (DAC) and should be noted so.

10 CFR 52.47(a)(2) states “the application must contain a level of design information sufficient to enable the Commission to judge the applicant’s proposed means of assuring that construction conforms to the design and to reach a final conclusion on all safety questions associated with the design before the certification is granted.” SECY-92-053 provides guidance on meeting the requirements through DAC since advanced instrumentation and controls is identified as an area where the use of DAC is appropriate. The ITAAC for the post-accident monitoring instrumentation to develop the final list of variables, their accuracy and ranges, etc. should be identified as DAC in the ITAAC itself.

Response to Question 07.05-9:

The Response to RAI 307, Question 14.03.03-45 will address identification of all DAC for the U.S. EPR design.

FSAR Impact:

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

U.S. EPR Final Safety Analysis Report Markups

Table 2.4.1-4~~5~~—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
CVCS Isolation
Anti-Dilution Isolation
PSRV Opening

07.02-31

Table 2.4.1-7~~9~~—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. 07.02-31	~~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-~~5~~4, the PS generates actuation signals ~~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. Deliberate manual action is required to return the PS to normal.
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 2.4.1-5~~7~~, 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.

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

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
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 at the level of replaceable modules and components. 07.03-23	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.
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.

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 at the level of replaceable modules and components. 07.03-23	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.

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 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 at the level of replaceable modules and components.. 07.03-23	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.