ArevaEPRDCPEm Resource

From: WELLS Russell (AREVA) [Russell.Wells@areva.com]
Sent: Monday, March 28, 2011 8:05 AM
To: Tesfaye, Getachew
Cc: HUDSON Greg (AREVA); BUDZIK Dennis (AREVA); BENNETT Kathy (AREVA); DELANO Karen (AREVA); HALLINGER Pat (EXTERNAL AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); WILLIFORD Dennis (AREVA)
Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Question 7.9-64
Attachments: RAI 442 Question 07.09-64 Response US EPR DC - DRAFT.pdf

Getachew,

Attached is a draft response for RAI No. 442, FSAR Ch. 7, Question 7.9.64 as shown below in advance of the April 28, 2011 final date. Proposed changes to the instrumentation and controls (I&C) architecture were communicated to the NRC staff in the February 15, 2011 public meeting. U.S. EPR FSAR Tier 2, Sections 7.4 and 7.6 attached to this response incorporate the revised I&C architecture. These sections are provided in their entirety with this response to facilitate NRC review.

Let me know if the staff has questions or if this can be sent as a final response.

Thanks,

Russ Wells
U.S. EPR Design Certification Licensing Manager
AREVA NP, Inc.
3315 Old Forest Road, P.O. Box 10935
Mail Stop OF-57
Lynchburg, VA 24506-0935
Phone: 434-832-3884 (work)
434-942-6375 (cell)
Fax: 434-382-3884
Russell.Wells@Areva.com

From: WELLS Russell (RS/NB)
Sent: Tuesday, March 15, 2011 12:51 PM
To: 'Tesfaye, Getachew'
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. 442, FSAR Ch. 7, Supplement 6

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. Supplement 1 response was sent on January 7, 2011 to provide a revised schedule for four of the questions. Supplement 2 response was sent on February 9, 2011 to provide a revised schedule. Supplement 3 response was sent on February 18, 2011 to provide technically correct and complete responses to four questions. Supplement 4 response was sent on February 25, 2011 to provide technically correct and complete response to one question. Supplement 5 response was sent on March 2, 2011 to provide technically correct and complete responses to three of the 12 remaining questions.

Based on discussions with NRC, the attached file, "RAI 442 Supplement 6 Response US EPR DC.pdf" provides technically correct and complete responses to two of the 9 questions, as committed.

The following table indicates the respective pages in the response document, "RAI 442 Supplement 6 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 442 07.01-32	2	3
RAI 442 07.09-67	4	5

AREVA NP's schedule for providing a technically correct and complete response to the remaining questions in RAI 442 remains unchanged and is provided below.

Question #	Response Date
RAI 442 — 7.1-26	April 21, 2011
RAI 442 — 7.1-27	April 14, 2011
RAI 442 — 7.1-28	April 7, 2011
RAI 442 — 7.1-30	April 28, 2011
RAI 442 — 7.1-31	April 7, 2011
RAI 442 — 7.3-32	April 14, 2011
RAI 442 — 7.9-64	April 28, 2011

Sincerely,

Russ Wells
U.S. EPR Design Certification Licensing Manager
AREVA NP, Inc.
3315 Old Forest Road, P.O. Box 10935
Mail Stop OF-57
Lynchburg, VA 24506-0935
Phone: 434-832-3884 (work)
434-942-6375 (cell)
Fax: 434-382-3884
Russell.Wells@Areva.com

From: WELLS Russell (RS/NB)
Sent: Wednesday, March 02, 2011 4:52 PM
To: Tesfaye, Getachew
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. 442, FSAR Ch. 7, Supplement 5

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. Supplement 1 response was sent on January 7, 2011 to provide a revised schedule for four of the questions. Supplement 2 response was sent on February 9, 2011 to provide a revised schedule. Supplement 3 response was sent on February 18, 2011 to provide technically correct and complete responses to four questions. Supplement 4 response was sent on February 25, 2011 to

provide technically correct and complete response to one question. Based on discussions with NRC, the attached file, "RAI 442 Supplement 5 Response US EPR DC.pdf" provides technically correct and complete responses to three of the 12 questions, as committed.

The following table indicates the respective pages in the response document, "RAI 442 Supplement 5 Response US EPR DC.pdf," that contain AREVA NP's response to the subject question.

Question #	Start Page	End Page
RAI 442 07.03-33	2	2
RAI 442 07.03-34	3	4
RAI 442 07.09-61	5	8

AREVA NP's schedule for providing a technically correct and complete response to all questions in RAI 442 remains unchanged and is provided below.

Question #	Response Date
RAI 442 — 7.1-26	April 21, 2011
RAI 442 — 7.1-27	April 14, 2011
RAI 442 — 7.1-28	April 7, 2011
RAI 442 — 7.1-30	April 28, 2011
RAI 442 — 7.1-31	April 7, 2011
RAI 442 — 7.1-32	April 7, 2011
RAI 442 — 7.3-32	April 14, 2011
RAI 442 — 7.9-64	April 28, 2011
RAI 442 — 7.9-67	April 7, 2011

Sincerely,

Russ Wells
U.S. EPR Design Certification Licensing Manager
AREVA NP, Inc.
3315 Old Forest Road, P.O. Box 10935
Mail Stop OF-57
Lynchburg, VA 24506-0935
Phone: 434-832-3884 (work)
434-942-6375 (cell)
Fax: 434-382-3884
Russell.Wells@Areva.com

From: WELLS Russell (RS/NB)
Sent: Friday, February 25, 2011 8:07 AM
To: Tesfaye, Getachew
Cc: BRYAN Martin (External RS/NB); 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. 442, FSAR Ch. 7, Supplement 4

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. Supplement 1 response was sent on January 7, 2011 to provide a revised schedule for four of the questions. Supplement 2 response was sent on February 9, 2011 to provide a revised schedule. Supplement 3 response was sent on February 18, 2011 to provide technically correct and complete responses to four questions. Based on discussions with NRC, the attached file, "RAI 442 Supplement 4 Response US EPR DC.pdf" provides technically correct and complete responses to one of the 13 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report and Technical Report ANP-10309P, in redline-strikeout format which support the response to RAI 442 Question 07.09-63.

The following table indicates the respective pages in the response document, "RAI 442 Supplement 4 Response US EPR DC.pdf," that contain AREVA NP's response to the subject question.

Question #	Start Page	End Page
RAI 442 07.09-63	2	2

Based upon the information presented to the NRC during the February 15, 2011, Public Meeting, the schedule for the remaining questions has been changed.

AREVA NP's schedule for providing a technically correct and complete response to all questions in RAI 442 is provided below.

Question #	Response Date
RAI 442 — 7.1-26	April 21, 2011
RAI 442 — 7.1-27	April 14, 2011
RAI 442 — 7.1-28	April 7, 2011
RAI 442 — 7.1-30	April 28, 2011
RAI 442 — 7.1-31	April 7, 2011
RAI 442 — 7.1-32	April 7, 2011
RAI 442 — 7.3-32	April 14, 2011
RAI 442 — 7.3-33	April 7, 2011
RAI 442 — 7.3-34	April 7, 2011
RAI 442 — 7.9-61	April 7, 2011
RAI 442 — 7.9-64	April 28, 2011
RAI 442 — 7.9-67	April 7, 2011

Sincerely,

Russ Wells
U.S. EPR Design Certification Licensing Manager
AREVA NP, Inc.
3315 Old Forest Road, P.O. Box 10935
Mail Stop OF-57
Lynchburg, VA 24506-0935
Phone: 434-832-3884 (work)
434-942-6375 (cell)
Fax: 434-382-3884

Russell.Wells@Areva.com

From: BRYAN Martin (External RS/NB)
Sent: Friday, February 18, 2011 12:21 PM
To: Tesfaye, Getachew
Cc: DELANO Karen (RS/NB); ROMINE Judy (RS/NB); BENNETT Kathy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Supplement 3

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. Supplement 1 response was sent on January 7, 2011 to provide a revised schedule for four of the questions. Supplement 2 response was sent on February 9, 2011 to provide a revised schedule. Based on discussions with NRC, the attached file, "RAI 442 Supplement 3 Response US EPR DC.pdf" provides technically correct and complete responses to four of the 17 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report and Technical Report ANP-10281P, in redline-strikeout format which support the response to RAI 442 Question 07.01-29.

The following table indicates the respective pages in the response document, "RAI 442 Supplement 3 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 442 07.01-29	2	2
RAI 413 07.09-62	3	4
RAI 413 07.09-65	5	5
RAI 413 07.09-66	6	6

The schedule for technically correct and complete responses to the remaining 13 questions is unchanged and provided below:

AREVA NP's schedule for providing a technically correct and complete response to all questions in RAI 442 is provided below.

Question #	Response Date
RAI 442 — 7.1-26	March 15, 2011
RAI 442 — 7.1-27	March 15, 2011
RAI 442 — 7.1-28	March 15, 2011
RAI 442 — 7.1-30	March 15, 2011
RAI 442 — 7.1-31	March 15, 2011
RAI 442 — 7.1-32	March 15, 2011
RAI 442 — 7.3-32	March 15, 2011
RAI 442 — 7.3-33	March 15, 2011
RAI 442 — 7.3-34	March 15, 2011
RAI 442 — 7.9-61	March 15, 2011
RAI 442 — 7.9-63	March 15, 2011

RAI 442 — 7.9-64	March 15, 2011
RAI 442 — 7.9-67	March 15, 2011

Sincerely,

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

From: BRYAN Martin (External RS/NB)
Sent: Wednesday, February 09, 2011 5:07 PM
To: Tesfaye, Getachew
Cc: DELANO Karen (RS/NB); ROMINE Judy (RS/NB); BENNETT Kathy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Supplement 2

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. Supplement 1 response was sent on January 7, 2011 to provide a revised schedule for four of the questions. To allow additional time to interact with the staff and to process the responses a revised schedule is provided below. It should be noted that the dates below may need to be adjusted following the February 15, 2011 public meeting between AREVA and the NRC on digital instrumentation and controls.

AREVA NP's schedule for providing a technically correct and complete response to all questions in RAI 442 is provided below.

Question #	Response Date
RAI 442 — 7.1-26	March 15, 2011
RAI 442 — 7.1-27	March 15, 2011
RAI 442 — 7.1-28	March 15, 2011
RAI 442 — 7.1-29	March 15, 2011
RAI 442 — 7.1-30	March 15, 2011
RAI 442 — 7.1-31	March 15, 2011
RAI 442 — 7.1-32	March 15, 2011
RAI 442 — 7.3-32	March 15, 2011
RAI 442 — 7.3-33	March 15, 2011
RAI 442 — 7.3-34	March 15, 2011
RAI 442 — 7.9-61	March 15, 2011
RAI 442 — 7.9-62	March 15, 2011
RAI 442 — 7.9-63	March 15, 2011
RAI 442 — 7.9-64	March 15, 2011
RAI 442 — 7.9-65	March 15, 2011
RAI 442 — 7.9-66	March 15, 2011
RAI 442 — 7.9-67	March 15, 2011

Sincerely,

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

From: BRYAN Martin (External RS/NB)
Sent: Friday, January 07, 2011 11:15 AM
To: Tesfaye, Getachew
Cc: DELANO Karen (RS/NB); ROMINE Judy (RS/NB); BENNETT Kathy (RS/NB); RYAN Tom (RS/NB); PANNELL George (CORP/QP)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Supplement 1

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. To allow additional time to interact with the staff a revised schedule is provided below for questions 7.1.29, 7.1.32, 7.9-65 and 7.9-67. The schedule for the other questions remains unchanged.

AREVA NP's schedule for providing a technically correct and complete response to all questions in RAI 442 is provided below.

Question #	Response Date
RAI 442 — 7.1-26	March 15, 2011
RAI 442 — 7.1-27	March 15, 2011
RAI 442 — 7.1-28	March 15, 2011
RAI 442 — 7.1-29	**February 9, 2011**
RAI 442 — 7.1-30	February 9, 2011
RAI 442 — 7.1-31	March 15, 2011
RAI 442 — 7.1-32	**February 9, 2011**
RAI 442 — 7.3-32	February 9, 2011
RAI 442 — 7.3-33	February 9, 2011
RAI 442 — 7.3-34	March 15, 2011
RAI 442 — 7.9-61	February 9, 2011
RAI 442 — 7.9-62	February 9, 2011
RAI 442 — 7.9-63	February 9, 2011
RAI 442 — 7.9-64	March 15, 2011
RAI 442 — 7.9-65	**March 15, 2011**
RAI 442 — 7.9-66	February 9, 2011
RAI 442 — 7.9-67	**February 9, 2011**

Sincerely,

Martin (Marty) C. Bryan
U.S. EPR Design Certification Licensing Manager
AREVA NP Inc.
Tel: (434) 832-3016

702 561-3528 cell
Martin.Bryan.ext@areva.com

From: BRYAN Martin (External RS/NB)
Sent: Friday, November 19, 2010 5:12 PM
To: 'Tesfaye, Getachew'
Cc: DELANO Karen (RS/NB); ROMINE Judy (RS/NB); BENNETT Kathy (RS/NB); PANNELL George (CORP/QP)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 442 Response US EPR DC.pdf" provides a schedule since a technically correct and complete response to the 17 question (s) is not provided.

The following table indicates the respective pages in the response document, "RAI 442 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 442 — 7.1-26	2	2
RAI 442 — 7.1-27	3	3
RAI 442 — 7.1-28	4	4
RAI 442 — 7.1-29	5	5
RAI 442 — 7.1-30	6	6
RAI 442 — 7.1-31	7	8
RAI 442 — 7.1-32	9	9
RAI 442 — 7.3-32	10	10
RAI 442 — 7.3-33	11	11
RAI 442 — 7.3-34	12	12
RAI 442 — 7.9-61	13	13
RAI 442 — 7.9-62	14	14
RAI 442 — 7.9-63	15	15
RAI 442 — 7.9-64	16	16
RAI 442 — 7.9-65	17	17
RAI 442 — 7.9-66	18	18
RAI 442 — 7.9-67	19	19

A complete answer is not provided for the 17 questions. The schedule for a technically correct and complete response to these questions is provided below.

Question #	Response Date
RAI 442 — 7.1-26	March 15, 2011
RAI 442 — 7.1-27	March 15, 2011
RAI 442 — 7.1-28	March 15, 2011
RAI 442 — 7.1-29	January 7, 2011
RAI 442 — 7.1-30	February 9, 2011
RAI 442 — 7.1-31	March 15, 2011
RAI 442 — 7.1-32	January 7, 2011
RAI 442 — 7.3-32	February 9, 2011

RAI 442 — 7.3-33	February 9, 2011
RAI 442 — 7.3-34	March 15, 2011
RAI 442 — 7.9-61	February 9, 2011
RAI 442 — 7.9-62	February 9, 2011
RAI 442 — 7.9-63	February 9, 2011
RAI 442 — 7.9-64	March 15, 2011
RAI 442 — 7.9-65	January 7, 2011
RAI 442 — 7.9-66	February 9, 2011
RAI 442 — 7.9-67	January 7, 2011

Sincerely,

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

From: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Wednesday, October 20, 2010 8:09 AM
To: ZZ-DL-A-USEPR-DL
Cc: Zhao, Jack; Morton, Wendell; Mott, Kenneth; Spaulding, Deirdre; Truong, Tung; Zhang, Deanna; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: U.S. EPR Design Certification Application RAI No. 442(4295,5076,5068,5067), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on September 10, 2010, and discussed with your staff on October 13, 2010. Drat RAI Questions 07.01-26 and 07.03-33 were modified as a result of that discussion. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 2751

Mail Envelope Properties (1F1CC1BBDC66B842A46CAC03D6B1CD4104247912)

Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Question 7.9-64
Sent Date: 3/28/2011 8:04:41 AM
Received Date: 3/28/2011 8:04:47 AM
From: WELLS Russell (AREVA)

Created By: Russell.Wells@areva.com

Recipients:
"HUDSON Greg (AREVA)" <Greg.Hudson@areva.com>
Tracking Status: None
"BUDZIK Dennis (AREVA)" <Dennis.Budzik@areva.com>
Tracking Status: None
"BENNETT Kathy (AREVA)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen (AREVA)" <Karen.Delano@areva.com>
Tracking Status: None
"HALLINGER Pat (EXTERNAL AREVA)" <Pat.Hallinger.ext@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
"WILLIFORD Dennis (AREVA)" <Dennis.Williford@areva.com>
Tracking Status: None
"Tesfaye, Getachew" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

Post Office: AUSLYNCMX02.adom.ad.corp

Files	**Size**	**Date & Time**	
MESSAGE	18429	3/28/2011 8:04:47 AM	
RAI 442 Question 07.09-64 Response US EPR DC - DRAFT.pdf			863253

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

Response to

Request for Additional Information No.442 (4295, 5076, 5068, 5067), Revision 1, Question 07.09-64

10/20/2010

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: 07.09 - Data Communication Systems

Application Section: FSAR Ch 7

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

Question 07.09-64:

Follow-up to RAI 56, Questions 7.9-11

Clarify U.S. EPR, Tier 2, FSAR, Figure 7.1-7 to demonstrate compliance with IEEE Std. 603-1998, Clause 5.1.

IEEE Std. 603-1998, Clause 5.1 requires safety systems to perform all safety functions required for a design basis event in the presence of: (1) any single detectable failure within the safety systems concurrent with all identifiable but non-detectable failures; (2) all failures caused by the single failure; and (3) all failures and spurious system actions that cause or are caused by the design basis event requiring the safety functions. In the case of SAS, U.S. EPR, Tier 2, FSAR, Figure 7.1-7 shows that the Control Units (CU)s of redundant Safety Automation System (SAS) divisions are interconnected in a bus network. As such, the staff finds that the applicant has not demonstrated how a failure within the CUs of one division will not propagate to another division. As a result, the staff requested the applicant to demonstrate how the SAS design meets the requirements of IEEE Std. 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21, in RAI 56, Question 7.9-11. In response, the applicant provided in "Response to Request for Additional Information No. 56, Supplement 1: U.S. EPR Design Certification Application," a description of how the data communications within the SAS meet IEEE Std. 603-1998, Clause 5.1, and 10 CFR Part 50, Appendix A, GDC 21. This response states that, as described in U.S. EPR, Tier 2, FSAR, Section 7.1.1.4.2, "Data Communications," the CU-CU networks within the SAS are point-to-point between divisions, and separate networks are provided for the A and B redundancies. This result in six individual point-to-point connections for redundancy A, and another six interdivisional connections exist for redundancy B. A single failure that impairs any one of these connections only affects communications between two CUs. For example, if the Division 1 CU(A) to Division 2 CU(A) connection fails, Division 1 CU(A) and Division 2 CU(A) both still communicate with the CU(A)s in Divisions 3 and 4. The staff finds this response is inconsistent with Figure 7.1-7 within the U.S. EPR, Tier 2, FSAR, as documented in RAI 07.09-54. Specifically, the staff reviewed Figure 7.1-7, "Safety Automation System Architecture," and finds that these CU-CU networks are connected in a bus topology and not point-to-point connections as specified in the RAI response. The staff requests the applicant to clarify the representation of the SAS network architecture to clearly demonstrate the point to point connection between CUs to show how the design meets IEEE Std. 603-1998, Clause 5.1.

Response to Question 07.09-64:

U.S. EPR, Tier 2, FSAR Figure 7.1-7 was modified to show point-to-point communication between different divisions of the safety automation system (SAS) (control unit-control unit (CU-CU)) and include legend descriptions. SAS interdivisional communication will occur via qualified isolation devices, as described in U.S. EPR, Tier 2, Section 7.1.1.6.4.

To support the submittal of complete and consistent information, and considering multiple RAI responses and design changes communicated to the NRC staff, U.S. EPR FSAR markups will be submitted with a corresponding RAI response. The U.S. EPR FSAR Tier 2, Section 7.1 revisions described in this response was submitted with the Response to RAI 442, Question 07.01-26.

Proposed changes to the instrumentation and controls architecture were communicated to the NRC staff in the February 15, 2011 public meeting. U.S. EPR FSAR Tier 2, Section 7.4 and

Section 7.6 have been revised to incorporate the modified I&C architecture. These sections are provided in their entirety with this response to facilitate NRC review.

FSAR Impact:

U.S. EPR FSAR Tier 2, Sections 7.4 and 7.6 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

7.4 Systems Required For Safe Shutdown

To achieve a safe shutdown configuration, the appropriate alignment of systems is required to implement the following functions associated with attaining and maintaining a safe shutdown condition:

- Reactivity control.
- Reactor coolant makeup.
- Reactor coolant system pressure control.
- Decay heat removal.
- Process monitoring.

The definition of safe shutdown, the criteria applicable to the shutdown, and the equipment that can be utilized to reach safe shutdown are different depending on the scenario. This section provides information on components and systems that are used to achieve safe shutdown for specific scenarios.

- Shutdown using only safety-related equipment to shutdown the plant in accordance with BTP 5-4 (Reference 2).
- Shutdown post-fire in accordance with RG 1.189.
- Shutdown required during and following a station blackout (SBO) in accordance with 10 CFR 50.63 and in accordance with RG 1.155.

Section 7.4.1 describes the systems necessary to achieve safe shutdown, including the instrumentation and control (I&C) systems that are associated with the safe shutdown functions. Several systems can perform a safe shutdown function. Section 7.4.1 also notes the description of these systems and their associated I&C references.

7.4.1 Description

7.4.1.1 I&C Systems Associated with Safe Shutdown

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. ~~The SAS provides manual and grouped commands execution initiated from either the safety information and control system (SICS) or the process information and control system (PICS).~~ The SAS provides grouped commands execution initiated from the safety information and control system (SICS). This is designed to provide control of the safety-related systems that are needed to reach safe

442, 07.09-64

442, 07.09-64

shut down of the plant. ~~for ESF features or to control other systems that are not ESF actuated, which include supporting systems.~~

~~In certain scenarios, non-safety-related systems perform shutdown functions. These functions are initiated in the process automation system (PAS).~~ The priority and actuator control system (PACS) controls safety-related components associated with safe shutdown. The functions performed by the ~~priority and actuator control system (~~PACS~~)~~ are described in Section 7.1.1.4.3. The manual functions needed for safe shutdown functions are duplicated in the process information and control system (PICS) and the process automation system (PAS). The SICS is directly hardwired to PACS for the component-level manual commands.

The human machine interface (HMI) is the PICS and SICS. ~~In case of unavailability of the PICS, functions needed to achieve and maintain a safe shutdown condition can be controlled through the SICS.~~ Monitoring and control of the safety-related systems are both available in the main control room (MCR) and the remote shutdown station (RSS). The operator uses the PICS as the primary HMI in the MCR and RSS to mitigate the event and to achieve and maintain cold shutdown. Because the PICS does not send commands to the DAS, PS, or SAS, there are some functions that the operator must perform using the SICS from the MCR. These include:

- Manual actuation of reactor trip (RT) and ESF actuation (as required).
- Manual reset of ESF actuation functions.
- Validating or inhibiting of DAS and PS permissives as needed to transition the plant to cold shutdown.
- Interfacing with automatic functions within SAS (e.g., auto/manual switchover) as needed.

The SICS inventory in the RSS consists of the following controls that are unavailable on PICS but are needed to achieve and maintain cold shutdown:

- RT.
- P12 permissive (switches safety injection (SI) modes, bypasses main steam relief train (MSRT) isolation, MSIV Isolation, MFW (SSS) isolation functions, and SI accumulator valve interlock bypass).
- P14 permissive (partial cooldown operating bypass, setpoint change for MSRT opening RHR interlock).
- P15 permissive (SI mode switching).
- P17 permissive (PSRV opening operating bypass, large miniflow line interlock).

- SI actuation reset.
- Emergency feedwater (EFW) actuation reset.
- EFW isolation reset.
- MSRT actuation reset.
- MSRT isolation reset.
- SG isolation reset.

7.4.1.2 Safe Shutdown Using Safety-Related Systems and Equipment

The plant is designed so that it can be taken from normal operating conditions to cold shutdown using only safety-related systems. The safety-related systems and equipment, that with proper alignment are capable of achieving a safe shutdown of the plant, are described in Section 7.4.1.2.1 through Section 7.4.1.2.13. These systems satisfy GDC 1, GDC 2, GDC 3, and GDC 4.

442, 07.09-64

The systems and equipment described in Section 7.4.1.2.1 through Section 7.4.1.2.13 are capable of bringing the plant to a cold shutdown condition, with only offsite or onsite power available along with the most limiting single failure. The entire shutdown procedure is completed from the MCR.

Table 7.4-1—SAS Automatic Safety Function lists the automatic SAS safety functions for the systems listed in Sections 7.4.1.2.1 through 7.4.1.2.13 by system, function name, function safety basis. This table also identifies which SAS functions include interdivisional communications, type of interdivisional communications data, signal type of the interdivisional communications, and the FSAR section referenced for each system.

7.4.1.2.1 Emergency Feedwater System

The emergency feedwater system (EFWS) provides a safety-related means of supplying feedwater to the steam generators (SG) for decay heat removal. This system is capable of maintaining hot standby and facilitating a plant cooldown. The I&C associated with the EFWS, are described in Section 10.4.9.

7.4.1.2.2 Main Steam ~~Supply~~ System

The main steam ~~supply~~ system (~~MSSS~~MSS) contains the ~~main steam relief train~~ (~~MSRT~~). The MSRT provides secondary side pressure control capability. The MSRT valves are located outside of containment upstream of the main steam isolation valves (MSIV). These valves are used to remove decay heat via the SGs in the event the condenser is unavailable (including loss of power), and to dissipate the heat to atmosphere. The MSRT may be used to cool and depressurize the reactor coolant

system (RCS) to conditions necessary to initiate residual heat removal (RHR). The ~~MSSS~~MSS contains the MSIVs and associated bypass valves that are necessary to isolate the secondary plant and to allow decay heat removal by the MSRT. The I&C associated with the ~~MSSS~~MSS are described in Section 10.3.

7.4.1.2.3 Medium Head Safety Injection

442, 07.09-64

The safety injection system (SIS) contains medium head safety injection (MHSI) pumps that are capable of providing negative reactivity by the injection of highly borated water into the RCS from the in-containment refueling water storage tank (IRWST). The MHSI pumps may be used to add boron to the RCS during hot shutdown and cold shutdown phases, if the extra borating system (EBS) is unavailable. The I&C associated with the MHSI pumps are described in Section 6.3.

7.4.1.2.4 Extra Borating System

The EBS provides negative reactivity by injecting highly borated water into the RCS during the cooldown from the controlled state to the safe shutdown state to achieve core shutdown margin. The I&C associated with the EBS are described in Section 6.8.

7.4.1.2.5 Residual Heat Removal System

The residual heat removal system (RHRS) provides the residual heat removal (RHR) needed to reach cold shutdown and to control the primary temperature during cold shutdown. The I&C associated with the RHRS are described in Section 5.4.7.

7.4.1.2.6 Excore Instrumentation System

The neutron flux range of measurement cannot be covered with sufficient accuracy by a single detector system. The range is subdivided into three overlapping ranges; source range, intermediate range, and power range. The source range monitors the lower six decades of neutron flux and is used to diagnose the plant status with regard to criticality in shutdown states.

7.4.1.2.7 Reactor Coolant System

The RCS transfers heat from the core to the SGs to allow cooldown and depressurization of the RCS. Once the appropriate RCS temperature and pressure~~s~~ are met, connection of the RHRS to the RCS is allowed for further cooldown of the plant. The RCS provides the interface between the core and the RHRS for decay heat removal. Section 5.4 describes the components of the RCS.

7.4.1.2.8 Emergency Diesel Generators and Auxiliaries

Four emergency diesel generators (EDG) (one per division) provide a reliable power source capable of starting and supplying necessary loads required to safely shut down

and maintain a shutdown condition during a loss of offsite power (LOOP). The diesel generator (DG) fuel oil storage and transfer system, the DG cooling water system, the DG starting air system, the DG lubricating~~on~~ oil system, and the DG ~~combustion~~ air intake and exhaust system are required to support EDG operation.

The I&C associated with the DG auxiliaries are described in Section 9.5.

7.4.1.2.9 Essential Service Water System

The essential service water system (ESWS) transfers heat from the component cooling water system (CCWS) to the ultimate heat sink. The I&C associated with the ESWS is described in Section 9.2.1.

7.4.1.2.10 Component Cooling Water System

The ~~system~~CCWS is an intermediate cooling system between safety-related loads and the ESWS. The CCWS transfers heat from plant safety-related and non-safety-related components to the ESWS. The I&C associated with the CCWS is described in Section 9.2.2.

7.4.1.2.11 Safety Chilled Water System

The safety chilled water system (SCWS) provides chilled water for heating, ventilation, and air conditioning (HVAC) heat removal to safety-related room cooling units and cooling to T~~t~~rain 1 and T~~t~~rain 4 of the RHRS. Refer to Section 5.4.7 for more information on cooling water supplies to the RHRS. The I&C associated with the SCWS is described in Section 9.2.8.

7.4.1.2.12 Heating Ventilation and Air Conditioning Systems

442, 07.09-64

The HVAC systems provide ambient temperature control for the systems and components that are necessary for safe shutdown. These are the HVAC systems required for safe shutdown:

- Main ~~C~~control room air conditioning system.
- Fuel building ventilation system.
- Safeguard building controlled-area ventilation system.
- Electrical division of safeguard building ventilation system.
- Emergency power generating building ventilation system.
- Emergency service water pump building ventilation system.
- Annulus ventilation system.

The I&C associated with the HVAC systems is described in ~~Section~~Sections 6.2.3 and ~~9.4~~9.4.

7.4.1.2.13 Power Distribution System

The power distribution system distributes the available power (onsite or offsite) to the loads required for safe shutdown. Section 8.3 describes the buses required for operation of the safety-related equipment necessary for shutdown of the plant.

7.4.1.3 Post-fire Safe Shutdown Systems

The selection of post-fire safe shutdown systems is based on meeting the guidance of RG 1.189. These assumptions, based on RG 1.189, were made in the selection process:

- All equipment in one fire area (except for the MCR and containment) is rendered inoperable by fire.
- Re-entry to the fire area for repair or operator actions is not possible.

442, 07.09-64

The fire protection analysis described in Appendix 9A confirms the plant capability to safely shutdown following a fire. The systems described in Section 7.4.1.2 and the additional systems listed in Section 7.4.1.3.1 through Section 7.4.1.3.3 were identified as post-fire safe shutdown systems.

7.4.1.3.1 Main Feedwater System

Associated circuits of concern were identified when selecting post-~~-~~fire safe shutdown systems. These circuits are non-safety or safety circuits that could adversely affect the identified shutdown equipment by feeding back potentially disabling conditions. One of these disabling conditions is spurious operation of the ~~motor driven~~ main feedwater pumps caused by fire damage to the power circuit of these pumps. In the event that spurious operation of the main feedwater pumps occur, capability to isolate the main feedwater system is necessary to prevent possible overcooling of the steam generator (SG).

7.4.1.3.2 Chemical and Volume Control System

The chemical and volume control system (CVCS) is a non-safety-related system that provides reactivity control and reactor coolant makeup water. Reactivity control is possible through the injection of borated water through the CVCS charging lines. The CVCS is an alternate to the safety-related systems in Section 7.4.1.2 that provides reactivity control and reactor coolant makeup water. The I&C associated with the CVCS are described in Section 9.3.4.

7.4.1.3.3 Fuel Pool Cooling and Purification System

The spent fuel pool cooling and purification system (FPCPS) provides cooling to the spent fuel pool to remove decay heat during normal operation, plant shutdown, and accident conditions. The FPCPS is included as a post-fire shutdown system because fires in the spent fuel areas must be considered. The I&C associated with the FPCPS are described in Section 9.1.3.

7.4.1.3.4 Remote Shutdown Station

The RSS provides an independent alternative shutdown capability that is physically and electrically independent of the MCR.

The RSS is a control center located in Safeguard Building ~~division~~ 3 near the MCR. It contains the equipment necessary to bring the plant to a safe shutdown state during an event requiring evacuation of the MCR, in conjunction with:

442, 07.09-64

- A single failure of a system, structure, or component required to bring the plant to safe shutdown (in the event of a fire, no additional single failure, unrelated to the damage caused by the fire, is considered).
- A sustained loss of either onsite or offsite AC power.

The RSS contains HMI workstations necessary to bring the plant to, and maintain it in, a safe shutdown state. The HMI control functions of the RSS are isolated during normal, emergency, routine shutdown, refueling, or maintenance operations as long as the MCR is available. The HMI workstations both in the MCR and the RSS will continue to display all parameters available on each workstation while the control functions are isolated. Also, these workstations contain PICS equipment, SICS equipment and select communication equipment. The PICS provides most of the necessary controls for safe shutdown. The SICS only provides the controls that are not available on PICS, which include RT and selected ESF resets and permissives. The architecture of the SICS and PICS is described in Section 7.1. Communication equipment is described in Section 9.5.2.

The SICS and PICS provide~~s~~ the displays and controls in the RSS to allow the monitoring and control of the following safe shutdown functions during a postulated fire in the MCR or during an event that could cause the MCR to become uninhabitable, coupled with a single failure:

- Reactivity control.
- Reactor coolant makeup.
- Reactor coolant system pressure control.
- Decay heat removal.

- Control and monitoring of safety support systems for the above functions, as well as essential service water, component cooling water, and onsite power including the emergency diesel generators.

442, 07.09-64

The physical layout of the RSS and equipment located in it is taken into consideration in the human factors engineering program described in Chapter 18.

In the event of a condition requiring MCR evacuation, operators will transfer control from the MCR to the RSS via the ~~control transfer switches~~MCR-RSS transfer switches, which are located in the RSS~~.~~. MCR actions required to transfer control to the RSS can be accomplished during a rapid evacuation of the MCR. Communications equipment is provided to support the transfer. ~~The RSS control transfer switches can disable MCR controls and enable control functions from the RSS.~~ If the MCR requires evacuation, the operator shall take the following actions:

- Perform an RT (from the MCR if time allows, from the RSS if there is not enough time).
- Log out of the PICS workstations in the MCR (if time allows).
- Transition to the RSS.
- Actuate the MCR-RSS transfer switches, which performs the following actions:
  - Disables diverse actuation system (DAS) outputs so that no DAS functions (automatic or manual) are operable.
  - Disables manual controls for PS, SAS and PACS from the MCR.
  - Disables the ability of the PICS workstations in the MCR to communicate to the RCSL and PAS.
  - Enables manual controls for PS in the RSS.
- Log into the PICS workstations in the RSS.
- Take actions as needed to reach and maintain hot standby from the PICS.

If the MCR will be unavailable for an extended period of time, the operation will use the PICS as well as the necessary permissives and ESF resets, if necessary, on the SICS to reach and maintain cold shutdown.

The RSS is only utilized following an evacuation of the MCR. No actions are required from the RSS during normal operation.

The MCR-RSS ~~control~~ transfer switches maintain divisional independence, so that an electrical failure in one safety division cannot affect another safety division. Additionally, the MCR-RSS ~~control~~ transfer switches cannot be disabled by a single

442, 07.09-64

active failure coincident with a LOOP. Access to the MCR-RSS ~~control~~ transfer switches results in annunciation of an alarm in the MCR. The MCR-RSS transfer switches are key-locked.

Displays in the MCR and RSS contain real-time plant data prior to, during, and after control transfer from one station to the other. The RSS data are populated from the same information buses that supply data to the MCR. During the time that control is transferred from the MCR to the RSS or vice versa, data are not lost or interrupted. An indication on the PICS and SICS shows that RSS control has been established.

7.4.1.4 Station Blackout Safe Shutdown

The SBO safe shutdown equipment are predicated on fulfilling those functions delineated by 10 CFR 50.63 and RG 1.155. Section 8.4 describes the systems and equipment, including I&C systems necessary for achieving safe shutdown.

7.4.2 Analysis

7.4.2.1 Conformance to General Design Criteria

Conformance to these GDC, applicable to safe shutdown systems, is described in Section 7.1:

- GDC 2, Design Bases for Protection against Natural Phenomena.
- GDC 4, Environmental and Missile Design Bases.
- GDC 13, Instrumentation and Control.
- GDC 19, Control Room.
- GDC 24, Separation of Protection and Control Systems.
- GDC 34, Residual Heat Removal.
- GDC 35, Emergency Core Cooling.
- GDC 38, Containment Heat Removal.

7.4.2.2 Conformance to 10 CFR 50.55 a(h) and IEEE 603

442, 07.09-64

10 CFR 50.55 a(h) requires safety-related systems to meet the requirements of IEEE 603. This section addresses these IEEE Std 603-1998 (Reference 1) requirements, as they pertain to particular safety-related I&C systems used for safe shutdown. An alternative request to use IEEE 603-1998 in lieu of IEEE 603-1991 is described in Section 7.1.

- Independence.

- Use of digital systems.
- Single failure.
- Testing.

7.4.2.2.1 Independence

442, 07.09-64

The safety-related I&C systems that are used for safe shutdown are designed to meet IEEE 603-1998, Clause 5.6, "Independence," and IEEE 603-1998, Clause 6.3, "Interaction Between the Sense and Command Features and other Systems~~.~~" subject to the alternative request described in Section 7.1. Independence provisions and measures are implemented between the redundant divisions of the SCDS, PS, SAS, and the SICS. In addition, independence provisions and measures between the safety-related I&C systems and the other I&C systems make sure that possible interdependence between the safety-related I&C systems and other I&C systems does not prevent the execution of safety-related functions. Safety-related I&C systems do not depend on non-safety-related I&C systems for their safety functions. Independence of the safety-related I&C systems is addressed in Section 7.1.

7.4.2.2.2 Use of Digital Systems

The safety-related I&C systems utilize digital I&C. They are implemented using the TELEPERM XS platform which is approved for use in safety-related systems of nuclear power generating stations in the United States. These digital systems are implemented in architectures designed to satisfy requirements applicable to all safety-related I&C systems, digital or otherwise.

The IEEE Std 603-1998 contains the requirements that govern the implementation of safety-related I&C systems. IEEE Std 7-4.3.2-2003 (Reference 3) contains the requirements that govern the use of digital computers in safety-related systems. Conformance with these requirements is addressed in Section 7.1.

7.4.2.2.3 Single Failure Criterion

The four subsystems of the safety-related I&C systems are physically separated and electrically isolated. Each subsystem controls one of the four redundant subsystems-fluid, mechanical, electrical and I&C. Consequently the safety function supported by the four redundant subsystems can be performed even in case of a single failure in the I&C subsystems. In the case of the EBS, only two trains exist. One train

442, 07.09-64

of the EBS is controlled by ~~d~~Division 1 of the SAS and the other train is controlled by ~~d~~Division 4 of the SAS. A single failure in the EBS system or in the SAS will not prevent the execution of safety functions of the EBS.

The RSS is located in separate physical locations other than the MCR. The RSS control transfer switches will disable MCR controls and enable control functions from the

RSS. The transfer switches also provide isolation between the RSS and the MCR. Therefore, no single credible event will cause the MCR to be evacuated and cause the RSS to malfunction.

A failure within the safety-related I&C systems will not lead to design basis accident events even during maintenance or periodic testing.

7.4.2.2.4 Testing

Self and periodic testing of the safety-related I&C systems is implemented to detect failures that could prevent the execution of the safety-related functions.

Measures are taken to detect and identify failures during reactor operation in order to avoid long periods of operation with degraded safety-related I&C systems, structures, and components which might lead to a loss of function due to an accumulation of failures.

7.4.2.3 Remote Shutdown Capability

442, 07.09-64

The RSS provides the capability to remotely shutdown the plant. The MCR-RSS transfer switches are located in a separate fire area than the MCR to allow transfer of control without entry into the MCR. Alarms in the MCR will alert operators that control is transferred to the RSS. Parameter indications common to both the MCR and RSS are maintained throughout the transfer of control.

The RSS contains controls and indications that will allow the operators to control and monitor the safe shutdown systems. Controls and indications of permissive signals are provided in the RSS. The capability to manually validate permissives allows the operator to enable or disable protective functions that may be necessary for proper shut down of the plant. Sections 7.4.1.1 and 7.4.1.3.4 also refer to RSS capability.

Administrative controls are provided to prevent unauthorized access to the RSS. The MCR-RSS transfer switches are key locked. Keys are maintained by appropriate plant personnel.

7.4.2.4 Loss of Plant Instrument Air Systems

The safety-related I&C necessary for safe shutdown are not reliant on instrument air. Any devices that use instrument air fail in a safe position upon loss of air. Section 9.3.1 describes the plant instrument air system.

7.4.2.5 Loss of Cooling Water to Vital Equipment

Cooling water systems required for safe shutdown are addressed in Section 7.4.1.2.9 through Section 7.4.1.2.11.

7.4.2.6 Turbine Trip and Plant Load Rejection

Safe shutdown capability is provided in the event of a LOOP associated with a turbine trip or plant load rejection. The EDGs will provide power to the safe shutdown system components and I&C systems in the event of a LOOP.

7.4.3 References

1. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1998.

2. NUREG-0800, BTP 5-4, "Design Requirements of the Residual Heat Removal System," U.S. Nuclear Regulatory Commission, ~~Standard Review Plan, Branch Technical Position,~~ Rev. 4, March 2007.

3. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

Table 7.4-1—SAS Automatic Safety Function (Sheet 1 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Annulus Ventilation System (AVS)	Accident Filtration Train Heater Control	The AVS has a safety-related function to maintain capability of the iodine absorbers to remove iodine from the annulus exhaust air. The radiological filter air heaters are used to limit the relative humidity to a maximum of 70% when the AVS accident trains are in operation (RG 1.52 and ASME N509-89).	NO	N/A	N/A	The I&C associated with the AVS is described in Sections 6.2.3 and 6.5.1.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 2 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Annulus Ventilation System (AVS)	Accident Train Switchover	The AVS has a safety related function to maintain a negative pressure (GDC 16, GDC 43, Containment Leakage Testing per 10 CFR 50 Appendix J, and NRC RG 1.52 Rev 3 to provide filtration of Engineered Safety Feature Atmospheric Cleanup). In case of a failure during accident operation of an operating accident filtration train, and a negative pressure is not being maintained in the annulus, operation shall be switched to the non-operating accident filtration train to maintain a negative pressure.	NO	N/A	N/A	The I&C associated with the AVS is described in Sections 6.2.3 and 6.5.1.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 3 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The safety-related function to perform an automatic switchover from Train 1 to Train 2 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 1.a and 1.b.	(1) Div 2 to Div 1 - To switch from Train 1 to Train 2 requires a low Surge Tank Level in Div 2 : (2) Close Train 1 supply and return valves by removing power from the valves associated pilot valves that are powered via Div 1, 2, 3, and 4: (3) Div 1 to Div 2 - Verify Train 1 1.b supply and return valves are closed prior to Train 2 supply and return valves opening (i.e. interlock function)): (4) Open Train 2 supply and return valves by applying power to the valves associated pilot valves that are powered via Div 1, 2, 3, and 4	Discrete	Vote	The I&C associated with the CCWS is described in Section 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 4 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Common 1.b Automatic Backup Switchover of Train 2 to Train 1	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The safety-related function to perform an automatic switchover from Train 2 to Train 1 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 1.a and 1.b.	Similar to Train 1 to Train 2 Switchover	Discrete	Vote	The I&C associated with the CCWS is described in Section 9.2.2.
Component Cooling Water System (CCWS)	CCWS Common 2.b Automatic Backup Switchover of Train 3 to Train 4	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The safety-related function to perform an automatic switchover from Train 3 to Train 4 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 2.a and 2.b.	Similar to Train 1 to Train 2 Switchover, but for Train 3 to Train 4	Discrete	Vote	The I&C associated with the CCWS is described in Section 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 5 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Common 2.b Automatic Backup Switchover of Train 4 to Train 3	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The safety-related function to perform an automatic switchover from Train 4 to Train 3 verifies that the CCWS is capable of fulfilling its safety-related function to remove heat from safety-related components on the CCWS Common 2.a and 2.b.	Similar to Train 1 to Train 2 Switchover, but for Train 4 to Train 3	Discrete	Vote	The I&C associated with the CCWS is described in Section 9.2.2.
Component Cooling Water System (CCWS)	CCWS Emergency Temperature Control	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The safety-related function to control the CCWS heat exchanger (HX) outlet temperature is required to maintain the temperature of the cooling water within its limits. This verifies that the CCWS is capable of fulfilling its safety relegated function to remove heat from safety-related components.	NO	N/A	N/A	The I&C associated with the CCWS is described in Section 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 6 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Emergency Leak Detection	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The safety-related function for emergency leak detection maintains the required cooling water inventory that supports the safety-related function to remove heat using indications to detect leaks and isolate them (GDC 44).	NO	N/A	N/A	The I&C associated with the CCWS is described in Section 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 7 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Switchover Valve Interlock	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The interlock function is required to verify that the two trains connected to their common headers remain separated and each are able to provide their corresponding LHSI HX with the required flow for heat removal. Removing heat from the LHSI HX is a safety-related function.	If the either of the supply and return valves for a given Train (1 or 2, 3 or 4) are open with respect to a given header (1.a, 1.b, 2.a, or 2.b) then the other corresponding train supply and return valves are given a close command. Train 1 valves are in Div 1, Train 2 valves in Div 2 and so on. Therefore, the signals are sent across divisions for the close command discussed. Hence, the on coming trains supply and return valves are not allowed to open until the corresponding off going trains supply and return valves are closed.	Discrete	Vote	The I&C associated with the CCWS is described in Sections 7.6 and 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 8 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS RCP Thermal Barrier Containment Isolation Valve Interlock	The CCWS has a safety-related function to remove heat from safety-related components (GDC 44). The interlock function is required to verify that the Common 1.b and 2.b headers remain separated and each of their trains are able to provide their corresponding LHSI HX with the required flow for heat removal. Removing heat from the LHSI HX is a safety-related function.	The Inner and Outer Containment Isolation Valves are powered from different divisions. For the Common 1.b header, the outer valves (supply and return) are supplied by Div 1 and the inner valves by Div 4. The opposite is true for the Common 2.b header. To be able to switch between headers, at least one of the supply valves (outer or inner) and one of the return valves (outer or inner) must be closed. Therefore, the state (open or closed) of these valves must be communicated across divisions.	Discrete	Vote	The I&C associated with the CCWS is described in Sections 7.6 and 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 9 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Switchover Valves Leakage or Failure	The CCWS has a safety-related function to remove heat from SAS components (GDC 44). The safety-related function for switchover valve leakage or failure isolates the CCWS trains from their common headers to verify that each train is able to provide their corresponding LHSI HX with the required flow for heat removal. Removing heat from the LHSI HX is a safety-related function.	This function looks at surge tank level in the two corresponding Trains (Trains 1 and 2, Trains 3 and 4) that feed a common header. If the surge tank level in the on-line train is lowering while the surge tank level the off-line train is rising then a seat leakage on one of the off line train switchover valves is likely. Therefore, interdivisional communication is required since information from more than one division is being utilized.	Discrete	Vote	The I&C associated with the CCWS is described in Section 9.2.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 10 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Component Cooling Water System (CCWS)	CCWS Condenser Supply Water Flow Control	The CCWS has a safety-related function that controls CCWS flow to the SCWS condenser and provides a heat sink for heat rejection, therefore providing reasonable assurance that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	NO	NA	NA	The I&C associated with the CCWS is described in Section 9.2.2.
Emergency Feedwater System (EFWS)	SG Closed Loop Level Control	The EFWS has a safety-related function to: 1. Provide flow to the steam generators to restore and maintain decay heat removal from the RCS to assist in the cool down and depressurization of the RCS to the RHRS entry conditions following design basis events.	NO	N/A	N/A	The I&C associated with the EFWS is described in Sections 7.3 and 10.4.9.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 11 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
		2. Maintain the water inventory in the steam generators following a LOOP, and the resulting loss of MFW, for decay heat removal. The safety-related function to provide SG Closed Loop Level Control verifies that the EFWS is capable of fulfilling its safety-related function of maintaining the SG water inventory for decay heat removal, following a LOOP and the resulting loss of MFW.				
Emergency Feedwater System (EFWS)	EFW Pump Flow Control	The EFWS has a safety-related function to: 1. Provide flow to the SGs to restore and maintain decay heat removal from the RCS to assist in the cool down and depressurization of the RCS to the RHRS entry conditions following design basis events.	NO	N/A	N/A	The I&C associated with the EFWs is described in Sections 7.3 and 10.4.9.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 12 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
		2. Maintain the water inventory in the steam generators following a LOOP, and the resulting loss of MFW, for decay heat removal. The safety-related function to provide EFW pump flow control to maintain EFWS pump flow at the design flow verifies that the EFWS is capable of fulfilling its safety-related function of providing flow to the steam generators, below the maximum allowable flow rate to a depressurized SG, to support its safe shut down capabilities.				

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 13 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Essential Service Water System (ESWS)	Automatic ESWS Actuation from CCWS Start	The ESWS has a safety-related function to remove heat from safety-related components (GDC 44). The Automatic ESWS Actuation from CCWS Start function removes heat from the CCWS (Trains 2 and 3) and the EDGs ensuring the ESWS is capable of fulfilling its safety-related function to remove heat from the corresponding CCWS train.	NO	N/A	N/A	The I&C associated with the ESWS is described in Section 9.2.1.
Essential Service Water Pump Building Ventilation System (ESWPBVS)	Remove Heat Generated by Essential Service Water Equipment	The ESWPBVS has an safety-related function that maintains ambient conditions for safety-related components during normal operation (GDC 4, GDC 17).	NO	N/A	N/A	The I&C associated with the ESWS systems is described in Section 9.4.11.
Fuel Building Ventilation System (FBVS)	Safety-related Room Heater Control	The FBVS has an safety-related function that maintains the room ambient conditions for safety-related boron rooms during normal operation, abnormal operation, and postulated accident events (GDC 27, GDC 60, GDC 61).	NO	N/A	N/A	The I&C associated with the FBVS system is described in Section 9.4.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 14 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Fuel Building Ventilation System (FBVS)	Maintain Ambient Conditions for EBS and FPCS pump rooms (Recirculation Coolers)	The FBVS has an safety-related function that maintains the room ambient conditions in the extra borating system pump rooms and fuel pool cooling system pump rooms during normal operation, abnormal operation, and postulated accident events (GDC 27, GDC 60, GDC 61).	NO	N/A	N/A	The I&C associated with the FBV system is described in Section 9.4.2.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 15 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Fuel Pool Cooling and Purification System (FPCPS)	Fuel Pool Cooling Pump Trip On Low SFP Level	The FPCPS has a safety-related function to: 1. Remove decay heat from the spent fuel pool during normal plant operation, outages, and design basis events. 2. Provide containment isolation by closure of the reactor pool purification supply and return containment isolation valves. 3. Preclude, by design, the drain down of the spent fuel pool (SFP) below its required level to verify that the spent fuel remains covered with water during storage conditions. 4. Provide SFP make-up capability (Seismic Category I water sources, pump, and piping) to compensate for normal SFP evaporation for up to seven days.	NO	N/A	N/A	The I&C associated with the FPCPS is described in Section 9.1.3.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 16 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
		5. Provide isolation capability of non-safety-related FPCPS piping from the reactor building transfer compartment, the fuel building transfer compartment and cask loading pit (per 10 CFR 50.34(a)(1) or 10 CFR 100.11). The safety-related function to trip the FPC pump on low level verifies that the FPCPS is capable of fulfilling its safety-related function of precluding the drain down of the SFP to eliminate the potential for fuel damage and its consequences.				

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 17 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
In-Containment Refueling Water Storage Tank System (IRWST)	IRWST Boundary Isolation for Preserving IRWST Water Inventory	The IRWST has a safety-related function to isolate the IRWST for purposes of preserving the IRWST water inventory to support the safety-related function of controlling core reactivity (via safety injection) by closing the IRWST isolation valves. This preserves IRWST inventory for long term availability of safety injection, given a pipe failure in a connected non-safety related system.	Interdivisional communications is required because an IRWST low level discrete signal is generated in each division, and 2/4 voting logic is used to close IRWST isolation valves in Division 1 and 4.	Discrete	Vote	The I&C associated with the IRWST is described in Section 6.3.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 18 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Main Control Room Air Conditioning System (CRACS)	Iodine Filtration Train Heater Control	The CRACS has an safety-related function to preheat the inlet air in order to reduce the airborne moisture prior to entry into the carbon bed within the filter unit. Carbon filter heaters shut down when the respective inlet or outlet dampers are not fully open. The heaters will turn off if the carbon filtration unit fan stops, the carbon filter inlet isolation damper is not open or the carbon filter outlet isolation damper is not open.	NO	N/A	N/A	The I&C associated with the CRACS systems is described in Sections 6.5.1 and 9.4.1.
Main Control Room Air Conditioning System (CRACS)	Heater Control for Outside Inlet Air	The CRACS has an safety-related function to preheat the outside air to verify that the inlet air temperature is not less than 37°F (GDC 19). Inlet air which bypasses the iodine filtration unit is heated by an electric heater for temperature control. Heating of the outside air is performed by multi-stage heaters located in each outside air intake duct.	NO	N/A	N/A	The I&C associated with the CRACS systems is described in Sections 6.5.1 and 9.4.1.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 19 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Main Control Room Air Conditioning System (CRACS)	Pressure Control	The CRACS has safety-related function to verify the MCR is maintained at a positive pressure with respect to the ambient air pressure in adjacent areas (GDC 19). Differential pressure sensors sense the pressure difference between the MCR and the pressure in a reference space.	NO	N/A	N/A	The I&C associated with the CRACS systems is described in Sections 6.5.1 and 9.4.1.
Main Control Room Air Conditioning System (CRACS)	Cooler Temperature Control	The CRACS has safety-related functions that verifies that the air supply temperature is maintained within the preset temperature range (GDC 19). A control signal is developed when the supply air temperature exceeds a preset temperature set point of 58°F. The control signal is used to adjust cooler outlet SCWS control valves to maintain the air supply temperature.	NO	N/A	N/A	The I&C associated with the CRACS systems is described in Sections 6.5.1 and 9.4.1.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 20 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Standby Position Control	The MSS has a safety-related function supporting the removal of decay heat and other residual heat from the reactor core (GDC 34). The function modulates the MSRCV to its standby control position, so in the event of an overpressure transient the MSRCVs will already be in its required relieving position.	NO	N/A	N/A	The I&C associated with the MSS is described in Sections 7.3 and 10.3.
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Pressure Control	The MSS has a safety-related function supporting the removal of decay heat and other residual heat from the reactor core (GDC 34). The function modulates the MSRCV to its required position in order to reduce secondary side pressure of the steam generators during overpressure events.	The MSRIV closed position is detected via 2 out of 4 voting (the position switches are associated with Div 1 through 4).	Discrete	Vote	The I&C associated with the MSS is described in Sections 7.3 and 10.3.
Safeguard Building Controlled-Area Ventilation System (SBVS)	SIS/RHRS Pump Rooms Heat Removal	The SBVS has an safety-related function that maintains ambient conditions for safety-related components during normal operation (GDC 60, GDC 61).	NO	N/A	N/A	The I&C associated with the SBVS system is described in Section 9.4.5.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 21 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safeguard Building Controlled-Area Ventilation System (SBVS)	SIS/RHRS Valve Rooms Heat Removal	The SBVS has an safety-related function that maintains ambient conditions for safety-related components during normal operation (GDC60, GDC61).	NO	N/A	N/A	The I&C associated with the SBVS system is described in Section 9.4.5.
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply and Recirculation Exhaust Air Flow Control	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Supply and Recirculation Exhaust Air Flow Control function supports this system safety function by controlling supply, exhaust, and recirculation flow as required to maintain ambient temperature and air quality (via filtration) within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 22 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Fan Safe Shut-off	The SBVSE has an safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). An inadvertent stopping of the supply fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603).	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 23 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Recirculation/ Exhaust Fan Safe Shut-off	The SBVSE has an safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). An inadvertent stopping of the recirculation/exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603).	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 24 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Exhaust Fan Safe Shut-off	The SBVSE has an safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). An inadvertent stopping of the exhaust fan, due to a spurious system action, may cause the SBVSE for a given division to become inoperable. Therefore, to mitigate the risk of system spurious actions, this function is to be designated as safety-related (IEEE 603).	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 25 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Air Temperature	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Supply Air Temperature function supports this system safety function by maintaining supply air temperature (downstream of heaters) as required to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 26 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Freeze Protection – Supply Air Temperature	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Freeze Protection Supply Air Temperature function supports this system safety function by maintaining supply air temperature (downstream of heaters) as required to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 27 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Freeze Protection – Heat Tracing	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Freeze Protection - Heat Tracing function supports this system safety function by preventing ice build-up on the louver bars (i.e. mitigating the risk of not having available makeup air).	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 28 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Air Temperature Control for Cooling	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Supply Air Temperature Control for Cooling function supports this system safety function by maintaining a constant air temperature as required to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 29 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Air Temperature Control for Supply Air Heating	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Supply Air Temperature Control for Supply Air Heating function supports this system safety function by maintaining a minimal air temperature as required to maintain ambient temperature within applicable limits for safety-related equipment located within the Safeguard Building areas and rooms.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 30 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Battery Room Temperature Control	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Battery Room Temperature Control function supports this system safety function by maintaining battery room ambient temperature within applicable limits.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Battery Room Supply Air Temperature	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Battery Room Supply Air Temperature function supports this system safety function by maintaining battery room ambient temperature within applicable limits.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 31 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Emergency Feedwater Pump Room Heat Removal	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Emergency Feedwater Pump Room Heat Removal function supports this system safety function by removing heat from the pump room and maintaining room temperature within a temperature band for safety-related equipment.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 32 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Component Cooling Water System Rooms Heat Removal	The SBVSE has a safety-related function to ventilate and maintain acceptable ambient temperature in the Safeguard Building areas and rooms ventilated by the system (GDC 4, GDC 17). The Component Cooling Water System Rooms Heat Removal function supports this system safety function by removing heat from the applicable rooms and maintaining room temperature within a temperature band for safety-related equipment.	NO	N/A	N/A	The I&C associated with the SBVSE is described in Section 9.4.6.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 33 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between trains (due to system faults - e.g., low evaporator flow) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 34 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between trains (due to system faults - e.g., low evaporator flow) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 35 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions per (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between trains (due to system faults - e.g., low evaporator flow) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 36 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between trains (due to system faults - e.g., low evaporator flow) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 37 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on Train 1 Chiller Black Box Internal Fault	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between trains (due to system faults - chiller black box internal fault) an auto-start of the standby train occurs. A verification of prerequisites is required to provide reasonable assurance that the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 38 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 2 to Train 1 Switchover on Train 2 Chiller Black Box Internal Fault	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between trains (due to system faults - chiller black box internal fault) an auto-start of the standby train occurs. A verification of prerequisites is required to provide reasonable assurance that the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 39 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 3 to Train 4 Switchover on Train 3 Chiller Black Box Internal Fault	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between trains (due to system faults - chiller black box internal fault) an auto-start of the standby train occurs. A verification of prerequisites is required to provide reasonable assurance that the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 40 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 4 to Train 3 Switchover on Train 4 Chiller Black Box Internal Fault	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between trains (due to system faults - chiller black box internal fault) an auto-start of the standby train occurs. A verification of prerequisites is required to provide reasonable assurance that the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 41 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 2 to Train 1 Switchover on Loss of Ultimate Heat Sink (LUHS)/ CCWS	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between Trains (due to an external system fault (loss of CCW = LUHS)) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 42 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 3 to Train 4 Switchover on Loss of Ultimate Heat Sink (LUHS)/ CCWS	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between Trains (due to an external system fault (loss of CCW = LUHS)) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 43 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on LOOP Re-start Failure	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions per (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between trains (re-start failure of the previous operating train or with its corresponding EDG) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 44 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 2 to Train 1 Switchover on LOOP Re-start Failure	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 1 is associated with Div 1 and Train 2 with Div 2. Div 1 and Div 2 are cross connected. When switching between trains (re-start failure of the previous operating train or with its corresponding EDG) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 45 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 3 to Train 4 Switchover on LOOP Re-start Failure	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between trains (re-start failure of the previous operating train or with its corresponding EDG) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 46 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Train 4 to Train 3 Switchover on LOOP Re-start Failure	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The automatic switchover function verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	Train 3 is associated with Div 3 and Train 4 with Div 4. Div 3 and Div 4 are cross connected. When switching between trains (re-start failure of the previous operating train or with its corresponding EDG) an auto-start of the standby train occurs. A verification of prerequisites is required to make sure the on-coming train is in ready standby mode and that the appropriate cross-tie valves are in the open position.	Discrete	Vote	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 47 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Chilled Water System (SCWS)	SCWS Chiller Evaporator Water Flow Control (Trains 1 and 4)	The SCWS has an safety-related function 1) to transfer heat loads from safety-related SSC to a heat sink under both normal operating and accident conditions, 2) component redundancy for performance of safety functions assuming a single, active component failure coincident with the loss of offsite power, and 3) the capability to isolate components, systems, or piping, if required, so system safety functions are not compromised. The SCWS Chiller Evaporator Water Flow Control function prevents freezing at the evaporator coil and therefore, verifies that the SCWS is capable of fulfilling these safety-related functions (GDC 44).	NO	NA	NA	The I&C associated with the SCWS is described in Section 9.2.8.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 48 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Injection and Residual Heat Removal System (SIS/RHRS)	Automatic RHRS Flow Rate Control	The SIS/RHRS has a safety-related function to provide the RCS RHR in order to reach cold shutdown, refueling modes and to control primary temperature. The function to automatically control the flow rate of the RHRS supports the safety-related function of providing RHR by modulating the bypass control valve ensuring a constant flow rate through the LHSI pump.	NO	NA	NA	The I&C associated with the SIS/RHRS is described in Section 5.4.7 and 6.3.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 49 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Injection and Residual Heat Removal System (SIS/RHRS)	Automatic Trip of LHSI Pump (in RHR Mode) on Low ΔPsat	The SIS/RHRS has a safety-related function to provide the RCS RHR in order to reach cold shutdown, refueling modes and to control primary temperature. The function to automatically trip the LHSI pump upon a low ΔPsat signal supports the safety-related function of providing RHR by maintaining LHSI pump operability by shutting down the pump to prevent pump damage due to inadequate NPSH or unavailability due to steam binding following a failure that results in RCS conditions approaching saturation.	Interdivisional communications is required because a low ΔPsat discrete signal is generated in each division, and 2/4 voting logic is used to trip the LHSI pump.	Discrete	Vote	The I&C associated with the SIS/RHRS is described in Section 5.4.7 and 6.3.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function (Sheet 50 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Injection and Residual Heat Removal System (SIS/RHRS)	Automatic Trip of LHSI Pump (in RHR Mode) on Low Loop Level	The SIS/RHRS has a safety-related function to provide the RCS RHR in order to reach cold shutdown, refueling modes and to control primary temperature. The function to automatically trip the LHSI pump upon a low RCS loop level signal supports the safety-related function of providing RHR by maintaining LHSI pump operability by shutting down the pump to prevent pump damage or unavailability due to air binding following a failure that results in low RCS loop level.	Interdivisional communications is required because a low RCS loop level discrete signal is generated in each division, and 2/4 voting logic is used to trip the LHSI pump.	Discrete	Vote	The I&C associated with the SIS/RHRS is described in Section 5.4.7 and 6.3.

442, 07.09-64

Table 7.4-1—SAS Automatic Safety Function
(Sheet 51 of 51)

System[1]	Function Name[2]	Function Safety Basis[3]	Interdivisional Communications[4]	Type of Data[5]	Signal Selection Type[6]	FSAR Section Referenced
Safety Injection and Residual Heat Removal System (SIS/RHRS)	LHSI Valves Actuation Based on RHRS Alignment	The SIS/RHRS has a safety-related function to provide RCS RHR in order to reach the cold shutdown, refueling modes and to control primary temperature. The function to actuate the LHSI valves supports the safety-related function of RHR by closing the LHSI suction isolation, radial miniflow line check, and tangential miniflow check valves upon RHRS alignment to the RCS thereby preventing diversion of water from the RCS to the IRWST.	NO	NA	NA	The I&C associated with the SIS/RHRS is described in Section 5.4.7 and 6.3.

Notes:

1. System – Mechanical system described in the referenced FSAR section.
2. Function Name – The automatic safety-related function is controlled by SAS in each mechanical system.
3. Function Safety Basis – Safety-related functions that provide reasonable assurance of either:
   - The integrity of the reactor coolant pressure boundary.
   - The capability to shut down the reactor and maintain it in a safe shutdown condition.

442, 07.09-64

– The capability to prevent or mitigate the consequences of accidents that could result in potential offsite exposures.

4. Interdivisional Communication – Point-to-point data communications between different safety divisions of SAS.

5. Type of Data – Analog or Discrete Signal.

6. Signal Selection Type – Vote means if two or more out of the four (or three) inputs are TRUE, then the output will be TRUE, otherwise output is FALSE.

442, 07.09-64

Next File

7.6 Interlock Systems Important to Safety

7.6.1 Description

This section describes the interlock functions important to safety that reduce the probability of occurrence of specific events, or maintain safety systems in a state that provides reasonable assurance of their availability. These interlocks are provided by instrumentation and control (I&C) functions designed to:

- Prevent over-pressurization of the residual heat removal (RHR) system when reactor coolant system (RCS) pressure and temperature are higher than the allowable values for RHR connection.
- Maintain the availability of the safety injection (SI) accumulators above specific RCS pressure conditions.
- Maintain separation between redundant component cooling water system (CCWS) trains.
- Prevent over-pressurization of the RCS and connected RHR system in case of SI actuation during low temperature operations.

7.6.1.1 System Description

The control logic for these interlock functions is processed by the protection system (PS), with the exception of the interlocks to maintain separation between redundant CCWS trains. The control logic for the CCWS interlocks is processed by the safety automation system (SAS). The relevant control logic for each function is described in Section 7.6.1.2.

When plant conditions dictate that an interlock be activated, the interlock signal is sent from the PS or SAS to the priority and actuator control system (PACS). While the interlock signal is present, the PACS prevents an override of the interlock by actuation or control orders having a lower priority than the interlock function. When plant conditions are such that an interlock can be removed, the PS or SAS removes the interlock signal and the PACS allows the actuator to be influenced by other control systems. Further discussion of the operation of the PACS is presented in Section 7.1.

The capability to perform manual actions related to these interlocks (i.e., acknowledgement of permissive signal status) is provided on ~~both the process information and control system (PICS) and~~ the safety information and control system (SICS). ~~Manual actions taken from the SICS have priority over those from the PICS as described in Section 7.1.~~

442, 07.09-64

7.6.1.2 Functional Descriptions

7.6.1.2.1 RHR Suction Valve Interlocks

There are four 100 percent low head safety injection (LHSI) trains that can be aligned to perform the RHR function. Each train has connections to the hot and cold legs of an RCS loop. The RHR function is performed by forced flow with the LHSI pumps taking suction from the hot legs, cooling the water via the LHSI heat exchangers, and injecting into the cold legs.

The operation of the LHSI and RHR systems is described in Section 5.4.7.

In RHR mode, each LHSI train takes suction from its respective hot leg through two motor operated isolation valves in series (first and second RHR reactor coolant pressure boundary (RCPB) isolation valves). These isolation valves are interlocked to prevent their opening when RCS pressure and temperature have not decreased below acceptable values. These acceptable values are the permissive P14 pressure and temperature thresholds.

When RCS pressure ~~or~~ and temperature ~~is~~are above the P14 threshold, the PS provides constant signals to hold the RHR RCPB isolation valves closed. After pressure and temperature decrease below the thresholds, the operator is prompted to manually acknowledge P14 which allows the isolation valves to be opened to connect RHR.

Generation of the P14 permissive signal is described in Section 7.2.1.3.

Two redundant actuation logic units (ALU) within a PS division each send the interlock signal to one isolation valve in each of two RHR trains (i.e., PS ~~d~~Division 1 holds closed a single valve on ~~t~~Train ~~one~~1 and a single valve on ~~t~~Train ~~two~~2. Division ~~two~~2 of the PS holds closed a single valve on ~~t~~Train ~~two~~2 and a single valve on ~~train one~~Train 1). This arrangement precludes a single failure from allowing opening of both interlocked isolation valves on any one RHR train. Additionally, no single failure can prevent the operator from aligning the isolation valves, on at least one suction line, for RHR after RCS pressure and temperature requirements are satisfied.

442, 07.09-64

Independence and diversity are provided between the interlocks of the two valves on each suction line to prevent their opening unless RCS pressure and temperature ~~is~~are below the RHR system design pressure. Independence is maintained between the two divisions of the PS that each provide the interlock to one of the two valves. Measures used to establish independence between redundant safety divisions are described in Section 7.1. Diversity is achieved by the fact that both RCS pressure and temperature measurements must be below the P14 setpoint values before the valves can be opened. Additionally, the operator is prompted to acknowledge the P14 condition, providing a third diverse condition that must be satisfied to allow valve opening.

When RHR is connected, an inadvertent increase in RCS pressure does not result in an automatic signal to close the RHR RCPB isolation valves. However, the following design features prevent an increasing pressure from exceeding the RHR system design pressure:

- Interlock holding the MHSI large miniflow lines open (see Section 7.6.1.2.4).
- Pressurizer safety relief valves operating in their LTOP mode (see Section 7.3.1.2.13).
- Spring loaded safety valves on the RHR suction lines.

During an intentional increase in pressure, when ~~either~~ RCS temperature ~~or~~and pressure exceed the P14 setpoint, the operator is prompted to acknowledge P14, and is then allowed to close the RHR RCPB isolation valves.

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P14 permissive ~~P14~~ signal. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Open or closed position of first RHR RCPB isolation valve (each train).
- Open or closed position of second RHR RCPB isolation valve (each train).

7.6.1.2.2 Safety Injection Accumulator Interlocks

There are four accumulators, one associated with each of the four independent SIS trains. Borated water is injected into the RCS from the accumulators when RCS pressure falls below the internal pressure of the accumulators.

The operation of the SI accumulators is described in Section 6.3.

442, 07.09-64

Each accumulator is connected to the cold leg injection line of its respective RCS loop through two check valves and a motor operated isolation valve in series. Each isolation valve is interlocked to remain open above a specified RCS pressure value. This pressure value is the ~~permissive~~ P12 permissive threshold.

Generation of the P12 permissive signal is described in Section 7.2.1.3.

Normally, the operator opens the isolation valves when RCS pressure exceeds accumulator pressure. Regardless, when RCS pressure increases above the P12 permissive threshold, the PS provides automatic signals to open the accumulator isolation valves. Once the valves are verified to be in the open position, control power is removed from the valves to prevent inadvertent closure. During a normal decrease in pressure, power is restored to the valves at a point in time determined by the operating procedures. Then, after RCS pressure decreases below the P12 permissive

threshold, the operator is prompted to manually acknowledge the P12 permissive, which allows the isolation valves to be closed before RCS pressure is reduced below the accumulator pressure.

A pressure region exists below the P12 permissive pressure threshold where the accumulators are required to be available but Plant Technical Specifications allow an accumulator isolation valve to be closed for a short period of time. To accommodate operation in this pressure region, an automatic 'open' signal is sent to the accumulator isolation valves when an SIS actuation occurs. The SIS actuation function is described in Section 7.3.1.2.

Two redundant ALU within a division send the automatic opening signal to the isolation valve of the corresponding accumulator (i.e., PS ~~d~~Division ~~one~~1 opens the isolation valve related to the ~~t~~Train 1 accumulator). This arrangement precludes a single actuator logic unit (ALU) failure from preventing the opening of a valve. Any other single failure which could prevent opening of a valve, such as failure of a PACS module or of the valve itself, is detected immediately by failure of the valve to open. Corrective actions can then be taken before continued increase in pressure.

442, 07.09-64

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P12 permissive signal. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Pressure and level of each accumulator.
- Open or closed position of each accumulator isolation valve.

7.6.1.2.3 Interlocks Isolating Redundant CCWS Trains

The CCWS is comprised of four closed-loop, safety-related supply trains that function to cool and transfer heat load from safety users to the heat sink. The common loads cooled by the CCWS consist of two separate sets, referred to as Common-1 and Common-2. The Common-1 header is supplied by either CCW ~~train one~~Train 1 or ~~train two~~Train 2 while the Common-2 header is supplied by either CCW ~~t~~Train ~~three~~3 or ~~t~~Train ~~four~~4. Each common header is further divided into two sub-headers designated as Common 1a and 1b or Common 2a and 2b.

The operation of the CCWS is described in Section 9.2.2.

Interlocks are provided so that no two redundant CCWS trains are connected to the same common header at the same time. Each CCWS train is provided with four switchover valves to perform the required train separation.

CCWS ~~train one~~Train 1 has a single valve on the supply side and a single valve on the return side of Common 1a. Train ~~two~~2 also has a single valve on both the supply and

return sides of Common 1a. These valves are interlocked so that both valves (supply and return) on ~~train one~~Train 1 must be closed before either valve on ~~train two~~Train 2 can be opened. Likewise, both valves on ~~train two~~Train 2 must be closed before either valve on ~~train one~~Train 1 can be opened. The same valve arrangement and interlocks are provided relative to Common 1b to provide separation between ~~t~~Trains ~~one~~1 and ~~two~~2, and on Common 2a and 2b to provide separation between ~~t~~Trains ~~three~~3 and ~~four~~4. The functional logic for the switchover valve interlock is shown in Figure 7.6-1.

Another interlocking function is required concerning the cooling paths of the Common 1b and Common 2b headers toward the reactor coolant pump (RCP) thermal barriers. Either the Common 1b or 2b headers can provide cooling to the RCP thermal barriers. To maintain strict CCWS train separation, ~~the~~ one of the supply containment isolation valves (CIV) and one of the return CIVs on the RCP thermal barriers cooling path must be closed on the header being removed from service (1b or 2b) prior to opening the CIVs on the header being placed in service (2b or 1b, respectively).~~on the supply and return side of Common 1b cannot be opened unless the CIVs on both the supply and return side of Common 2b are closed, and vice versa.~~ The functional logic for the CIV interlock is shown in Figure 7.6-2.

442, 07.09-64

The interlock functions maintaining separation between redundant CCWS trains are performed by the SAS. Each switchover valve is assigned to a SAS division based on the CCWS train it belongs to (i.e., switchover valves on ~~train one~~Train 1 are assigned to SAS ~~d~~Division ~~one~~1). Each division of SAS acquires position information from the valves to which it is assigned, and controls those same valves. In any SAS division, the information about the position of valves in other trains that is needed to control a switchover valve is provided via network connection by the SAS division which acquires the information. For example, the positions of the ~~train two~~Train 2 valves on the supply and return of Common 1a are acquired by SAS ~~d~~Division ~~two~~2. This information is ~~transmitted~~provided via a network connection to SAS ~~d~~Division ~~one~~1 to perform the interlock function for the ~~train one~~Train 1 valves on the supply and return of Common 1a.

The interlock function concerning the CIVs is also performed by the SAS, but is only performed in ~~d~~Divisions ~~one~~1 and ~~four~~4. The CIVs are assigned to SAS divisions for control based on which electrical division provides power to the valves (i.e., valves powered by electrical ~~d~~Division ~~one~~1 are controlled by SAS ~~d~~Division ~~one~~1). The closed position indications of the CIVs on Common 1b are used to allow opening of the CIVs on Common ~~1a~~2b, and vice versa.

Redundant SAS controllers are provided in each division, and redundant networks are used between the divisions so that no single failure within the SAS can result in inadvertent connection of redundant CCWS trains. Each valve is equipped with redundant open/closed position sensors so that a single sensor failure does not result in

inadvertent connection of redundant CCWS trains. While each switchover valve is controlled by one ~~I&C~~SAS division, ~~multiple~~ PACS modules in ~~that~~ multiple divisions, acting on multiple solenoid devices, are required in order to change the position of a switchover valve. Therefore, a single PACS module failure does not result in inadvertent connection of redundant CCWS trains. For the CIV interlock, redundancy is obtained through the use of inner and outer CIVs, each controlled by a different division of ~~I&C~~SAS.

The single failure tolerance of the CCWS with respect to availability of the required cooling function is encompassed within the redundancy of the mechanical system design, as described in Section 9.2.2.

The following indications are provided to the operator relative to th~~is~~ese interlocks:

- Indication of open or closed position of each interlocked valve.
- Alarm indicating position conflict between supply and return switchover valve of the same CCWS train relative to the same common header.
- Alarm indicating position conflict between CIVs of the same common header.
- Alarm indicating connection of two CCWS trains to the same common header.

442, 07.09-64

7.6.1.2.4 Interlocks to Provide Low Temperature Over-Pressure Protection

Section 5.2.2 describes LTOP for the U.S. EPR design. Low temperature RCPB overpressure events include mass input events and heat input events. A start of four medium head safety injection (MHSI) pumps with one large miniflow line isolation valve failed into the closed position is the limiting case.

The ~~medium head safety injection (~~MHSI~~)~~ pumps are used to inject borated water from the in-containment refueling water storage tank (IRWST) into the cold legs when a safety injection signal is present. A large miniflow line branches off from the discharge side of each MHSI pump and provides a path, through a motor operated isolation valve, to the IRWST. These isolation valves are interlocked in the open position during low temperature operations to reduce the MHSI injection pressure.

The interlock holding open the MHSI large miniflow lines serves two purposes:

- Protection against brittle fracture of the reactor pressure vessel (RPV).
- Protection of the RHR system from over-pressurization when it is connected to the RCS.

Brittle Fracture Protection:

The PSRVs ultimately provide protection against brittle fracture of the RPV. However, the PSRV setpoints and sizing are based on the pressure and flow rates of four MHSI pumps, with one large miniflow line failed closed, injecting into the RCS. For this reason, below the P17 permissive temperature threshold, the large miniflow line isolation valves are interlocked in the open position to make brittle fracture protection via the PSRVs effective. Actuation of the PSRVs by the PS in an LTOP capacity is described in Section 7.3.

RHR System Protection:

The RHR system can only be connected to the RCS below the P14 RCS temperature value. Below the P14 permissive temperature, over-pressure protection of the RHR system is provided differently in two different RCS temperature regimes, as described below. In both temperature regimes, a start of four MHSI pumps with one MHSI large miniflow line valve failed into the closed position is representative of the limiting pressure addition event.

P14 temperature > RCS temperature > P17 temperature

When the P14 permissive is validated and one or more trains of RHR are connected to the RCS, the MHSI large miniflow lines are interlocked in the open position. The RHR spring-loaded safety valves along with the interlock holding the large miniflow lines open provide over-pressure protection of the RHR system in this temperature regime.

442, 07.09-64

During the postulated pressure addition event, by the time RCS pressure reaches the RHR safety valve opening setpoint, the three MHSI pumps with open large miniflow lines are no longer able to inject due to a higher RCS pressure caused by the single MHSI pump with its large miniflow line valve closed. Therefore the other three MHSI pumps re-circulate through their miniflow lines to the IRWST. This leaves the one MHSI pump with its (failed) closed large miniflow line injecting into the RCS. The RHR spring loaded safety valves are sized based on the pressure and flow rate of one MHSI pump, with large miniflow line closed, injecting into the RCS while RHR is connected.

P17 temperature > RCS temperature

When the P17permissive is validated, the MHSI large miniflow valves are interlocked in the open position. The PSRVs operating in their LTOP mode along with the interlock holding the large miniflow lines open provide over-pressure protection of the RHR system in this temperature regime.

The LTOP setpoints for opening of PSRVs are lower than the RHR spring-loaded safety valve setpoints. Therefore, during the postulated pressure addition event, the

PSRVs relieve pressure ~~well~~ before the design pressure of the connected RHR system is reached. The PSRV setpoints and sizing are based on the pressure and flow rate of four MHSI pumps, with one miniflow line closed, injecting into the RCS. Actuation of the PSRVs by the PS in an LTOP capacity is described in Section 7.3.

Generation of the P14 and P17 permissive signals is described in Section 7.2.1.3.

Detection of the RHR connected condition is shown in Figure 7.6-3.

Two redundant ALU within a PS division each send the interlock signal to the large miniflow line isolation valve of one MHSI train. This arrangement precludes a single ALU failure from preventing the opening of a valve. The failure of a single PACS module or of a single valve results in one MHSI large miniflow line being closed, which is accounted for in the design of the RHR safety valves and PSRVs as previously described.

442, 07.09-64

Additionally, no single failure can prevent the isolation valve from being closed on at least one MHSI injection path during power operation when maximum MHSI discharge pressure is required.

The operational status of the PS on a divisional basis is provided to the operator. Indications and alarms are provided to the operator regarding the state of the P14 and P17 permissives. Additionally, the following indications are provided to the operator to verify correct operation of the interlock:

- Open or closed position of each MHSI large miniflow line isolation valve (each train).
- Status of MHSI pump (on or off, each train).
- Open or closed position of each valve as shown in Figure 7.6-3.

7.6.2 Analysis

The analysis provided in this section pertains to the I&C functionality related to interlocks important to safety, or supports U.S. EPR compliance with requirements at the plant level. Compliance of specific mechanical configurations or valves and piping with applicable codes and standards is addressed in the appropriate sections identified in Section 7.6.1.

7.6.2.1 Compliance to Applicable Criteria

7.6.2.1.1 Compliance to the Single Failure Criterion (Clause 5.1 of IEEE Std 603-1998)

The interlocks important to safety are designed to satisfy the single failure criteria. Specific aspects of single failure accommodation are described as part of the functional

description of each interlock in Section 7.6.1.2. Accommodation of single failures at the system level for the PS, SAS, and PACS is described in Section 7.1.

Accommodation of single failures at the system level for the mechanical safety systems described in this chapter is addressed in the relevant sections identified in Section 7.6.1.2.

7.6.2.1.2 Compliance to Requirements for Quality of Components and Modules (Clause 5.3 of IEEE Std 603-1998 and Clause 5.3 of IEEE 7-4.3.2-2003)

Components and modules that are required to perform the interlocking functions described in this section are classified as safety-related. They are designed to Class 1E standards and are applied in accordance with a stringent quality assurance program. Software used in these functions is developed and applied in accordance with a safety-related software program. Further discussion of safety-related I&C system conformance to requirements for quality is found in Section 7.1.

7.6.2.1.3 Compliance to Requirements for Independence (Clauses 5.6 and 6.3 of IEEE Std 603-1998)

Redundant divisions of the safety-related I&C systems are independent from one another so that a failure in any one portion of the system does not prevent the redundant portions from performing their function. Both electrical and communication independence are maintained as described in Section 7.1.

I&C equipment required to perform the interlock functions described in this section is independent from the effects of design basis events. The computerized portions of the safety systems are located in areas that are not subject to degraded environmental conditions as the result of an event. Equipment that may be located in areas subject to a degraded environment (e.g., sensors) is required to be qualified to operate in the expected post-event conditions. Environmental qualification of instrumentation and control equipment is discussed in Section 3.11 and Section 7.1.

The PS and SAS do not rely on input from non-safety-related systems to perform the interlock functions described in this section. Certain sensor measurements are used as inputs to both a safety-related interlock function, and a non-safety-related control function performed by a non-safety-related I&C system. In these cases, the signal conditioning and distribution system (SCDS) is provided to condition (if necessary) and distribute signal inputs needed within multiple DCS subsystems. ~~the measurement is acquired by the signal conditioning of the safety-related system, is multiplied, and then passed to the non-safety-related system through an electrically isolated connection.~~

442, 07.09-64

7.6.2.1.4 Compliance to Requirements for System Testing and Inoperable Surveillance

Surveillance of the safety-related I&C systems consists of overlapping tests to verify performance of the interlock function from sensor to PACS module.

Sensors and acquisition circuits are periodically tested. The input channel to be tested is placed in a lockout condition, and the downstream logic is automatically modified to disregard the input under test and maintain the interlock function in its current state.

The computerized portions of the safety systems are continuously monitored through self-testing during power operation. During outages, extended computer self-testing is performed to verify functionality that cannot be tested with the reactor at power.

442, 07.09-64

With respect to the connections between the output circuits of the PS and SAS and the PACS modules, and to the actuators themselves, surveillance of interlocking functions during power operations can be satisfied by observing the correct interlocked position of the actuators.

The safety-related I&C systems are designed to provide bypassed and inoperable status information to the operator. Sufficient indications are provided to the operator to evaluate the status of each interlock as described in the relevant functional descriptions in Section 7.6.1.2.

7.6.2.1.5 Conformance to Guidance Regarding the Use of Digital Systems (IEEE 7-4.3.2-2003)

The interlock functions described in this section are implemented in I&C systems using the TELEPERM XS platform, which is approved for use in safety systems of nuclear power generating stations in the United States. These systems are implemented in architectures designed to satisfy requirements applicable to all safety-related I&C systems, digital or otherwise.

Implementation of safety-related I&C systems is governed by the requirements of IEEE Std 603-1998 (Reference 1). Guidance on the use of digital computers in safety systems is provided by IEEE 7-4.3.2-2003 (Reference 2). Conformance to these standards is described in Section 7.1.

7.6.3 References

1. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 1998.

2. IEEE 7.4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," Institute of Electrical and Electronics Engineers, 2003.

Next File