ArevaEPRDCPEm Resource

From: WILLIFORD Dennis (AREVA) [Dennis.Williford@areva.com]
Sent: Friday, December 02, 2011 3:57 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy (AREVA); CRIBB Arnie (EXTERNAL AREVA); DELANO Karen (AREVA); HATHCOCK Phillip (AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); LENTZ Tony (EXTERNAL AREVA); HUDSON Greg (AREVA); MEACHAM Robert (AREVA)
Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Batch 2
Attachments: RAI 505 Batch 2 Draft Response - US EPR DC.pdf

Getachew,

Attached is a draft response for RAI 505, Questions 7.1-34, 7.1-36, 7.1-39, 7.1-40, 7.8-45, and 7.9-71 in advance of the final response date of January 10, 2012 shown below.

Please let me know if the staff has questions or if these responses can be sent as final.

Thanks,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Tuesday, November 22, 2011 2:51 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 3

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. On October 27, 2011, and November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33.

After discussions with NRC staff, the attached file, “RAI 505 Supplement 3 Response US EPR DC.pdf” provides technically correct and complete responses to 4 of the 34 questions. Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the responses to RAI 505 Question 07.07-23, Question 07.08 -46 and Question 07.09.02-72.

The following table indicates the respective pages in the response document, “RAI 505 Supplement 3 Response US EPR DC.pdf,” that contain AREVA NP’s response to the subject questions.

Question #	Start Page	End Page
RAI 505 — 07.01-43	2	3
RAI 505 — 07.07-23	4	4
RAI 505 — 07.08-46	5	5
RAI 505 — 07.09-72	6	7

The schedule for the response to the remaining 30 questions remains unchanged, as indicated below. In addition, the preliminary revised schedule for a response to Question 07.01-33 remains unchanged. The schedule for Question 07.01-33 is being reevaluated and a new supplement with a revised schedule will be transmitted by December 14, 2011.

Question #	Response Date
RAI 505 — 07.01-33	December 14, 2011
RAI 505 — 07.01-34	January 10, 2012
RAI 505 — 07.01-35	January 10, 2012
RAI 505 — 07.01-36	January 10, 2012
RAI 505 — 07.01-37	December 11, 2011
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	January 10, 2012
RAI 505 — 07.01-40	January 10, 2012
RAI 505 — 07.01-41	January 10, 2012
RAI 505 — 07.01-42	January 10, 2012
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	January 10, 2012
RAI 505 — 07.01-46	January 10, 2012
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012
RAI 505 — 07.03-37	December 11, 2011
RAI 505 — 07.03-38	January 10, 2012
RAI 505 — 07.04-15	December 11, 2011
RAI 505 — 07.05-10	December 11, 2011
RAI 505 — 07.05-11	December 11, 2011
RAI 505 — 07.08-43	December 11, 2011
RAI 505 — 07.08-44	January 10, 2012
RAI 505 — 07.08-45	January 10, 2012
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012
RAI 505 — 07.08-49	December 11, 2011
RAI 505 — 07.09-71	January 10, 2012

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, November 17, 2011 5:44 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 2

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. On October 27, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 13 questions and a preliminary revised schedule for Question 07.01-33.

The schedule for the final responses has been revised, as indicated in bold below. In addition, the preliminary revised schedule for a response to Question 07.01-33 has been revised. The schedule for Question 07.01-33 is being reevaluated and a new supplement with a revised schedule will be transmitted by December 14, 2011.

Question #	Response Date
RAI 505 — 07.01-33	**December 14, 2011**
RAI 505 — 07.01-34	**January 10, 2012**
RAI 505 — 07.01-35	**January 10, 2012**
RAI 505 — 07.01-36	**January 10, 2012**
RAI 505 — 07.01-37	**December 11, 2011**
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	**January 10, 2012**
RAI 505 — 07.01-40	**January 10, 2012**
RAI 505 — 07.01-41	**January 10, 2012**
RAI 505 — 07.01-42	**January 10, 2012**
RAI 505 — 07.01-43	**December 11, 2011**
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	January 10, 2012
RAI 505 — 07.01-46	January 10, 2012
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012

RAI 505 — 07.03-37	**December 11, 2011**
RAI 505 — 07.03-38	January 10, 2012
RAI 505 — 07.04-15	**December 11, 2011**
RAI 505 — 07.05-10	**December 11, 2011**
RAI 505 — 07.05-11	**December 11, 2011**
RAI 505 — 07.07-23	**December 11, 2011**
RAI 505 — 07.08-43	**December 11, 2011**
RAI 505 — 07.08-44	**January 10, 2012**
RAI 505 — 07.08-45	**January 10, 2012**
RAI 505 — 07.08-46	**December 11, 2011**
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012
RAI 505 — 07.08-49	**December 11, 2011**
RAI 505 — 07.09-71	**January 10, 2012**
RAI 505 — 07.09-72	**January 10, 2012**

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, October 27, 2011 11:22 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 1

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for a technically correct and complete response to the 34 questions in RAI 505.

The schedule for the final response to Questions 07.01-38, 07.01-44, 07.01-45, 07.01-46, 07.01-47, 07.01-48, 07.01-49, 07.01-50, 07.01-51, 07.03-38, 07.08-43, 07.08-47, 07.08-48 has been revised, as indicated in bold below. In addition, a preliminary revised schedule for a technically correct and complete response to Question 07.01-33 is provided below. The schedule for Question 07.01-33 is being reevaluated and a new supplement with a revised schedule will be transmitted by November 17, 2011.

Question #	**Response Date**
RAI 505 — 07.01-33	**November 17, 2011**
RAI 505 — 07.01-34	December 8, 2011

RAI 505 — 07.01-35	November 17, 2011
RAI 505 — 07.01-36	December 8, 2011
RAI 505 — 07.01-37	December 8, 2011
RAI 505 — 07.01-38	**January 10, 2012**
RAI 505 — 07.01-39	December 8, 2011
RAI 505 — 07.01-40	December 8, 2011
RAI 505 — 07.01-41	November 17, 2011
RAI 505 — 07.01-42	December 20, 2011
RAI 505 — 07.01-43	November 17, 2011
RAI 505 — 07.01-44	**January 10, 2012**
RAI 505 — 07.01-45	**January 10, 2012**
RAI 505 — 07.01-46	**January 10, 2012**
RAI 505 — 07.01-47	**January 10, 2012**
RAI 505 — 07.01-48	**January 10, 2012**
RAI 505 — 07.01-49	**January 10, 2012**
RAI 505 — 07.01-50	**January 10, 2012**
RAI 505 — 07.01-51	**January 10, 2012**
RAI 505 — 07.03-37	November 17, 2011
RAI 505 — 07.03-38	**January 10, 2012**
RAI 505 — 07.04-15	November 17, 2011
RAI 505 — 07.05-10	November 17, 2011
RAI 505 — 07.05-11	November 17, 2011
RAI 505 — 07.07-23	November 17, 2011
RAI 505 — 07.08-43	**January 10, 2012**
RAI 505 — 07.08-44	December 8, 2011
RAI 505 — 07.08-45	December 8, 2011
RAI 505 — 07.08-46	December 8, 2011
RAI 505 — 07.08-47	**January 10, 2012**
RAI 505 — 07.08-48	**January 10, 2012**
RAI 505 — 07.08-49	November 17, 2011
RAI 505 — 07.09-71	December 8, 2011
RAI 505 — 07.09-72	December 8, 2011

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, September 29, 2011 11:04 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)

Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 505 Response US EPR DC.pdf," provides a schedule since a technically correct and complete response to the 34 questions cannot be provided at this time.

The following table indicates the respective pages in the response document, "RAI 505 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 505 — 07.01-33	2	2
RAI 505 — 07.01-34	3	3
RAI 505 — 07.01-35	4	4
RAI 505 — 07.01-36	5	5
RAI 505 — 07.01-37	6	6
RAI 505 — 07.01-38	7	7
RAI 505 — 07.01-39	8	8
RAI 505 — 07.01-40	9	9
RAI 505 — 07.01-41	10	10
RAI 505 — 07.01-42	11	11
RAI 505 — 07.01-43	12	12
RAI 505 — 07.01-44	13	13
RAI 505 — 07.01-45	14	14
RAI 505 — 07.01-46	15	15
RAI 505 — 07.01-47	16	16
RAI 505 — 07.01-48	17	18
RAI 505 — 07.01-49	19	19
RAI 505 — 07.01-50	20	20
RAI 505 — 07.01-51	21	22
RAI 505 — 07.03-37	23	23
RAI 505 — 07.03-38	24	24
RAI 505 — 07.04-15	25	25
RAI 505 — 07.05-10	26	26
RAI 505 — 07.05-11	27	27
RAI 505 — 07.07-23	28	28
RAI 505 — 07.08-43	29	29
RAI 505 — 07.08-44	30	30
RAI 505 — 07.08-45	31	31
RAI 505 — 07.08-46	32	32
RAI 505 — 07.08-47	33	33
RAI 505 — 07.08-48	34	34
RAI 505 — 07.08-49	35	35
RAI 505 — 07.09-71	36	36

RAI 505 — 07.09-72	37	37

A complete answer is not provided for the 34 questions. The schedule for a technically correct and complete response to these questions is provided below.

Please note that the date for the response to Question 07.01-33 is a commitment date to provide a final schedule for the response in a follow-up letter.

Question #	**Response Date**
RAI 505 — 07.01-33	October 27, 2011
RAI 505 — 07.01-34	December 8, 2011
RAI 505 — 07.01-35	November 17, 2011
RAI 505 — 07.01-36	December 8, 2011
RAI 505 — 07.01-37	December 8, 2011
RAI 505 — 07.01-38	December 20, 2011
RAI 505 — 07.01-39	December 8, 2011
RAI 505 — 07.01-40	December 8, 2011
RAI 505 — 07.01-41	November 17, 2011
RAI 505 — 07.01-42	December 20, 2011
RAI 505 — 07.01-43	November 17, 2011
RAI 505 — 07.01-44	December 20, 2011
RAI 505 — 07.01-45	December 20, 2011
RAI 505 — 07.01-46	December 20, 2011
RAI 505 — 07.01-47	December 8, 2011
RAI 505 — 07.01-48	December 20, 2011
RAI 505 — 07.01-49	December 20, 2011
RAI 505 — 07.01-50	December 20, 2011
RAI 505 — 07.01-51	December 20, 2011
RAI 505 — 07.03-37	November 17, 2011
RAI 505 — 07.03-38	December 20, 2011
RAI 505 — 07.04-15	November 17, 2011
RAI 505 — 07.05-10	November 17, 2011
RAI 505 — 07.05-11	November 17, 2011
RAI 505 — 07.07-23	November 17, 2011
RAI 505 — 07.08-43	December 20, 2011
RAI 505 — 07.08-44	December 8, 2011
RAI 505 — 07.08-45	December 8, 2011
RAI 505 — 07.08-46	December 8, 2011
RAI 505 — 07.08-47	December 20, 2011
RAI 505 — 07.08-48	December 20, 2011
RAI 505 — 07.08-49	November 17, 2011
RAI 505 — 07.09-71	December 8, 2011
RAI 505 — 07.09-72	December 8, 2011

Sincerely,

Dennis Williford, P.E.
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
7207 IBM Drive, Mail Code CLT 2B
Charlotte, NC 28262
Phone: 704-805-2223
Email: Dennis.Williford@areva.com

From: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Tuesday, August 30, 2011 1:23 PM
To: ZZ-DL-A-USEPR-DL
Cc: Zhang, Deanna; Morton, Wendell; Spaulding, Deirdre; Mott, Kenneth; Truong, Tung; Zhao, Jack; Mills, Daniel; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 12, 2011, and discussed with your staff on August 22 and 25, 2011. No change is made to the draft RAI as a result of those discussions. 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: 3601

Mail Envelope Properties (2FBE1051AEB2E748A0F98DF9EEE5A5D49B6216)

Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Batch 2
Sent Date: 12/2/2011 3:57:24 PM
Received Date: 12/2/2011 3:58:41 PM
From: WILLIFORD Dennis (AREVA)

Created By: Dennis.Williford@areva.com

Recipients:
"BENNETT Kathy (AREVA)" <Kathy.Bennett@areva.com>
Tracking Status: None
"CRIBB Arnie (EXTERNAL AREVA)" <arnie.cribb.ext@areva.com>
Tracking Status: None
"DELANO Karen (AREVA)" <Karen.Delano@areva.com>
Tracking Status: None
"HATHCOCK Phillip (AREVA)" <Phillip.Hathcock@areva.com>
Tracking Status: None
"ROMINE Judy (AREVA)" <Judy.Romine@areva.com>
Tracking Status: None
"RYAN Tom (AREVA)" <Tom.Ryan@areva.com>
Tracking Status: None
"LENTZ Tony (EXTERNAL AREVA)" <Tony.Lentz.ext@areva.com>
Tracking Status: None
"HUDSON Greg (AREVA)" <Greg.Hudson@areva.com>
Tracking Status: None
"MEACHAM Robert (AREVA)" <Robert.Meacham@areva.com>
Tracking Status: None
"Tesfaye, Getachew" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

Post Office: auscharmx02.adom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	15041	12/2/2011 3:58:41 PM
RAI 505 Batch 2 Draft Response - US EPR DC.pdf	937457	

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

Response to

Request for Additional Information No. 505 (5902,5735,5869,5754,5803,5950,5744), Revision 0

8/30/2011

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.01 - Instrumentation and Controls - Introduction
SRP Section: 07.03 - Engineered Safety Features Systems
SRP Section: 07.04 - Safe Shutdown Systems
SRP Section: 07.05 - Information Systems Important to Safety
SRP Section: 07.07 - Control Systems
SRP Section: 07.08 - Diverse Instrumentation and Control Systems
SRP Section: 07.09 - Data Communication Systems

Application Section: FSAR Chapter 7

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

Question 07.01-34:

OPEN ITEM

The staff requests the applicant to provide additional information on diagnostic tools and testing machines (excluding the Service Unit) utilized in the U.S. EPR. In particular, the staff requests the applicant to provide more details on the "maintenance laptop" and "test machine", as documented in Technical Report ANP-10315P, Revision 1.

Clause 5.6 of IEEE Std. 603-1991 requires, in part, that safety system design be such that credible failures in and consequential actions by other systems of the design basis, shall not prevent the safety systems from meeting the requirements of this standard. Both the maintenance laptop and portable test machine perform functions based on information provided by the applicant in Technical Report ANP-10315P. In Technical Report ANP-10315P, the applicant provides limited information concerning the maintenance laptop. The applicant also provides limited information on the portable test machine. The staff requests the applicant provide information regarding the following clarifying questions:

a. Summarize the types of maintenance activities, equipment issues, etc., that would require a local connection to a function processor by the maintenance laptop or portable test machine.

b. Justify why there is no form of isolation (data, electrical, etc.) between the maintenance laptop and test machines when a local connection is made at the serial port of a given function processor, similar to what has been implemented with the SU.

c. Do the test machines have the same software and access controls placed on them similar to the maintenance laptop, described in Section 2.2.6.1.2 of ANP-10315?

d. Are the test machines utilized in testing that involves bi-directional communications, such as with the SU? If so, is an MSI incorporated?

e. According to Section 2.2.6.1.3 of Technical Report ANP-10315P, the maintenance laptop is prevented from being able to change the operating mode of a function processor. If the a failure of a function processor occurs, such that the processor is no longer running within the runtime environment and the maintenance laptop can only retrieve information in the diagnosis state, then how is an individual function processor returned to normal operation (cyclic processing)? According to the applicant, the SU cannot establish communications with a processor that is not running within the runtime environment.

Response to Question 07.01-34:

a.) The types of maintenance activities that would require a local connection by the maintenance laptop is described in Technical Report ANP-10315P, Section 2.2.6.1.1. This includes initial software loading, install software on new processor boards (after maintenance repair), install system software upgrades, load application software revisions (if Service Unit not available), and retrieve diagnostic failure information. The test machine is only used for periodic testing and is normally not connected to the system. As discussed in ANP-10315P, the test machine is used in the sensor operational test, the no-go test, and the APU and ALU response time test. An

explanation of how the test machine interfaces the system which limits the activities it is involved in will be added to ANP-10315P, Section 2.2.6.1.3.

b.) The test machine has isolation devices between itself and the function processors shown in Technical Report ANP-10315P, Figures 2-2 to 2-5. The maintenance laptop is not normally connected to a function processor. Once the maintenance laptop is connected to a single function processor in one division that function processor is manually rebooted and run in diagnosis state (i.e., function processor is inoperable and provides no outputs or communication to the system). This information will be added to ANP-10315P, Section 2.2.6.1. In conclusion, AREVA does not believe isolation devices for the local connection of the maintenance laptop are necessary.

c.) The test machine has similar software and access controls to the maintenance laptop. The test machine only interfaces to the system under test through hardwired interfaces (24 VDC input and output); therefore, the software controls for modifying changeable parameters, issue service request, etc. are not applicable. Technical Report ANP-10315P, Section 2.2.6.1.3, will be revised to include the software and access controls for the test machine.

d.) The periodic tests that involve the test machine are described in Technical Report ANP-10315P, Sections 2.2.2 to 2.2.5, and Figures 2-2 to 2-5. The test machine only interfaces with the system under test through hardwired interfaces (24 VDC input and output). This information will be added to ANP-10315P, Section 2.2.6.1.3. The test machine has bi-directional data communication with the Service Unit as shown in Technical Report ANP-10315P, Figures 2-2 and 2-3. There is no MSI between the test machine and the Service Unit, but the Service Unit interfaces with the system under test through an MSI.

e.) Once the function processor is in a diagnostic state, and the maintenance laptop is connected and retrieving information, then maintenance is executed to repair the fault on the failed function processor. Once maintenance is finished, the maintenance laptop is disconnected and the function processor is manually reset. The function processor automatically executes an extended self-test during the restart process; and, if there are no errors, then the function processor automatically enters cyclic operation. This information will be added to ANP-10315P, Section 2.2.6.1.

FSAR Impact:

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

Technical Report Impact:

Technical Report ANP-10315P, Section 2.2.6.1, will be revised as described in the response and indicated on the enclosed markup.

Question 07.01-36:

OPEN ITEM

Clarify the new voting scheme for Safety Automation System (SAS) voting logic and how the voting logic is modified in the presence of a single failure.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. As part of an alternative request, the applicant proposes to use IEEE Std. 603-1998. Clause 5.1 of IEEE Std. 603-1998 require, in part, that safety systems perform all safety functions in the presence of any single detectable failure, all failures caused by a single failure, and all failures or spurious actuations caused by a design basis event.

Upon receiving a start signal from the PS, SAS provides closed-loop controls for specified engineered safety features (ESF) systems to allow the plant reach and maintain safe shutdown conditions. Initially, the design of SAS incorporated a 2nd min / 2nd max selection scheme as part of its divisional logic scheme, which can be seen in U.S. EPR FSAR, Tier 2, Section 7.3, Revision 2. In response to RAI 442, Question 07.03-32, the applicant provided Interim Revision 3 mark-ups of Tier 2, Section 7.3. As shown in Tier 2, Figure 7.3-12, Interim Revision 3 mark-ups, a single sensor voting scheme has replaced the 2nd min / 2nd max function. Given this change to a more conventional voting scheme, the applicant did not provide any design information on the new voting scheme in the FSAR. The applicant also did not provide any information on how SAS voting logic is modified in the presence of a single failure, similar to information provided for the PS in Technical Report ANP-10309P. This information is critical to the staff's evaluation of SAS compliance with IEEE Std. 603-1998, Clause 5.1. The staff requests the applicant provide information in the FSAR concerning the new SAS voting scheme and to also provide information on how SAS voting logic is modified in the presence of single failures, faulty signals and messages, etc.

Response to Question 07.01-36:

An FMEA for SAS, that demonstrates SAS failure modes, will be incorporated into U.S. EPR FSAR Tier 2, Section 7.1, as Table 7.1-7, SAS FMEA Results.

U.S. EPR FSAR, Section 7.4.1.1, states the following: “Engineered safety features (ESF) are used to achieve and maintain safe shutdown. The actuation of the ESF is performed by the protection system (PS). The I&C that perform ESF actuation are described in Section 7.3. The safety automation system (SAS) automatically controls the safety-related systems once those systems are actuated by the PS.”

FSAR Section 7.3.1.1, states the following: “Automatic actuation of ESF systems and auxiliary supporting systems is performed by the protection system (PS) when selected plant parameters reach the appropriate setpoints. The safety automation system (SAS) performs closed loop automatic controls of certain ESF systems following their actuation by the PS.”

In order to bound the possible failures, both detected and undetected failures of sensors and digital equipment are analyzed and the worst-case effect of each failure is identified. Detected failures are defined as those automatically detected by the inherent and engineered monitoring mechanisms of the system. Two types of undetected failures are analyzed. A failure denoted “undetected–spurious” is defined as a failure not automatically detected which results in an

actuation. A failure denoted “undetected–blocking” is defined as a failure not automatically detected which results in failure to issue an actuation when needed.

Failures in the hardwired output logic are generally not detected automatically by the SAS. Therefore, only undetected single failures of these devices are considered. A failure of the output logic can result in a spurious actuation (“undetected–spurious”), or failure to actuate when needed (“undetected–blocking”).

Network failures within the SAS allow the receiver of data to be affected in one of three ways. First, the network failure can result in an invalid message being received. By definition, invalid messages are always detected failures, and are analyzed as single failures. Second, a network failure can result in a message received as valid that contains spurious information. This type of failure is bounded by the “undetected–spurious” failure of the sending equipment, and is therefore not considered. Third, a network failure can result in a message received as valid that fails to request an action when one is needed. This type of failure is bounded by the “undetected–blocking” failure of the sending equipment; and is, therefore, not considered.

The architecture of the SAS allows Control Units (CU) to be analyzed for single failure without regard to which specific CU in the division is the failure point. For these single failures, all functions of the system are considered affected, as every function is processed by at least one CU in a division. Considering the effect on every function of the system bounds all cases of specific CU single failures.

When referring to the nature of a single failure, the terms “detected” and “undetected” as used in the context of the SAS FMEA do not correspond to the definition of a detectable failure in IEEE 603-1998. All of the failures denoted “undetected” in the U.S. EPR FSAR Table 7.1-7 are detectable through periodic testing. The terms “detected” and “undetected”, as used in U.S. EPR FSAR Table 7.1-7, refer to the ability of the SAS to automatically detect a failure through self surveillance. As defined by IEEE 603-1998, the SAS has only detectable failures and no identifiable, but non-detectable failures.

U.S. EPR FSAR, Figure 7.1-7, provides the Safety Automation System architecture. Each division of the SAS implements redundant CU pairs that operate in a master/standby configuration as described in Table 7.1-7. One CU of the pair, the master, controls the process. The other CU of the pair, the standby, immediately takes over the control and interlock functions if a fault occurs.

The outputs of each pair of CUs are combined in a Functional OR gate by hardwiring, but only the master CU output signals are enabled while the output signals of the standby CU are disabled. Disabled output signals are electrically set to 0 V or 0 mA as shown in Figure 7.1-7.

Table 7.1-7 describes that in the event of interrupted master CU operation, the standby CU automatically switches over to become the master CU. In order to ensure a seamless switch over without loss of data, the standby CU is continuously synchronized with the master CU. As shown in Revision 3 to U.S. EPR Tier 2, Figures 7.3-4 and 7.3-12, a sensor/setpoint comparison scheme vs. a single sensor voting scheme replaced the 2nd min / 2nd max function. Table 7.1-7 also provides a description of the SAS sensor/setpoint comparison scheme, with modifications for single failures.

Hardware faults within the redundant parts of the SAS CUs, as listed in the table below, are automatically detected. A detected fault leads to an automatic switch over: the redundant standby CUs become the new SAS master CUs and enable their output modules. The previous master CU disables its output modules as a consequence of the fault.

Master/Standby Assignments in the Event of Faults

SAS Control Unit Fault	SAS Control Unit Assignment
Division X, a fault occurs in CU A of that divisional pair	All Divisions, the master CU becomes CU B
Division X, a fault occurs in CU B of that divisional pair	All Divisions, the master CU becomes CU A
Division X, a fault occurs in both CUs of that divisional pair	All Divisions, the master CU becomes CU A
Division X, a fault occurs in CU A of that divisional pair, and in Division Y, a fault occurs in CU B of that divisional pair	Division X, the master becomes CU B, for all other Divisions, the master becomes CU A

Note: Division X denotes any division. Division Y denotes any division that is not Division X.

Example: If CU A in Division 1 fails and CU B in Division 3 fails, then CU B in Division 1 becomes the master CU and, for all other divisions, CU A becomes the master.

FSAR Tier 2, Section 7.1.1.4.2, will be updated to include a description of the concept of invalid signal identification and voting modification in case of a faulty signal as shown in the attached markup.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.1.1.4.2, will be revised to include a new Table 7.1-7, SAS FMEA Results.

Question 07.01-39:

OPEN ITEM

Discuss how the self-test features in the U.S. EPR design are fully tested and verified on a periodic basis. This RAI question is part of a series of follow-up questions to RAI 285, Question 07.03-21.

IEEE Std. 603-1998, Clause 5.7 requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Appendices 7.1-C and 7.1-D provide guidance on meeting the requirements of Clause 5.7. SRP-BTP 7-17 was also used as guidance. In its response to RAI 285, Question 07.03-21, the applicant provided Technical Report ANP-10315, which provides the overall surveillance and self-testing philosophy for the U.S. EPR design. The technical report was provided in order to provide the staff information regarding the design implementation of the self-testing features. In Section 3.6 of Technical Report ANP-10315, the applicant provided four technical points intended to address guidance provided in BTP 7-17, which states, in part, that automatic self-diagnostic features should be verified during periodic tests.

The staff's review yielded the following points:

- Overall, the four points do not appear to adequately verify the full design functionality of the self-testing features as enumerated in Section 2.2.6 of Technical Report ANP-10315.
- The applicant did not link the four points, or any other verification method, to the overall surveillance philosophy provided in Technical Report ANP-10315. Technical Report ANP-10315 provides methods for how tests such as response time tests are performed, as illustrated in Figure 2-4. The staff did not find specific information on how self-test verification would be performed as part of a surveillance test.
- If there is a failure of self-tests, whether system-wide, or isolated to an individual function processor, there is no mention of how operability is affected.

In particular, the staff's concern lies with hardware portions of the self-test features that may degrade and fail. To these points, the staff requests the applicant to provide the following:

a. Address verification of self-test features during the life of the system; particularly hardware self-test components that can degrade over time (e.g., hardware watchdog timer and other such hardware components).

b. For the method of self-test verification determined by the applicant, describe how the verification is performed during surveillance testing of all the applicable TXS safety systems.

c. How does the applicant address operability for a processor that has a failed self-test feature?

Response to Question 07.01-39:

Item a.

Direct verification of the proper operation of the self-test functionality is not performed on the function processors, because this would require the non-prudent injection of faults into the safety system. But, reasonable assurance of self-test operation is provided via other means as described in the four points in ANP-10315P, Section 3.6:

1. The function processors and communication paths are exercised as part of the periodic surveillance testing as described in ANP-10315P, Section 2.2.1 through 2.2.5. These tests verify that faults resulting in the inability of the equipment to perform its safety function would be detected. These faults should be detected by the self-tests. If during the periodic testing, it is found that a fault was detected but not flagged with an error by the self-test feature, then incorrect operation of the self-test features is also detected. This is described in ANP-10315P, Section 3.6.
2. Self-test qualification and configuration control: The TXS system software, including the software used in the self-test, is developed and tested within the quality program described in EMF-2110(NP)(A). This verifies that the self-test features function properly, see ANP-10315P, Section 3.6, Page 3-10, for details.
3. The integrity of the program memory containing the system software (including the self-test features) is verified by self-test of the function processor module, see ANP-10315P, Section 3.6, Page 3-8 and Section 2.2.6.1, for details.
4. Periodic extended self-test (extended self-test surveillance requirement in U.S. EPR FSAR Tier 2, Chapter 16, Section 3.3.1) checks the memory containing the cyclic self-test software and the CRC check to verify the proper self-test routines are loaded, see ANP-10315P, Section 3.6, Pages 3-10 and 3-11, and Section 2.2.6.1 for details.
5. The hardware watchdog timer and the runtime environment are used to continuously monitor the correct operation of the self-test. The watchdog timer is described in ANP-10315P, Section 2.2.6.2. The Runtime Environment (RTE) is responsible for initiating an alarm when a complete set of self-tests are not completed within one hour of the previous set. The RTE is described in ANP-10315P, Section 2.2.6.4.
   a. The watchdog timer is tested by the cyclic self-test. A trip of the watchdog timer is triggered and verified on the associated interrupt signal. The watchdog-interrupt is blocked for the duration of this test. (ANP-10315P, Table 2-1). ANP-10315P, Section 2.2.6.2, "Hardware Watchdog (Inherent)," will be revised to clarify the software test performed on the watchdog timer.
   b. A function processor module fault that would normally be recognized by the faulted watchdog timer would be recognized and alarmed by its I/O modules and communication partners through communication monitoring as described in ANP-10315P, Section 2.2.6.5.

Item b.

The self-test features are verified though the design process of the self-test, during cyclic self-test, and extended self-test (extended self-test surveillance requirement in U.S. EPR FSAR Tier

2, Chapter 16, Section 3.3.1 performed every 24 months) and during startup self-test on reset or return of power, see ANP-10315P, Section 3.9, Page 3-24, for details.

Item c.

Upon receiving an alarm that is the result of a failed self-test, the Service Unit will be used to inspect the cause of the alarm and to record information about the failure. If necessary, the module will be reset. After reset, the module will perform the startup self-test (which includes all cyclic self-test) and will not connect to the system unless this test is passed. If this does not fix the module, it will be considered inoperable and will be replaced. A discussion about actions for failed self-test will be added to ANP-10315P, Section 2.2.6.1.

FSAR Impact:

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

Technical Report Impact:

Technical Report ANP-10315P, Sections 2.2.6.1 and 2.2.6.2, will be revised as described in the response and indicated on the enclosed markups.

Question 07.01-40:

OPEN ITEM

Provide information on what operator actions are taken on a failure of the self-tests to perform a full system scan within one hour. Also, provide more information on the acceptability of allowing a function processor or division or TXS safety system to continue to operate normally, with a failed self-test run. This RAI question is part of a series of follow-up questions to RAI 285 Question 07.03-21.

IEEE Std. 603-1998, Clause 5.7 requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Appendices 7.1-C and 7.1-D provide guidance on meeting the requirements of Clause 5.7. SRP-BTP 7-17 was also used as guidance. In terms of a failure of the self-testing features, Section 2.2.6.1 of Technical Report ANP-10315, states that,

> "*If the continuous self-test is not complete after one hour, the runtime environment issues an error message to the SU. This error message is also transferred to the application software for inclusion in engineered alarms to the operator.*"

Section 2.2.6.6 of Technical Report ANP-10315 states,

> *"The runtime environment monitors the operation of the cyclic self-test. If the cyclic self-test does not complete one self-test cycle within one hour, the runtime environment issues an error message. This does not disrupt runtime environment operation. In particular, the processing of the application software functions is not affected."*

The applicant is crediting the self-test features of the U.S. EPR design to meet the requirements of Clause 5.7. The staff did not identify why the failure of a self test did not yield a more significant operator response. As Section 2.2.6.6 is currently written, a TXS function processor, and potentially, a TXS safety system, could continue running indefinitely without any continuous self-tests being performed because no interruption of operations occurs. Failure of the continuous monitoring self-tests indicates a potentially more significant issue with the system if it was originally designed to perform the tests on a regular periodicity. The staff requests the applicant address the following concerns:

a. If a self-test failure to run fully within one hour occurs, what is the operability state of the function processor or system?
b. How long does the applicant believe the function processor or TXS system can be credited to safely run without cyclic self-testing being active?
c. What operator actions would be required if a self-testing failure is alarmed in the main control room?

Response to Question 07.01-40:

Item a.

A failure to complete self-test in an hour could be an indication of a potential problem in a module. If this alarm is received the affected module is declared inoperable until such time as it passes extended self-test as a result of a module reset (see Item c).

Item b.

For a module to be operable, it must be capable of passing all self-tests and they must be active. Operability of equipment with regard to self-test is discussed in ANP-10315P, Section 3.6. If a module fails to complete its self-test in an hour, it is declared inoperable. Technical Specifications (U.S. EPR FSAR, Tier 2, Chapter 16) describes the operation requirements for inoperable equipment.

Item c.

Upon receiving a self-test-related alarm in the main control room (MCR), the Service Unit will be connected to the faulted function processor to investigate the cause for the alarm. After the required information is collected from the message buffer, the function processor will be reset. The reset will initiate the extended self-test. This test includes the test of the cyclic self-test and must be passed for the function processor to begin communication with the system. If extended self-test are not passed, the module should be replaced.

A description of actions to be taken for a self-test alarm and module operability was added to ANP-10315P as a response to RAI 505, Question 07.01-39.

FSAR Impact:

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

Question 07.08-45:

OPEN ITEM

The staff requests the applicant to provide clear and unambiguous design descriptions for the claimed PS subsystem diversity descriptions for all applicable design documents.

10CFR52.47(a)(2) requires that a description and analysis of the structures, systems, and components (SSCs) of the facility shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. The staff reviewed the U.S. EPR design documents for PS subsystem diversity design. Technical Report ANP-10309, Revision 3, states in Section 1.0, last paragraph, that:

> *"The PS provides signal diversity, as described in Section 10.0, "Signal Diversity." The signal diversity design rules presented in Section 10 represent elements of diversity described in NUREG/CR-6303 (Reference 3). AREVA NP* **takes credit** *[emphasis added] for the signal diversity within the PS, as described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report, ANP-10304."*

However, Section 10.1 of Technical Report ANP-10309 states:

> *"Signal diversity, as applied to the PS, is the use of two diverse parameters to initiate RT to mitigate the effects of the same AOO or PA. This signal diversity* **is not credited** *[emphasis added] in the diversity and defense-in-depth plant response analysis to mitigate any AOO or PA."*

Furthermore, Section 4.2.4 of Technical Report ANP-10304 states:

> *"Each PS division is divided into two independent subsystems (i.e., A and B). Subsystem A in each division is redundant to Subsystem A of other divisions; the same is true of Subsystem B. The primary purpose of this arrangement* **is to provide** *[emphasis added] signal diversity for RT functions."*

In addition, it is not always stated within the design descriptions that the credited signal diversity is only applicable for RT functions. As stated in Section 2.2 of Technical Report ANP-10304:

> *"Each division of the PS contains two independent subsystems to support signal diversity."*

The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. The staff request the applicant to provide clear, consistent, and unambiguous design descriptions about the functions that PS subsystem diversity is credited for and specify when the PS subsystem design diversity is credited for all applicable design documents.

Response to Question 07.08-45:

The diversity and defense-in-depth analysis, as described in ANP-10304, "U.S. EPR Diversity and Defense-in-Depth Assessment," assumes that there is a complete failure of the PS. Therefore, signal diversity for RT functions implemented in the subsystems of the PS is not

credited to mitigate any events in the D3 plant response analysis. However, the signal diversity within the PS provides an added layer of protection in the overall U.S. EPR plant defense-in-depth strategy.

Section 1.0 in Technical Report ANP-10309P, and Technical Report ANP-10304, Section 2.2, will be revised as shown in the attached markups to provide clarification and consistent interpretation.

FSAR Impact:

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

Technical Report Impact:

Technical Report ANP-10309P, Section 1.0, will be revised as described in the response and indicated on the enclosed markup.

Technical Report ANP-10304, Section 2.2, will be revised as described in the response and indicated on the enclosed markup.

Question 07.09-71:

OPEN ITEM

Explain how invalid signals are identified by safety automation system (SAS) processors and state whether the voting logic in the SAS is modified to accommodate the identified invalid signals to meet the requirements of IEEE Std. 603-1998, Clause 5.6.1.

IEEE Std. 603-1998, Clause 5.6.1, requires redundant portions of the safety system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. The staff issued Digital Instrumentation and Controls Interim Staff Guidance 4 (D I&C ISG-04) to provide criteria for implementing interdivisional data communications. Criterion 2 in Section 1 of D I&C ISG-04 states that "The safety channel should be protected from adverse influence from outside the division of which that channel is a member…" In addition, Criterion 12 in Section 1 of D I&C ISG-04 states that, "Communication faults should not adversely affect the performance of required functions in any way…" The staff evaluated the SAS interdivisional communication functions and determined that the SAS has not adequately addressed Criteria 2 and 12. Specifically, the staff finds that the applicant has not provided sufficient detail regarding provisions in the design that prevents SAS divisions from being adversely impacted by information originating from outside the division. As such, the staff requests the applicant explain how invalid signals are identified by SAS processors and state whether the voting logic in the SAS is modified to accommodate the identified invalid signals. Incorporate this description into the U.S. EPR FSAR, Tier 2, or in documents incorporated by reference.

Response to Question 07.09-71:

The safety automation system (SAS) meets the requirements of IEEE Std. 603-1998, Clause 5.6.1, which requires redundant portions of the SAS to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function.

Divisional SAS functions are performed in the redundant computer subsystems (master and standby). Identification of redundancies within a division is indicated by uppercase letters (A, B). Therefore, master subsystems in each division are identified by A1 to Ax and standby subsystems are identified as B1 to Bx, where x is the number of control units (CU) in each division.

Each SAS division operates in a redundant master/standby configuration. In one CU pair, the master controls the process. The other CU, the standby unit, immediately takes over the control functions if a fault occurs. The faulty CU can then be repaired without interrupting the process.

The SAS system is distributed over the four spatially separated divisions. In each division a two-fold redundant SAS CUs performs the tasks assigned to it. The outputs of the two SAS CUs are OR-gated by hard wiring, but only the master system outputs signals. The two redundant SAS CUs of one division perform their functions according to the following principle:

All input signals of a division are acquired redundantly in both SAS CUs, which calculate the same output signals. Hardwired output signals of both CUs are electrically combined before

transferring the signals to the electrical receivers. One CU, the current master subsystem, enables its hardwired output signals. The other CU, the current standby subsystem, disables its hardwired output signals. Disabled output signals are electrically set to zero V or zero mA (switching off the power supply of corresponding output modules).

In case of interrupted operation of the master CUs within a division, or within the functional networks, the redundant standby CU becomes the master subsystem. A switchover to the other CU can be triggered manually by the means of the Service Unit, or automatically by fault detection. In order to ensure a seamless switchover without loss of data, the standby subsystem is permanently synchronizing all relevant memories with the master. This is performed via the functional network connecting master and standby subsystems in each division.

Hardware faults within the redundant parts of the SAS CUs, listed in the table shown in the response to RAI 07.01-36, are automatically detected. The detection of a fault leads to an automatic switchover of the master role to the CUs of the other redundancy (standby) in all divisions. The previous standby subsystem enables its output modules, thus becoming the new master. The previous master disables its output modules as a consequence of the fault.

Faults in the CUs are detected by diverse means, including a hardware watchdog that monitors the disruption of cyclical processing. Notification of failure by the watchdog initiates automatic disabling of all output signals. In addition, the following non fatal faults initiate an automatic switch over:

- Fault detection of I/O modules.
- Fault of the functional network of the same redundancy.

In case of faults in both of the CUs (double failure) in one division; CU A, by default, becomes the master. This could mean the loss of a division in some cases. On the other hand, if faults are detected in CU B in Division 3 and in CU A in Division 2, CU A becomes master in all divisions, except in Division 2, where CU B becomes master.

The SAS meets the requirements of the Digital Instrumentation and Controls Interim Staff Guidance 4, which states that signal faults should not adversely affect the performance of required safety function in any way. In case of failure of sensors, sensor maintenance, or communication failure between SAS functional units detected by the SAS; the 2 out of 4 voting logic in the CU layer is automatically modified for data signals. This allows the CU to disregard the faulty signal while retaining the ability to actuate on the basis of the remaining non-faulty signals. This automatic voting modification is accomplished using the status of the signals that are inputs to the voting function block.

The data signals within the SAS carry a value and a status. The signal status can be propagated through the software function blocks; therefore, if an input signal to a function block has a faulty status, the output of the function block also has a faulty status. When a signal with a faulty status reaches the voting function block, the signal is disregarded through modification of the vote. This results in the output of the voting function block having a non-faulty status. A signal typically obtains a faulty status through the following mechanisms:

- During sensor maintenance, or when a sensor is suspected to be faulty, the sensor can be placed in maintenance bypass. This lockout attaches a faulty status to the sensor's signal.

The lockout is a software function performed in the CU layer before any processing is performed using the signal.

- If the SAS detects a faulty sensor through range monitoring, or by monitoring the status of the signal conditioning hardware, the corresponding signal is marked with a faulty status. This monitoring is also performed in the CU layer.
- In case of a communication failure between SAS functional units, the receiving functional unit detects errors such as incorrect message length, format, or age.

This detection occurs when the functional unit retrieves the message from the associated communication module before the individual signals are extracted from the message. If a communication failure is detected, a faulty status is attached to the signals in the message before they are used in function block processing.

Single failures upstream of the CU layer, that could result in an invalid signal being used in the SAS actuation, are accommodated by modifying the vote in the CU layer.

Each SAS actuation function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation., In cases where inappropriate actuation of an SAS function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The concept of modification toward no actuation, based on the number of input signals to the voting function block that carry a faulty status, is as follows:

- 0 faulty input signals: Vote is 2/4.
- 1 faulty input signal: Vote is 2/3.
- 2 faulty input signals: Vote is 2/2.
- 3 faulty input signals: No actuation.
- 4 faulty input signals: No actuation.

Hardwired signals which fail within range are detected during periodic testing of the CUs. Hardwired signals with fail out of range are automatically disregarded.

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

In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

Refer to Chapter 8 for more information on the electrical power systems.

7.1.1.4.2 Safety Automation System

The SAS is a Class 1E control system. The SAS performs automatic and manual grouped control functions to perform safety-related controls during normal operations, mitigate the effects of AOOs and PAs, and to achieve and maintain safe shutdown.

Classification

The SAS is classified as safety-related.

Functions

~~Table 7.1-3~~Table 7.1-5 shows the functions of the SAS.

Interfaces

Table 7.1-4 shows the interfaces of the SAS.

Architecture

RAI 505, Q. 07.01-36

Figure 7.1-7—Safety Automation System Architecture provides a functional representation of the SAS.

A system-level failure modes and effects analysis (FMEA) is performed on the SAS to identify potential single point failures and their consequences. The architecture of the SAS is redundant by the means of the use of redundant CUs and divisional redundancy. The system is designed so that a single failure during corrective or periodic maintenance, or a single failure and the effects of an internal hazard does not prevent performance of the safety functions. Table 7.1-7 provides the FMEA for the SAS.

Each division of the SAS implements redundant CU pairs that operate in a master/standby configuration as described in Table 7.1-7. One CU of the pair, the master, controls the process. The other CU of the pair, the standby, immediately takes over the control and interlock functions if a fault occurs.

In case of interrupted operation of the master CU within a division, or within the functional networks, the redundant standby CU becomes the master CU. A switchover from the master CU to the standby CU can be triggered manually by the means of the service unit, or automatically by fault detection. In order to ensure a

RAI 505, Q. 07.01-36

seamless switchover without loss of data, the standby CU is permanently synchronizing all relevant memories with the master CU. This is performed via the functional network connecting master and standby CUs in each division.

Hardware faults within the redundant parts of the SAS CUs, listed in the Table 7.1-7 are automatically detected. The detection of a fault leads to an automatic switchover of the master role to the redundant CUs (standby) in all other divisions. The previous standby CUs enable their output modules, thus becoming the new master. The previous master CUs disable their output modules as a consequence of the fault.

The outputs of each pair of CUs are combined in a Functional OR gate by hardwiring, but only the master CU output signals are enabled while the output signals of the standby CU are disabled. Disabled output signals are electrically set to 0 V or 0 mA as shown in Figure 7.1-7.

Table 7.1-7 provides a description of the SAS sensor/setpoint comparison scheme, with modifications for single failures.

The SAS is organized into four independent divisions located in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.

The SAS consists of these functional units:

- Control Units (CU).
- MSIs.
- GWs.
- SU.

The CUs execute the logic for the assigned automatic and manual grouped control functions. There are redundant pairs of CUs within a division. The number of redundant pairs of CUs is dependent on sizing requirements for the SAS. Redundant pairs of CUs that perform functions requiring interdivisional communication identified in Table 7.1-5 have data communications between CUs in different divisions. For those redundant pairs of CUs that do not have any functions allocated that require interdivisional communication, there are no data connections between redundant pairs CUs in different divisions. The CUs acquire hardwired inputs from the signal conditioning and distribution system (SCDS), the PS, or the SICS via hardwired connections. Hardwired outputs from the CUs are sent to the PACS for

- GW-PICS - bi-directional, point-to-point data communications. Signals are only engineered to be sent from the SAS to the PICS. Signals coming from the PICS to the SAS GW are to request messages to be sent.

RAI 505, Q. 07.01-36

Fault Detection

Signal Faults in the SAS are detected via diverse means dependent on the signal type.

Hardwired signals, which fail within range, are detected during the periodic testing of the CU. Hardwired signals which fail out of range are automatically disregarded.

Data signals within the SAS carry a value and a status. The signal status can be propagated through the software function block; therefore, if an input signal to a function block has a faulty status, the output of the function block also has a faulty status. When a signal with a faulty status reaches the voting function block, the signal is disregarded through modification of the vote. This results in the output of the voting function block having a non-faulty status. A signal typically obtains a faulty status through the following mechanisms:

- During sensor maintenance, or when a sensor is suspected to be faulty, the sensor can be placed in maintenance bypass. This lockout attaches a faulty status to the sensor's signal. The lockout is a software function performed in the CU layer before any processing is performed using the signal.
- If the SAS detects a faulty sensor through range monitoring, or by monitoring the status of the signal conditioning hardware, the corresponding signal is marked with a faulty status. This monitoring is also performed in the CU layer.
- In case of a communication failure between SAS functional units, the receiving functional unit detects errors such as incorrect message length, format, or age. This detection occurs when the functional unit retrieves the message from the associated communication module before the individual signals are extracted from the message. If a communication failure is detected, a faulty status is attached to the signals in the message before they are used in function block processing.

Single failures upstream of the CU layer that could result in an invalid signal being used in the SAS actuation are accommodated by modifying the vote in the CU layer. Each SAS actuation function is evaluated on a case-by-case basis to determine whether the vote is modified toward actuation or no actuation. In cases where inappropriate actuation of an SAS function could challenge plant safety, the function is modified toward no actuation. Otherwise, the function is modified toward actuation. The concept of modification toward no actuation based on the number of input signals to the voting function block that carry a faulty status is as follows:

0 faulty input signals: Vote is 2/4.

1 faulty input signal: Vote is 2/3.

RAI 505, Q. 07.01-36

2 faulty input signals: Vote is 2/2.

3 faulty input signals: No actuation.

4 faulty input signals: No actuation.

Power Supply

The SAS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of a LOOP. In the event of an SBO, the EUPS has the capability of receiving power from the SBODGs.

Refer to Chapter 8 for more information on the electrical power systems.

7.1.1.4.3 Priority and Actuator Control System

The PACS is a safety-related system that performs prioritization of signals from different I&C systems, drive actuation, and monitoring plant actuators.

Classification

The PACS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the PACS.

Interfaces

Table 7.1-4 shows the interfaces of the PACS.

Architecture

Figure 7.1-8—Priority and Actuator Control System Architecture provides a functional representation of the PACS.

The PACS is organized into four independent divisions located in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Buildings.

In each division, there are safety-related and non-safety-related PACS equipment to interface with safety-related and non-safety-related actuators, respectively. The

Table 7.1-7—SAS FMEA Results
Sheet 1 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
1	In-Containment Refueling Water Storage Tank System	IRWSTS Boundary Isolation for Preserving IRWST Water Inventory	IRWST Water Level	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Four redundant channels and 2/4 voting	Voting logic modified to 2/3	No effects on the system function
				b) Undetected - Spurious	None	2/4 voting	Voting logic becomes 1/3	
				c) Undetected - Blocking	None	Four redundant channels and 2/4 voting	Voting logic becomes 2/3	
2	Main Steam System	Steam Generator 1-4 Main Steam Relief Valve Regulation during Pressure Control	MSRIV Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; Four redundant channels	Voting logic modified to 2/3	No effects on the system function
				b) Undetected - Spurious	None	2/4 voting	Voting logic becomes 1/3	
				c) Undetected - Blocking	None	Four redundant channels and 2/4 voting	Voting logic becomes 2/3	
3	Main Steam System	Steam Generator 1-4 Main Steam Relief Valve Regulation during Pressure Control	SG Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Loss of pressure signal to the automatic MSRCV positioning logic	Loss of automatic MSRCV position control of the affected steam generator. Main Steam relief train integrity maintained by redundant Main Steam Safety Valves.
				b) Undetected - Spurious	None	Redundant main steam relief train.	MSRCV position out of alignment with plant conditions.	
				c) Undetected - Blocking	None	Redundant main steam relief train.	MSRCV position out of alignment with plant conditions.	
4	Main Steam System	Steam Generator 1-4 Main Steam Relief Valve Regulation during Position Control	MSRCV Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid	Loss of MSRCV position signal to the automatic MSRCV positioning logic for standby position control.	Loss of MSRCV position signal to the automatic MSRCV positioning logic for standby position control. Main Steam relief train integrity maintained by redundant Main Steam Safety Valves.
				b) Undetected - Spurious	None	Redundant main steam relief train.	Loss of MSRCV position signal to the automatic MSRCV positioning logic for standby position control.	
				c) Undetected - Blocking	None	Redundant main steam relief train.	Loss of MSRCV position signal to the automatic MSRCV positioning logic for standby position control.	

Table 7.1-7—SAS FMEA Results
Sheet 2 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
5	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Chiller Evaporator Outlet Temperature	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs.	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
6	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Chiller Compressor Oil Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs.	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function	
7	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Condenser Refrigerant Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs.	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 3 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
8	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs.	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
9	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs.	Unable to automatically start Train 2 circulating pump 1. Unable to automatically switchover from Train 1 to Train 2	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant trains pairs.	Unable to automatically start Train 2 circulating pump 1. Unable to automatically switchover from Train 1 to Train 2	
				c) Undetected - Blocking	None	Two redundant trains pairs.	Unable to automatically start Train 2 circulating pump 1. Unable to automatically switchover from Train 1 to Train 2	

Table 7.1-7—SAS FMEA Results
Sheet 4 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
10	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs.	Unable to automatically start Train 2 circulating pump 1. Unable to automatically switchover from Train 1 to Train 2	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant trains pairs.	Unable to automatically start Train 2 circulating pump 1. Unable to automatically switchover from Train 1 to Train 2	
				c) Undetected - Blocking	None	Two redundant trains pairs.	Unable to automatically start Train 2 circulating pump 1. Unable to automatically switchover from Train 1 to Train 2	
11	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Circulating Pump 1 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to start Train 2 circulating pump 2. Unable to automatically switchover from Train 1 to Train 2	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 2 circulating pump 2. Unable to automatically switchover from Train 1 to Train 2	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 2 circulating pump 2. Unable to automatically switchover from Train 1 to Train 2	
12	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Circulating Pump 2 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to position bypass valve for Train 2	In cross-tie operation two pumps in the operating train of each divisional pair provides flow to two user divisions. A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position bypass valve for Train 2	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position bypass valve for Train 2	

Table 7.1-7—SAS FMEA Results
Sheet 5 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
13	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Evaporator ΔP	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to position bypass valve for Train 2	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position bypass valve for Train 2	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position bypass valve for Train 2	
14	Safety Chilled Water System	Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow/Blackbox Fault/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to start Train 2 chiller	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 2 chiller	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 2 chiller	
15	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Condenser Flow Rate	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 6 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
16	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Chiller Evaporator Outlet Temperature	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
17	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Chiller Compressor Oil Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
18	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Condenser Refrigerant Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 7 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
19	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
20	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 2 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to automatically start Train 1 circulating pump 1. Unable to automatically switchover from Train 2 to Train 1.	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to automatically start Train 1 circulating pump 1. Unable to automatically switchover from Train 2 to Train 1.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to automatically start Train 1 circulating pump 1 Unable to automatically switchover from Train 2 to Train 1.	

Table 7.1-7—SAS FMEA Results
Sheet 8 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
21	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to automatically start Train 1 circulating pump 1. Unable to automatically switchover from Train 2 to Train 1.	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to automatically start Train 1 circulating pump 1. Unable to automatically switchover from Train 2 to Train 1.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to automatically start Train 1 circulating pump 1. Unable to automatically switchover from Train 2 to Train 1.	
22	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to start Train 1 chiller.	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 1 chiller.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 1 chiller.	
23	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Evaporator ΔP	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to position bypass valve for Train 1.	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position bypass valve for Train 1.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position bypass valve for Train 1.	

Table 7.1-7—SAS FMEA Results
Sheet 9 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
24	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Circulating Pump 1 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to start Train 1 circulating pump 2. Unable to automatically switchover from Train 2 to Train 1.	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 1 circulating pump 2. Unable to automatically switchover from Train 2 to Train 1.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 1 circulating pump 2. Unable to automatically switchover from Train 2 to Train 1.	
25	Safety Chilled Water System	Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow/Blackbox Fault/Loss of UHS-CCWS/ SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 1 Circulating Pump 2 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to position bypass valve for Train 1.	A second cross-tie pair Train 3 and Train 4 serves its associated heat exchangers. Adequate cooling is provided by Train 3 and Train 4.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position bypass valve for Train 1.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position bypass valve for Train 1.	
26	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Condenser Flow Rate	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No affect on the system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 10 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
27	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Chiller Evaporator Outlet Temperature	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
28	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Chiller Compressor Oil Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
29	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Condenser Refrigerant Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 11 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
30	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of Ultimate Heat Sink/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function.	No effects on the system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic.	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	
31	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to automatically start Train 4 circulating pump 1. Unable to automatically switchover from Train 3 to Train 4.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to automatically start Train 4 circulating pump 1. Unable to automatically switchover from Train 3 to Train 4.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to automatically start Train 4 circulating pump 1. Unable to automatically switchover from Train 3 to Train 4.	

Table 7.1-7—SAS FMEA Results
Sheet 12 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
32	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to automatically start Train 4 circulating pump 1. Unable to automatically switchover from Train 3 to Train 4.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to automatically start Train 4 circulating pump 1. Unable to automatically switchover from Train 3 to Train 4.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to automatically start Train 4 circulating pump 1. Unable to automatically switchover from Train 3 to Train 4.	
33	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Circulating Pump 1 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to start Train 4 circulating pump 2. Unable to automatically switchover from Train 3 to Train 4.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 4 circulating pump 2. Unable to automatically switchover from Train 3 to Train 4.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 4 circulating pump 2. Unable to automatically switchover from Train 3 to Train 4.	
34	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Circulating Pump 2 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Unable to position Bypass Valve for Train 4	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position Bypass Valve for Train 4	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position Bypass Valve for Train 4	

Table 7.1-7—SAS FMEA Results
Sheet 13 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
35	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Evaporator ΔP	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to position Bypass Valve for Train 4.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position Bypass Valve for Train 4.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position Bypass Valve for Train 4.	
36	Safety Chilled Water System	Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow/Loss of UHS-CCWS/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to start Train 4 chiller.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 4 chiller.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 4 chiller.	
37	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Circulating Pump 1 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to start Train 3 Circulating Pump 2. Unable to automatically switchover from Train 4 to Train 3.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 3 Circulating Pump 2. Unable to automatically switchover from Train 4 to Train 3.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 3 Circulating Pump 2. Unable to automatically switchover from Train 4 to Train 3.	
38	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Circulating Pump 2 Running	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to position Bypass Valve for Train 3	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position Bypass Valve for Train 3	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position Bypass Valve for Train 3	

Table 7.1-7—SAS FMEA Results
Sheet 14 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
39	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Evaporator ΔP	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid,.two redundant train pairs	Unable to position Bypass Valve for Train 3	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to position Bypass Valve for Train 3	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to position Bypass Valve for Train 3	
40	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to start Train 3 Chiller	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 3 Chiller	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 3 Chiller	
41	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 3 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to start Train 3 Circulating Pump 1. Unable to automatically switchover from Train 4 to Train 3	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 3 Circulating Pump 1. Unable to automatically switchover from Train 4 to Train 3	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 3 Circulating Pump 1. Unable to automatically switchover from Train 4 to Train 3	

Table 7.1-7—SAS FMEA Results
Sheet 15 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
42	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Cross-Tie Valves Position	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, two redundant train pairs	Unable to start Train 3 Circulating Pump 1. Unable to automatically switchover from Train 4 to Train 3.	A second cross-tie pair Train 1 and Train 2 serves its associated heat exchangers. Adequate cooling is provided by Train 1 and Train 2.
				b) Undetected - Spurious	None	Two redundant train pairs	Unable to start Train 3 Circulating Pump 1. Unable to automatically switchover from Train 4 to Train 3.	
				c) Undetected - Blocking	None	Two redundant train pairs	Unable to start Train 3 Circulating Pump 1. Unable to automatically switchover from Train 4 to Train 3.	
43	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Chiller Evaporator Flow	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function	No effect on system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 16 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
44	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Condenser Refrigerant Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function	No effect on system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function	
45	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Chiller Compressor Oil Pressure	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function	No effect on system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function	
46	Safety Chilled Water System	Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow/SCWS Chiller Evaporator Water Flow Control/LOOP Re-Start Failure	Train 4 Chiller Evaporator Outlet Temperature	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid; two redundant train pairs	Failed sensor is ignored. Other remaining sensors combine in the OR logic in order to execute the safety function	No effect on system function.
				b) Undetected - Spurious	None	OR and AND logic configuration	Sensor provides a spurious signal but spurious actuation is prevented by the AND logic	
				c) Undetected - Blocking	None	OR logic configuration	Other remaining sensors combine in the OR logic in order to execute the safety function.	

Table 7.1-7—SAS FMEA Results
Sheet 17 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
47	Safety Injection and Heat Removal System	Automatic Trip of LHSI Pump (in RHR Mode) on Low ΔPsat	Hot Leg Pressure WR	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, 2/4 voting	Voting logic modified to 2/3	No effect on system function
				b) Undetected - Spurious	None	2/4 voting	Voting logic becomes 1/3	
				c) Undetected - Blocking	None	2/4 voting	Voting logic becomes 2/3	
48	Safety Injection and Heat Removal System	Automatic Trip of LHSI Pump (in RHR Mode) on Low ΔPsat	Hot Leg Temperature WR	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, 2/4 voting	Voting logic modified to 2/3	No effect on system function
				b) Undetected - Spurious	None	2/4 voting	Voting logic becomes 1/3	
				c) Undetected - Blocking	None	2/4 voting	Voting logic becomes 2/3	
49	Safety Injection and Heat Removal System	Automatic Trip of LHSI Pump (in RHR Mode) on Low-Low RCS Loop Level	Hot Leg Loop Level	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Failed sensor marked invalid, 2/4 voting	Voting logic modified to 2/3	No effect on system function
				b) Undetected - Spurious	None	2/4 voting	Voting logic becomes 1/3	
				c) Undetected - Blocking	None	2/4 voting	Voting logic becomes 2/3	
50	All	All	Divisional CU	a) Detected Failure	TXS inherent or engineered fault detection mechanism	Redundant CUs in each division operating in Master/Hot-Stand-by, four redundant divisions)	Master CU switches to Slave CU. See Note 2	Hardware faults within the redundant parts of the SAS CUs, as listed in Note 2 are automatically detected. A spurious failure of a CU can cause a spurious actuation of one division. Plant actuators which, if spuriously actuated can challenge plant safety require actuation orders from more than one division.
				b) Undetected - Spurious	None	Redundant CUs in each division operating in Master/Hot-Stand-by, four redundant divisions)	Spurious signal is generated from the affected division.	
				c) Undetected - Blocking	None	Redundant CUs in each division operating in Master/Hot-Stand-by, four redundant divisions)	One division is unable to complete it's function. The safety function is completed by the other divisions.	
51	All	All	Hardwired Output Logic	b) Undetected - Spurious	None	Four redundant divisions	One division issues spurious signal to PACS, spurious actuation of single actuator with indication on PAS.	Plant actuators which, if spuriously actuated can challenge plant safety require actuation signals from more than one division to actuate (e.g., more than one pilot operator actuated from different divisions are required to change state of the main valve).
				c) Undetected - Blocking	None	Four redundant divisions.	One division unable to issue a signal to PACS, redundant divisions remain operable.	

Table 7.1-7—SAS FMEA Results
Sheet 18 of 18

No	System	SAS Function[3]	Name of Sensor, Functional Unit, or Equipment	Failure Mode[1]	Method of Detection	Inherent Compensating Provision	Effect on the SAS Function	Comments
49	All	All	PAC Module	b) Undetected - Spurious	None	Failure is toward the safe state.	Spurious actuation signal given to the attached actuator.	Plant actuators which, if spuriously actuated can challenge plant safety require actuation signals from more than one division to actuate (e.g., more than one pilot operator actuated from different divisions are required to change state of the main valve).
				c) Undetected - Blocking	None	Redundant divisions of ESF actuation.	Failure to actuate the actuator; redundant divisions remain operable.	

Notes:

1. Failure Mode – The failure cause is not identified in the system-level analysis. The failure modes are selected to bound the results of any specific failure cause. Specific failure causes can be identified only after specific equipment is selected and application software is developed.

2. Master/Hot Stand-by Assignments in the Event of Faults:

Fault In	SAS Control Unit = Master
One Division in CU A	All Divisions CU B
One Division in CU B	All Divisions CU A
Division X in both CUs	All Divisions CU A
Division X in CU A, and Division Y in CU B	Division X CU B, all other Divisions CU A

3. The following functions are bounded by the mechanical systems listed below and no I&C FMEA is required for these systems:

SYSTEM	SAS FUNCTION
Annulus Ventilation System	Accident Filtration Train Heater Control
Annulus Ventilation System	Accident Train Switchover
Component Cooling Water System	CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2
Component Cooling Water System	CCWS Common 1.b Automatic Backup Switchover of Train 2 to Train 1
Component Cooling Water System	CCWS Common 2.b Automatic Backup Switchover of Train 3 to Train 4
Component Cooling Water System	CCWS Common 2.b Automatic Backup Switchover of Train 4 to Train 3
Component Cooling Water System	CCWS Emergency Temperature Control
Component Cooling Water System	CCWS Emergency Leak Detection Sequence
Component Cooling Water System	CCWS Switchover Valves Interlock
Component Cooling Water System	CCWS RCP Thermal Barrier Containment Isolation Valves Interlock
Component Cooling Water System	CCWS Switchover Valves Leakage or Failure

SYSTEM	SAS FUNCTION
Component Cooling Water System	CCWS Condenser Supply Water Flow Control
Emergency Feedwater System	SG Closed Loop Level Control
Emergency Feedwater System	EFW Pump Flow Control
Essential Service Water System	Automatic ESW Actuation from CCWS Start
Essential Service Water Pump Building Ventilation System	Remove Heat Generated by Essential Service Water System Equipment
Fuel Building Ventilation System	Safety Related Rooms Heater Control
Fuel Building Ventilation System	Maintain Ambient Conditions for EBS & FPCS pump rooms (Recirculation Coolers)
Fuel Pool Cooling and Purification System	Pump Trip on Low SFP Level
Main Control Room Air Conditioning System	Iodine Filtration Train Heater Control
Main Control Room Air Conditioning System	Heater Control for Outside Inlet Air
Main Control Room Air Conditioning System	Pressure Control
Main Control Room Air Conditioning System	Cooler Temperature Control
Safeguard Building Controlled-Area Ventilation System	SIS / RHRS Pump Rooms Heat Removal
Safeguard Building Controlled-Area Ventilation System	CCW / EFW Valve Rooms Heat Removal
Electrical Division of Safeguard Building Ventilation System	Supply and Recirculation-Exhaust Air Flow Control
Electrical Division of Safeguard Building Ventilation System	Supply Fan Safe Shut-Off
Electrical Division of Safeguard Building Ventilation System	Recirculation Fan Safe Shut-off
Electrical Division of Safeguard Building Ventilation System	Exhaust Fan Safe Shut-off
Electrical Division of Safeguard Building Ventilation System	Supply Air Temperature
Electrical Division of Safeguard Building Ventilation System	Freeze Protection - Supply Air Temperature
Electrical Division of Safeguard Building Ventilation System	Freeze Protection - Heat Tracing
Electrical Division of Safeguard Building Ventilation System	Supply Air Temperature Control for Cooling
Electrical Division of Safeguard Building Ventilation System	Supply Air Temperature Control for Supply Air Heating
Electrical Division of Safeguard Building Ventilation System	Battery Room Heater Control
Electrical Division of Safeguard Building Ventilation System	Battery Room Supply Air Temperature
Electrical Division of Safeguard Building Ventilation System	EFWS Pump Room Heat Removal
Electrical Division of Safeguard Building Ventilation System	CCWS Pump Room Heat Removal
Safety Injection and Heat Removal System	Automatic RHRS Flow Rate Control
Safety Injection and Heat Removal System	LHSI Valves Actuation Based on RHRS Alignment

Next File

U.S. EPR Diversity and Defense-in-Depth Assessment

Technical Report ANP-10304

MARKUPS

which these diverse initiation signals are combined with the automatic actuation logic in the diverse actuation system (DAS) is similar to the PS logic.

The SICS also contains qualified display system (QDS) video display units. These are provided, in addition to the required dedicated SICS indications, to provide trending and graphing capabilities of a limited number of plant parameters to improve operator situational awareness. The QDS displays receive input from the PS for display and do not have control capabilities.

The safety-related portions of the SICS are designed to the requirements of 10 CFR 50.55a(h) (Reference 1) The design of U.S. EPR I&C systems conforms to IEEE 603-1998 in lieu of IEEE 603-1991 based on an alternative request pursuant to 10 CFR 50.55a(a)(3)(i), (Reference 16).

2.2 *Automation Systems*

The PS is a safety-related integrated RT and ESF actuation system. The PS detects the conditions indicative of an AOO or PA and actuates the plant safety features to mitigate these events. This is accomplished primarily through the execution of automatic safety I&C actuation functions; specifically, RT and actuation of ESF systems. The PS has four redundant, independent divisions. Each division is located in a physically separated Safeguards Building. Each division of the PS contains two independent subsystems to support signal diversity for RT functions. The PS utilizes the TXS platform and is designed to the requirements of 10 CFR 50.55a(h) subject to the alternative request described in Section 2.1.

RAI 505, Q. 07.08-45

The safety automation system (SAS) is a safety-related system. The SAS processes automatic control functions, and manually initiated grouped control functions, to mitigate AOOs and PAs and to reach and maintain safe shutdown. The SAS has four independent divisions. Each division is located in a physically separated Safeguards Building. Additional SAS equipment is located in the two physically separated Emergency Diesel Generating Buildings and the four Essential Service Water Pump Structures. For maximum reliability, there are redundant controllers within each division of the SAS. The SAS utilizes the TXS platform and is designed to the requirements of 10 CFR 50.55a(h) subject to the alternative request described in Section 2.1.

U.S. EPR Protection System

Technical Report ANP-10309P

MARKUPS

1.0 INTRODUCTION

This technical report describes the design of the U.S. EPR™ protection system (PS), which includes the PS architecture and the typical implementation of functionality within this architecture, and is provided to support the design certification application for the U.S. EPR. Generic terms for the PS equipment are used (e.g., function processor, communication module, input module). Table 1-1Table 1-1 lists the generic equipment references used in correlation with the equivalent specific equipment that was audited as part of the NRC review of the TXS topical report (References 23 and 24).

The PS is a reactor protection system (RPS) and an engineered safety features actuation system (ESFAS) that is implemented using TELEPERM XS (TXS) technology. The TXS platform, described in Siemens Topical Report EMF-2110 (Reference 24), has been approved by the U.S. Nuclear Regulatory Commission (NRC) for use in safety-related instrumentation and control (I&C) applications (Reference 23). The PS detects plant conditions that indicate the occurrence of an anticipated operational occurrence (AOO) and postulated accident (PA) and initiates the plant safety features required to mitigate the AOO and PA. These actions are accomplished through automatic actuation of reactor trips (RT) and engineered safety features (ESF) systems.

The PS uses state-of-the-art TXS hardware and software, adheres to the approved TXS system design principles (both hardware and software), and meets applicable regulatory requirements and industry standards.

The PS provides signal diversity for reactor trip functions, as described in Section 10.0, "Signal Diversity." The signal diversity design rules presented in Section 10 represent elements of diversity described in NUREG/CR-6303 (Reference 3). AREVA NP takes credit for the signal diversity within the PS, as The diversity attributes of the PS are described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report, ANP-10304 (Reference 30).

RAI 505, Q. 07.08-45

U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring

Technical Report ANP-10315P

MARKUPS

2.2.6.1 *Software Based Self-Test (Inherent)*

Extensive self-testing is designed as part of the TXS system software. It consists of one part, which is executed once during every startup (i.e., extended self-test), and another part, which is processed repeatedly during operation of the TXS function processor (i.e., continuous self-test). Table 2-1 provides an overview of the self-tests including whether they are executed as part of continuous and/or extended self-testing.

The continuous self-test performs only those tests which can be performed without affecting the operation of the application software. The continuous self-test is executed repeatedly during the function processor's cyclic processing. It is executed as an operating system task with the lowest priority. Thus, the operating system schedules the continuous self-test only if no other task with higher priority (e.g., the cyclic processing of application software and the processing of service commands) is pending. If the continuous self-test detects an error, it activates the exception-handler to receive error information. The exception-handler (see Section 2.2.6.3) then executes a reset or ends function processor communication by disabling the power supply of the output modules.

Executing each test of the continuous self-test task takes several minutes, the exact amount of time depends on the free time available in each clock cycle after the application processing and the service task. The runtime environment monitors the periodic execution of the continuous self-test. If the continuous self-test is not complete after one hour, the runtime environment issues an error message to the SU. This error message is also transferred to the application software for inclusion in engineered alarms to the operator.

RAI 505, Q. 07.01-40

When a self-test alarm is received, it is necessary to connect the SU to the faulted function processor to download all error messages to inspect the cause of the alarm. After required information is collected, a reset of the function processor will be performed. This reset will initiate extended self-test that must be passed to resume communication with the system. If the module is unable to pass the extended self test,

RAI 505, Q. 07.01-40

it should be replaced. Upon receiving the alarm, the module is considered inoperable until it or a replacement passes extended self-test.

The extended self-test is initiated by resetting the function processor; it is performed as part of the function processor's startup routine. During the extended self-test, additional tests are performed which can not be performed during operation without affecting the processing of the application software. Any errors detected by the extended self-test prevent the function processor from starting its cyclic processing. The function processor does not complete its startup, but instead enters an endless loop allowing for diagnosis using the maintenance laptop. The maintenance laptop connects to the card front serial interface and communicates only with this single processor while connected. The single function processor is manually rebooted and run in diagnosis state. This processor is not considered operational while the maintenance laptop is connected and in diagnosis state. Once maintenance is finished, the maintenance laptop is disconnected and the function processor is manually reset. The function processor automatically executes an extended self-test during the restart process; and, if there are no errors, then the function processor automatically enters cyclic operation.

RAI 505, Q. 07.01-34

2.2.6.1.1 Functions of the TELEPERM XS Maintenance Laptop

The maintenance laptop connects to the serial interface on the front of a processor. It is used to perform the following functions:

1. Initial Software Loading

   The initial software load is made using the TELEPERM XS maintenance laptop, because bootstrap loading of any TELEPERM XS processor is not possible via the TELEPERM XS service unit because access from the service unit is not possible without TELEPERM XS system software, application software, and pre-defined communication links installed. The SVEx processor can load software from this interface only when the processor is in boot load mode, which requires the function

RAI 505, Q. 07.01-34

2.2.6.1.3 Maintenance Laptop and Test Machine Access Control

The administrative controls for the maintenance laptop and test machine provide software and data security protection from unauthorized activities attempting to introduce or use unrecognized software vulnerabilities. The interface can be accessed only by opening the TELEPERM XS cabinet door, which generates a control room alarm. Resetting a TELEPERM XS processor (to enter boot load or diagnostic monitor modes) also generates a control room alarm. The use of the sveload software requires a license dongle.

The maintenance laptop (including the X4.1 interface connection cable) and test machine are controlled in accordance with the plant software and data security plan required by 10 CFR 73.54. The test machine is only used for periodic testing and is normally not connected to the system.

RAI 505, Q. 07.01-34

Controls for the maintenance laptop include the following:

- Storage in physically secure location when not in use.
- Physical access controls to prevent unauthorized individuals from obtaining access.
- Ability to configure or secure drives and ports to prevent alternate boot methods.
- Prohibit use for general purpose computing.
- User authorization process.
- Ability to modify or configure TELEPERM XS system files in accordance with established configuration control processes.
- Verify that adequate precautions (e.g., patches up-to-date and on demand virus scan) have been taken prior to connecting to the TELEPERM XS system.
- Verify work authorization prior to connecting to the TELEPERM XS system.
- Prevent ability to modify changeable parameters.

- Prevent ability to initiate signal tracing or issue service requests.
- Prevent ability to access the TELEPERM XS RunTime Environment to change modes.
- Prevent ability to change predefined communication channels in TELEPERM XS system via the maintenance laptop.

RAI 505, Q. 07.01-34

The test machine only interfaces to the system under test through hard-wired interfaces (24 VDC input and output); therefore, some of the software controls applicable to the maintenance laptop (modifying changeable parameters, issue service request, etc.) are not applicable to the test machine.

Controls for the test machine include the following:

- Storage in physically secure location when not in use.
- Physical access controls to prevent unauthorized individuals from obtaining access.
- Prohibit use for general purpose computing.
- User authorization process.
- Verify that adequate precautions (e.g. patches up-to-date and on demand virus scan) have been taken prior to connecting to the TELEPERM XS system.
- Verify work authorization prior to connecting to the TELEPERM XS system.

2.2.6.2 *Hardware Watchdog (Inherent)*

TXS function processors are equipped with a hardware based watchdog timer. The monitoring time of the watchdog is the cycle time of the runtime environment + 110 millisecond (ms). The hardware watchdog must be re-triggered by the runtime environment software before its expiration. If the software fails to do so, an error is assumed and a hardwired signal is used to indicate a processor failure, and to switch off the (input/output (I/O) modules' power supply to verify a defined fail-safe behavior of the

affected function processor, independently from software based monitoring. Additionally, the exception-handler is activated, initiating a specific response (see section 2.2.6.3).

The hardware watchdog timer is periodically tested by the cyclic self-test. For this test, a trip of the watchdog is triggered by the self-test task, and the trip is verified on the associated interrupt signal. The "normal" response to this watchdog-interrupt is blocked for the duration of the test.

RAI 505, Q. 07.01-39

2.2.6.3 *Exception-Handler (Inherent)*

The exception handler is activated when exceptional situations are encountered during runtime (also in case of a fault detected by the cyclic self-test). After activation, the exception-handler deactivates all output boards through driver calls, and cyclic communication is stopped. Self monitoring result information is saved, which includes: exception type, exception number, exception address, memory dump and stack dump.

Depending on the type of fault, the exception-handler either resets or halts the function processor, as indicated. If a second exceptional situation occurs within a specified period after a reset (depends on cycle time: e.g., 5 minutes for a 50 ms cycle), the function processor is deactivated. Tables 2-2, 2-3, and 2-4 show the exceptional situations that activate the exception handler.

2.2.6.4 *Error Detection by the Runtime Environment (Inherent)*

[ ]