ArevaEPRDCPEm Resource

From: WILLIFORD Dennis (AREVA) [Dennis.Williford@areva.com]
Sent: Tuesday, February 14, 2012 5:31 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy (AREVA); CRIBB Arnie (EXTERNAL AREVA); DELANO Karen (AREVA); HATHCOCK Phillip (AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); RYAN Tom (AREVA); HUDSON Greg (AREVA); MEACHAM Robert (AREVA)
Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Questions 7.1.37 - 7.1.41 and 7.3-38
Attachments: RAI 505 Questions 7.1.37 - 7.1.41 and 7.3-38 Response US EPR DC - DRAFT.pdf

Getachew,

Attached are DRAFT responses to Questions 7.1-37 (second draft), 7.1-41 (second draft) and 7.3-38 in RAI No. 505 (FSAR Ch. 7) in advance of the March 8, 2012 final date.

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

Thanks,

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

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, February 09, 2012 8:15 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 9

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. In Supplement 1 sent on October 27, 2011, and Supplement 2 sent on November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33. AREVA NP provided Supplement 3 on November 22, 2011 to provide a final response to 4 questions. On December 9, 2011, AREVA NP provided Supplement 4 to revise the schedule for 7 questions. On December 14, 2011, AREVA NP provided Supplement 5 to revise the schedule for 5 questions. On December 15, 2011, AREVA NP provided Supplement 6 to provide a complete and final response to 6 questions. On January 10, 2012, AREVA NP provided Supplement 7 to provide a complete and final response to 2 questions. On January 19, 2012, AREVA NP provided Supplement 8 to provide a complete and final response to one question and a revised preliminary schedule for the response to Question 07.01-33.

The schedule for a technically correct and complete response to 11 of the remaining 21 questions has been changed as provided below. The response schedule to the other 10 questions remains unchanged.

Question #	Response Date
RAI 505 — 07.01-33	February 21, 2012
RAI 505 — 07.01-34	April 5, 2012
RAI 505 — 07.01-35	April 26, 2012
RAI 505 — 07.01-36	**April 5, 2012**
RAI 505 — 07.01-37	March 8, 2012
RAI 505 — 07.01-38	**April 5, 2012**
RAI 505 — 07.01-39	**April 26, 2012**
RAI 505 — 07.01-40	**April 26, 2012**
RAI 505 — 07.01-41	**March 8, 2012**
RAI 505 — 07.01-44	**April 5, 2012**
RAI 505 — 07.01-45	April 26, 2012
RAI 505 — 07.01-46	April 26, 2012
RAI 505 — 07.01-47	**April 5, 2012**
RAI 505 — 07.01-48	**April 5, 2012**
RAI 505 — 07.01-49	**April 26, 2012**
RAI 505 — 07.01-50	April 26, 2012
RAI 505 — 07.01-51	**April 26, 2012**
RAI 505 — 07.03-38	**March 8, 2012**
RAI 505 — 07.05-10	March 8, 2012
RAI 505 — 07.08-47	April 26, 2012
RAI 505 — 07.09-71	April 5, 2012

Sincerely,

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

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, January 19, 2012 11:19 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 8

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. In Supplement 1 sent on October 27, 2011, and Supplement 2 sent on November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33. AREVA NP provided Supplement 3 on November 22, 2011 to provide a final response to 4 questions. On December 9, 2011, AREVA NP provided Supplement 4 to revise the schedule for 7 questions. On December 14, 2011, AREVA NP provided Supplement 5 to revise the schedule for 5 questions. On December 15, 2011, AREVA NP provided Supplement 6 to provide a complete and final response to 6 questions. On January 10, 2012, AREVA NP provided Supplement 7 to provide a complete and final response to 2 questions.

The attached file, "RAI 505 Supplement 8 Response US EPR DC.pdf" provides a technically correct and complete final response to 1 of the remaining 22 questions.

The following table indicates the respective pages in the response document, "RAI 505 Supplement 8 Response US EPR DC.pdf," that contain AREVA NP's response to the subject question.

Question #	Start Page	End Page
RAI 505 — 07.01-42	2	2

The schedule for a technically correct and complete response to the remaining 21 questions is provided below. The preliminary schedule for the response to Question 07.01-33 has been revised and is being reevaluated and a new supplement with a revised schedule will be transmitted by February 21, 2012.

Question #	Response Date
RAI 505 — 07.01-33	**February 21, 2012**
RAI 505 — 07.01-34	April 5, 2012
RAI 505 — 07.01-35	April 26, 2012
RAI 505 — 07.01-36	February 9, 2012
RAI 505 — 07.01-37	March 8, 2012
RAI 505 — 07.01-38	February 9, 2012
RAI 505 — 07.01-39	February 9, 2012
RAI 505 — 07.01-40	February 9, 2012
RAI 505 — 07.01-41	February 9, 2012
RAI 505 — 07.01-44	February 9, 2012
RAI 505 — 07.01-45	April 26, 2012
RAI 505 — 07.01-46	April 26, 2012
RAI 505 — 07.01-47	February 9, 2012
RAI 505 — 07.01-48	February 9, 2012
RAI 505 — 07.01-49	February 9, 2012
RAI 505 — 07.01-50	April 26, 2012
RAI 505 — 07.01-51	February 9, 2012
RAI 505 — 07.03-38	April 26, 2012
RAI 505 — 07.05-10	March 8, 2012
RAI 505 — 07.08-47	April 26, 2012
RAI 505 — 07.09-71	April 5, 2012

Sincerely,

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

From: WILLIFORD Dennis (CORP/QP)
Sent: Tuesday, January 10, 2012 5:21 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 7

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. In Supplement 1 sent on October 27, 2011, and Supplement 2 sent on November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33. AREVA NP provided Supplement 3 on November 22, 2011 to provide a final response to 4 questions. On December 9, 2011, AREVA NP provided Supplement 4 to revise the schedule for 7 questions. On December 14, 2011, AREVA NP provided Supplement 5 to revise the schedule for 5 questions. On December 15, 2011, AREVA NP provided Supplement 6 to provide a complete and final response to 6 questions.

The attached file, "RAI 505 Supplement 7 Response US EPR DC.pdf" provides technically correct and complete final responses to 2 of the remaining 24 questions. Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 505 Question 07.08-48.

The following table indicates the respective pages in the response document, "RAI 505 Supplement 7 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 505 — 07.08-44	2	3
RAI 505 — 07.08-48	4	5

The schedule for a technically correct and complete response to the remaining 22 questions has changed as provided below. The preliminary schedule for the response to Question 07.01-33 is being reevaluated and a new supplement with a revised schedule will be transmitted by January 25, 2012.

Question #	Response Date
RAI 505 — 07.01-33	January 25, 2012
RAI 505 — 07.01-34	**April 5, 2012**

RAI 505 — 07.01-35	**April 26, 2012**
RAI 505 — 07.01-36	**February 9, 2012**
RAI 505 — 07.01-37	**March 8, 2012**
RAI 505 — 07.01-38	**February 9, 2012**
RAI 505 — 07.01-39	**February 9, 2012**
RAI 505 — 07.01-40	**February 9, 2012**
RAI 505 — 07.01-41	**February 9, 2012**
RAI 505 — 07.01-42	**February 9, 2012**
RAI 505 — 07.01-44	**February 9, 2012**
RAI 505 — 07.01-45	**April 26, 2012**
RAI 505 — 07.01-46	**April 26, 2012**
RAI 505 — 07.01-47	**February 9, 2012**
RAI 505 — 07.01-48	**February 9, 2012**
RAI 505 — 07.01-49	**February 9, 2012**
RAI 505 — 07.01-50	**April 26, 2012**
RAI 505 — 07.01-51	**February 9, 2012**
RAI 505 — 07.03-38	**April 26, 2012**
RAI 505 — 07.05-10	**March 8, 2012**
RAI 505 — 07.08-47	**April 26, 2012**
RAI 505 — 07.09-71	**April 5, 2012**

Sincerely,

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

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, December 15, 2011 1:49 PM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 6

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. In Supplement 1 sent on October 27, 2011, and Supplement 2 sent on November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33. AREVA NP provided Supplement 3 on November 22, 2011 to provide a final response to 4 questions. On December 9, 2011, AREVA NP provided Supplement 4 to revise the schedule for 7 questions. On December 14, 2011, AREVA NP provided Supplement 5 to revise the schedule for 5 questions.

The attached file, "RAI 505 Supplement 6 Response US EPR DC.pdf" provides technically correct and complete responses to 6 of the remaining 30 questions. Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the responses. Also appended to this file are affected pages of Technical Reports ANP-10304 and ANP-10309P. Revisions to these Technical Reports will be submitted by separate letter after completion of all responses to RAI 505.

The following table indicates the respective pages in the response document, "RAI 505 Supplement 6 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 505 — 07.03-37	2	3
RAI 505 — 07.04-15	4	5
RAI 505 — 07.05-11	6	6
RAI 505 — 07.08-43	7	8
RAI 505 — 07.08-45	9	10
RAI 505 — 07.08-49	11	12

The schedule for a technically correct and complete response to the remaining 24 questions remains unchanged. The preliminary schedule for the response to Question 07.01-33 is being reevaluated and a new supplement with a revised schedule will be transmitted by January 25, 2012.

Question #	Response Date
RAI 505 — 07.01-33	January 25, 2012
RAI 505 — 07.01-34	January 10, 2012
RAI 505 — 07.01-35	February 9, 2012
RAI 505 — 07.01-36	January 10, 2012
RAI 505 — 07.01-37	January 19, 2012
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	January 10, 2012
RAI 505 — 07.01-40	January 10, 2012
RAI 505 — 07.01-41	January 10, 2012
RAI 505 — 07.01-42	January 10, 2012
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	February 9, 2012
RAI 505 — 07.01-46	February 9, 2012
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012
RAI 505 — 07.03-38	February 9, 2012
RAI 505 — 07.05-10	January 19, 2012
RAI 505 — 07.08-44	January 10, 2012
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012

RAI 505 — 07.09-71	January 10, 2012

Sincerely,

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

From: WILLIFORD Dennis (RS/NB)
Sent: Wednesday, December 14, 2011 11:30 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 5

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. In Supplement 1 sent on October 27, 2011, and Supplement 2 sent on November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33. AREVA NP provided Supplement 3 on November 22, 2011 to provide a final response to 4 questions. On December 9, 2011, AREVA NP provided a revised schedule for 7 questions.

The schedule for the response to four questions (Questions 7.1-35, 7.1-45, 7.1-46, and 7.3-38) is being changed, as indicated in bold below. In addition, the preliminary schedule for the response to Question 07.01-33 has been revised as indicated. This schedule is being reevaluated and a new supplement with a revised schedule will be transmitted by January 25, 2012. The schedule for a technically correct and complete response to the remaining 25 questions remains unchanged.

Question #	**Response Date**
RAI 505 — 07.01-33	**January 25, 2012**
RAI 505 — 07.01-34	January 10, 2012
RAI 505 — 07.01-35	**February 9, 2012**
RAI 505 — 07.01-36	January 10, 2012
RAI 505 — 07.01-37	January 19, 2012
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	January 10, 2012
RAI 505 — 07.01-40	January 10, 2012
RAI 505 — 07.01-41	January 10, 2012
RAI 505 — 07.01-42	January 10, 2012
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	**February 9, 2012**

RAI 505 — 07.01-46	**February 9, 2012**
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012
RAI 505 — 07.03-37	January 19, 2012
RAI 505 — 07.03-38	**February 9, 2012**
RAI 505 — 07.04-15	January 19, 2012
RAI 505 — 07.05-10	January 19, 2012
RAI 505 — 07.05-11	January 19, 2012
RAI 505 — 07.08-43	January 19, 2012
RAI 505 — 07.08-44	January 10, 2012
RAI 505 — 07.08-45	January 10, 2012
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012
RAI 505 — 07.08-49	January 19, 2012
RAI 505 — 07.09-71	January 10, 2012

Sincerely,

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

From: RYAN Tom (RS/NB)
Sent: Friday, December 09, 2011 8:35 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB); WILLIFORD Dennis (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Supplement 4

Getachew,

On September 29, 2011, AREVA NP Inc. provided a schedule for technically correct and complete responses to the 34 questions in RAI 505. On October 27, 2011, and November 17, 2011, AREVA NP provided a revised schedule for technically correct and complete responses to 33 questions and a preliminary revised schedule for Question 07.01-33. On November 22, 2011, AREVA NP provided a final response to four questions.

The schedule for the response to the questions 7.1-37, 7.3-37, 7.4-15, 7.5-10, 7.5-11, 7.8-43, and 7.8-49 is being changed and indicated in bold below, the remaining 23 questions remains unchanged, as indicated below. In addition, the preliminary schedule for a response to Question 07.01-33 remains unchanged. The

schedule for Question 07.01-33 is being reevaluated and a new supplement with a revised schedule will be transmitted by December 14, 2011.

Question #	Response Date
RAI 505 — 07.01-33	December 14, 2011
RAI 505 — 07.01-34	January 10, 2012
RAI 505 — 07.01-35	January 10, 2012
RAI 505 — 07.01-36	January 10, 2012
RAI 505 — 07.01-37	**January 19, 2012**
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	January 10, 2012
RAI 505 — 07.01-40	January 10, 2012
RAI 505 — 07.01-41	January 10, 2012
RAI 505 — 07.01-42	January 10, 2012
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	January 10, 2012
RAI 505 — 07.01-46	January 10, 2012
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012
RAI 505 — 07.03-37	**January 19, 2012**
RAI 505 — 07.03-38	January 10, 2012
RAI 505 — 07.04-15	**January 19, 2012**
RAI 505 — 07.05-10	**January 19, 2012**
RAI 505 — 07.05-11	**January 19, 2012**
RAI 505 — 07.08-43	**January 19, 2012**
RAI 505 — 07.08-44	January 10, 2012
RAI 505 — 07.08-45	January 10, 2012
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012
RAI 505 — 07.08-49	**January 19, 2012**
RAI 505 — 07.09-71	January 10, 2012

Sincerely,

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

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

Getachew,

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

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

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

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

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

Question #	Response Date
RAI 505 — 07.01-33	December 14, 2011
RAI 505 — 07.01-34	January 10, 2012
RAI 505 — 07.01-35	January 10, 2012
RAI 505 — 07.01-36	January 10, 2012
RAI 505 — 07.01-37	December 11, 2011
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	January 10, 2012
RAI 505 — 07.01-40	January 10, 2012
RAI 505 — 07.01-41	January 10, 2012
RAI 505 — 07.01-42	January 10, 2012
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	January 10, 2012

RAI 505 — 07.01-46	January 10, 2012
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012
RAI 505 — 07.03-37	December 11, 2011
RAI 505 — 07.03-38	January 10, 2012
RAI 505 — 07.04-15	December 11, 2011
RAI 505 — 07.05-10	December 11, 2011
RAI 505 — 07.05-11	December 11, 2011
RAI 505 — 07.08-43	December 11, 2011
RAI 505 — 07.08-44	January 10, 2012
RAI 505 — 07.08-45	January 10, 2012
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012
RAI 505 — 07.08-49	December 11, 2011
RAI 505 — 07.09-71	January 10, 2012

Sincerely,

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

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

Getachew,

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

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

Question #	Response Date
RAI 505 — 07.01-33	**December 14, 2011**
RAI 505 — 07.01-34	**January 10, 2012**
RAI 505 — 07.01-35	**January 10, 2012**
RAI 505 — 07.01-36	**January 10, 2012**
RAI 505 — 07.01-37	**December 11, 2011**
RAI 505 — 07.01-38	January 10, 2012
RAI 505 — 07.01-39	**January 10, 2012**
RAI 505 — 07.01-40	**January 10, 2012**
RAI 505 — 07.01-41	**January 10, 2012**
RAI 505 — 07.01-42	**January 10, 2012**
RAI 505 — 07.01-43	**December 11, 2011**
RAI 505 — 07.01-44	January 10, 2012
RAI 505 — 07.01-45	January 10, 2012
RAI 505 — 07.01-46	January 10, 2012
RAI 505 — 07.01-47	January 10, 2012
RAI 505 — 07.01-48	January 10, 2012
RAI 505 — 07.01-49	January 10, 2012
RAI 505 — 07.01-50	January 10, 2012
RAI 505 — 07.01-51	January 10, 2012
RAI 505 — 07.03-37	**December 11, 2011**
RAI 505 — 07.03-38	January 10, 2012
RAI 505 — 07.04-15	**December 11, 2011**
RAI 505 — 07.05-10	**December 11, 2011**
RAI 505 — 07.05-11	**December 11, 2011**
RAI 505 — 07.07-23	**December 11, 2011**
RAI 505 — 07.08-43	**December 11, 2011**
RAI 505 — 07.08-44	**January 10, 2012**
RAI 505 — 07.08-45	**January 10, 2012**
RAI 505 — 07.08-46	**December 11, 2011**
RAI 505 — 07.08-47	January 10, 2012
RAI 505 — 07.08-48	January 10, 2012
RAI 505 — 07.08-49	**December 11, 2011**
RAI 505 — 07.09-71	**January 10, 2012**
RAI 505 — 07.09-72	**January 10, 2012**

Sincerely,

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

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

Getachew,

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

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

Question #	Response Date
RAI 505 — 07.01-33	**November 17, 2011**
RAI 505 — 07.01-34	December 8, 2011
RAI 505 — 07.01-35	November 17, 2011
RAI 505 — 07.01-36	December 8, 2011
RAI 505 — 07.01-37	December 8, 2011
RAI 505 — 07.01-38	**January 10, 2012**
RAI 505 — 07.01-39	December 8, 2011
RAI 505 — 07.01-40	December 8, 2011
RAI 505 — 07.01-41	November 17, 2011
RAI 505 — 07.01-42	December 20, 2011
RAI 505 — 07.01-43	November 17, 2011
RAI 505 — 07.01-44	**January 10, 2012**
RAI 505 — 07.01-45	**January 10, 2012**
RAI 505 — 07.01-46	**January 10, 2012**
RAI 505 — 07.01-47	**January 10, 2012**
RAI 505 — 07.01-48	**January 10, 2012**
RAI 505 — 07.01-49	**January 10, 2012**
RAI 505 — 07.01-50	**January 10, 2012**
RAI 505 — 07.01-51	**January 10, 2012**
RAI 505 — 07.03-37	November 17, 2011
RAI 505 — 07.03-38	**January 10, 2012**
RAI 505 — 07.04-15	November 17, 2011
RAI 505 — 07.05-10	November 17, 2011
RAI 505 — 07.05-11	November 17, 2011
RAI 505 — 07.07-23	November 17, 2011
RAI 505 — 07.08-43	**January 10, 2012**
RAI 505 — 07.08-44	December 8, 2011

RAI 505 — 07.08-45	December 8, 2011
RAI 505 — 07.08-46	December 8, 2011
RAI 505 — 07.08-47	**January 10, 2012**
RAI 505 — 07.08-48	**January 10, 2012**
RAI 505 — 07.08-49	November 17, 2011
RAI 505 — 07.09-71	December 8, 2011
RAI 505 — 07.09-72	December 8, 2011

Sincerely,

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

From: WILLIFORD Dennis (RS/NB)
Sent: Thursday, September 29, 2011 11:04 AM
To: Getachew.Tesfaye@nrc.gov
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7

Getachew,

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

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

Question #	Start Page	End Page
RAI 505 — 07.01-33	2	2
RAI 505 — 07.01-34	3	3
RAI 505 — 07.01-35	4	4
RAI 505 — 07.01-36	5	5
RAI 505 — 07.01-37	6	6
RAI 505 — 07.01-38	7	7
RAI 505 — 07.01-39	8	8
RAI 505 — 07.01-40	9	9
RAI 505 — 07.01-41	10	10
RAI 505 — 07.01-42	11	11
RAI 505 — 07.01-43	12	12
RAI 505 — 07.01-44	13	13
RAI 505 — 07.01-45	14	14

RAI 505 — 07.01-46	15	15
RAI 505 — 07.01-47	16	16
RAI 505 — 07.01-48	17	18
RAI 505 — 07.01-49	19	19
RAI 505 — 07.01-50	20	20
RAI 505 — 07.01-51	21	22
RAI 505 — 07.03-37	23	23
RAI 505 — 07.03-38	24	24
RAI 505 — 07.04-15	25	25
RAI 505 — 07.05-10	26	26
RAI 505 — 07.05-11	27	27
RAI 505 — 07.07-23	28	28
RAI 505 — 07.08-43	29	29
RAI 505 — 07.08-44	30	30
RAI 505 — 07.08-45	31	31
RAI 505 — 07.08-46	32	32
RAI 505 — 07.08-47	33	33
RAI 505 — 07.08-48	34	34
RAI 505 — 07.08-49	35	35
RAI 505 — 07.09-71	36	36
RAI 505 — 07.09-72	37	37

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

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

Question #	**Response Date**
RAI 505 — 07.01-33	October 27, 2011
RAI 505 — 07.01-34	December 8, 2011
RAI 505 — 07.01-35	November 17, 2011
RAI 505 — 07.01-36	December 8, 2011
RAI 505 — 07.01-37	December 8, 2011
RAI 505 — 07.01-38	December 20, 2011
RAI 505 — 07.01-39	December 8, 2011
RAI 505 — 07.01-40	December 8, 2011
RAI 505 — 07.01-41	November 17, 2011
RAI 505 — 07.01-42	December 20, 2011
RAI 505 — 07.01-43	November 17, 2011
RAI 505 — 07.01-44	December 20, 2011
RAI 505 — 07.01-45	December 20, 2011
RAI 505 — 07.01-46	December 20, 2011
RAI 505 — 07.01-47	December 8, 2011
RAI 505 — 07.01-48	December 20, 2011

RAI 505 — 07.01-49	December 20, 2011
RAI 505 — 07.01-50	December 20, 2011
RAI 505 — 07.01-51	December 20, 2011
RAI 505 — 07.03-37	November 17, 2011
RAI 505 — 07.03-38	December 20, 2011
RAI 505 — 07.04-15	November 17, 2011
RAI 505 — 07.05-10	November 17, 2011
RAI 505 — 07.05-11	November 17, 2011
RAI 505 — 07.07-23	November 17, 2011
RAI 505 — 07.08-43	December 20, 2011
RAI 505 — 07.08-44	December 8, 2011
RAI 505 — 07.08-45	December 8, 2011
RAI 505 — 07.08-46	December 8, 2011
RAI 505 — 07.08-47	December 20, 2011
RAI 505 — 07.08-48	December 20, 2011
RAI 505 — 07.08-49	November 17, 2011
RAI 505 — 07.09-71	December 8, 2011
RAI 505 — 07.09-72	December 8, 2011

Sincerely,

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

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

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 12, 2011, and discussed with your staff on August 22 and 25, 2011. No change is made to the draft RAI as a result of those discussions. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 3746

Mail Envelope Properties (2FBE1051AEB2E748A0F98DF9EEE5A5D4AE917C)

Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7, Questions 7.1.37 - 7.1.41 and 7.3-38
Sent Date: 2/14/2012 5:30:46 PM
Received Date: 2/14/2012 5:30:49 PM
From: WILLIFORD Dennis (AREVA)

Created By: Dennis.Williford@areva.com

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

Post Office: auscharmx02.adom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	34142	2/14/2012 5:30:49 PM
RAI 505 Questions 7.1.37 - 7.1.41 and 7.3-38 Response US EPR DC - DRAFT.pdf	1457939	

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

Response to

Request for Additional Information No. 505 (5902,5735,5869,5754,5803,5950,5744), Revision 0, Questions 07.01-37, 07.01-41 and 07.03-38

8/30/2011

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

Application Section: FSAR Chapter 7

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

Question 07.01-37:

OPEN ITEM

Provide an ITAAC Item in U.S. EPR FSAR Tier 1, Section 2.4.4, that ties together satisfactory completion of the SAS ITAAC to completion of referenced ITAAC provided by the applicant in response to RAI 78, Questions 14.03.05-3&4 (Supplement 2).

IEEE Std. 603-1998, Clause 5.2, requires, in part, that the safety system design provide features to ensure that system-level actions go to completion. 10 CFR 52.47(b)(1) requires, in part, that ITAAC are necessary and sufficient to provide reasonable assurance that if the ITAAC are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. For the staff's review of compliance for SAS, the staff did not find an ITAAC item in Tier 1, Section 2.4.4, that verified SAS system design incorporates features that ensure completion of protective action. The SAS performs safety-related closed loop controls to help the plant achieve and maintain safe shutdown conditions as well as providing safety-related interlocks. In the applicant's response to RAI 78, Questions 14.03.05-3&4 (Supplement 2), the applicant states the following:

> *"Completion of protective action is verified by several ITAAC. ITAAC Item 4.2 in Section 2.4.1 verifies that an ESF actuation signal remains as long as conditions that represent the completion of the function do not exist and requires deliberate operator action to be returned to normal. ITAAC Item 4.4 in Section 2.4.5 verifies proper connections from the other I&C systems to the PACS. Various mechanical system PACS ITAAC is provided that verifies that the actuator responds to the state requested by the test signal sent to the PACS. Examples of this ITAAC can be found in Tier 1, Sections 2.2.1, 2.2.3, 2.2.4, 2.2.7, 2.6.1, 2.6.6, 2.7.1, 2.7.2, 2.7.11. All ITAAC items mentioned above provide verification that completion of protective action requirement is satisfied."*

The staff understood the applicant's rationale in this excerpt. However, the staff requests the applicant provide an ITAAC Item in Tier 1, Section 2.4.4, that ties these commitments together into the SAS ITAAC to ensure that the ITAAC for SAS will not be completed until satisfactory completion of the above-mentioned sections are satisfactory.

Response to Question 07.01-37:

U.S. EPR FSAR Tier 1, Section 2.4.4 will be revised to include ITAAC for safety automation system (SAS) functions.

FSAR Impact:

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

Question 07.01-41:

OPEN ITEM

Define the terms such as 'halted', 'disabled' and 'out of service', when used in the U.S. EPR FSAR and associated technical reports. This RAI question is part of a series of follow-up questions to RAI 285, Question 07.03-21.

10 CFR 52.47(a)(2) requires, in part, that design description of SSCs in the application shall be sufficient to permit understanding of system designs and their relationships to safety evaluations.

The staff requests the applicant clarify what it means in terms of design functionality, when the U.S. EPR FSAR and associated technical reports use terms such as 'halted', 'out of service', 'disabled' and other such terms, when applied to components such as APUs, ALUs, CPUs, etc. In addition, outline what these terms mean for the operations of these components in the U.S. EPR FSAR and/or Technical Reports ANP-10309 and ANP-10315.

Response to Question 07.01-41:

The U.S. EPR FSAR, Technical Report ANP-10309, and Technical Report ANP-10315 were reviewed to determine if any terminology such as 'halted', 'disabled', and 'out of service' and other related terms were applied to processing components such as APUs, ALUs, and function processors. The following table describes the instances where this terminology is found, and the actions that were taken.

Table 07.01-41—U.S. EPR Design Functionality Terminology

(4 Sheets)

Section	Terminology	Comment	Action
U.S. EPR FSAR Tier 2, Section 7.1	Disable	Used to describe the turning on/off of a function.	None
	Operable/Inoperable	Used to refer to the operability of equipment defined by Technical Specifications.	None
	Out of service	Used to describe when a device does not operate according to its intended functionality, or does not communicate with the DCS (e.g. failure, loss of power, or maintenance).	None
	Removed from service	The act of placing an item out of service.	None
U.S. EPR FSAR Tier 2, Section 7.2	Enable/Disable	Used to describe the turning on/off of a function.	None
	Activate	Used to describe when a setpoint allowed for use.	None

Table 07.01-41—U.S. EPR Design Functionality Terminology

(4 Sheets)

Section	Terminology	Comment	Action
	Inoperable	Used to describe the effects of a SWCCF on the PS. This complies with the definition of inoperable in the Technical Specifications.	None
U.S. EPR FSAR Tier 2, Section 7.3	Enable/Disable	Add clarification on what disabling/enabling the outputs of the PACS means. Did not clarify where terms were used, but not applied to APUs, ALUs, other function processors, and PACS.	Revise Section
	Activate	Used to describe the manual ability to open a PSRV.	None
	Inoperable	Used to describe the effects of a SWCCF on the PS. This complies with the definition of inoperable in the Technical Specifications.	None
U.S. EPR FSAR Tier 2, Section 7.4	Enable/Disable	Used to describe the turning on/off of a function.	None
	Operable/Inoperable	Used to refer to the operability of equipment defined by Technical Specifications.	None
U.S. EPR FSAR Tier 2, Section 7.5	Enable	Used to describe the turning on of a function.	None
	Inoperable	Used to refer to the inoperable equipment states defined by Technical Specifications.	None
U.S. EPR FSAR Tier 2, Section 7.6	Activate	Used to describe when an interlock function is allowed for use.	None
	Removed from service	The act of placing an item out of service.	None
U.S. EPR FSAR Tier 2, Section 7.7	Disable	Used to describe the turning off of a function.	None
	Activate/Deactivate	Used to describe the turning on/off of a function.	Revise terminology
	Operable	Used to describe during which plant states a function shall be available. This complies with the definition of inoperable in the Technical Specifications.	None
U.S. EPR FSAR Tier 2, Section 7.8	Enable/Disable	Used to describe the turning on/off of a function.	None

Table 07.01-41—U.S. EPR Design Functionality Terminology

(4 Sheets)

Section	Terminology	Comment	Action
Technical Report ANP-10309	Enable/Disable	Used to describe the turning on/off of a function.	None
	Activate	Used to describe the turning on of a function.	Revise to enable
	Operable/Inoperable	Added a reference to U.S. EPR FSAR Tier 2, Table 7.1-6, to clarify the operability states of the function processors in accordance with Technical Specification.	Clarification
	Out of service	Used to describe when a device does not operate according to its intended functionality, or does not communicate with the DCS (e.g. failure, loss of power, or maintenance).	None
	Removed from service	The act of placing an item out of service.	None
Technical Report ANP-10315	Enable	Added clarification on what enabling the outputs of the PACS means.	Clarification
	Activate/Deactivate	Added clarification on what activating/ deactivating (i.e. provide a signal output, or shutdown) function processors mean. Did not clarify when the terms were used to describe the execution of a function.	Clarification
	Halt	Added additional detail to describe a halted function processor.	Clarification
	Operable/Inoperable	Used when cited from the regulatory requirements and describes the state of the PS as a whole or per division. Used to refer to the inoperable equipment states defined by Technical Specifications.	None
	Out of service	Used to describe when a device does not operate according to its intended functionality, or does not communicate with the DCS (e.g. failure, loss of power, or maintenance).	None

Table 07.01-41—U.S. EPR Design Functionality Terminology

(4 Sheets)

Section	Terminology	Comment	Action
	Removed from service	The act of placing an item out of service.	None

The U.S. EPR FSAR, Technical Reports ANP -10309, and ANP-10315 will be revised to clarify terms such as ‘halt’, ‘activate’, ’inoperable’, ‘operable’, ‘disable’, ‘enable’ and ‘deactivate’ when applied to components such as function processors, APUs, and ALUs. No actions were taken if the terms were used to describe system or plant functions.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.3 and 7.7, will be revised as described in the response and indicated on the enclosed markup.

Technical Report Impact:

Technical Reports ANP-10309 and ANP-10315 will be revised as described in the response and indicated on the enclosed markup.

Question 07.03-38:

OPEN ITEM

Provide information on how SAS and other TXS safety-related I&C systems comply with the requirements of IEEE Std. 603-1998, Clause 4, as shown on U.S. EPR FSAR, Tier 2, Table 7.1-2.

Section 4 of IEEE Std. 603-1991, requires, in part, the specific basis established for the design of each safety system. The staff reviewed the FSAR to determine how the applicant addressed design basis requirements of IEEE Std. 603-1998, Clause 4, and applicable general design criteria, for SAS and other safety-related systems. The staff was unable to determine that for SAS and other safety-related I&C systems, all design basis requirements have been incorporated. For example, in Tier 2, Section 7.1.2.6.10, Interim Revision 3 mark-ups, the applicant states that the U.S. EPR design does contain equipment protective features that may prevent a piece of safety-related equipment from performing its function and that a failure of this type would be bounded by the single failure analysis. The applicant goes on to state that failure modes and effects analysis (FMEA) have been performed for the safety-related process systems to demonstrate that no single failure can prevent performance of a safety function.

The staff accepted the applicant's rationale in its evaluation of the PS for compliance with Clause 4.k. However, the staff has not received an FMEA for SAS, or the other safety-related systems in the U.S. EPR design. The applicant has bounded compliance with Clause 4.k by the single failure criterion but without similar analysis for SAS and other safety-systems available to the staff for review, the staff cannot make a reasonable assurance finding. Table 7.1-2 matches individual requirements to the various TXS I&C systems. Table 7.1-2 does not demonstrate specifically how the requirements are met for each system that is applicable to IEEE Std. 603-1998, Clause 4.

The staff requests the applicant specifically address the requirements of Clause 4 for each TXS safety-related I&C system in U.S. EPR FSAR Tier 2, Section 7.1. If particular sub-clauses to IEEE Std. 603-1998, Clause 4 are not applicable to a TXS safety-related I&C system then the staff requests the applicant state this and provide a justification for the exclusion.

Response to Question 07.03-38:

Safety Information and Control System

Information about the safety information and control system (SICS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.3.1. Specific information for the SICS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The anticipated operational occurrence (AOOs) and postulated accident (PAs) that require protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5. The human system interface (HSI) design concept in relation to the SICS is addressed in U.S. EPR FSAR Tier 2, Section 18.7.4 and in Tier 1, Table 3.4-1, Item 8.

b) The SICS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

   – Single detectable failures within the SICS.

   – Failures caused by the single failure.

   – Failures and spurious system actions that cause, or are caused by the AOO or PA that requires the safety function.

   The SICS provides controls in the main control room (MCR) for the manual actuation of engineered safety features (ESF) functions listed in FSAR Tier 2, Table 7.3-5.

c) Bypassed and inoperable status indication (BISI) of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The SICS does not provide variables that control protective actions to the protection system (PS).

e) The SICS provides a manual actuation of reactor trip in the MCR and reactor shutdown system (RSS).

   The SICS provides controls in the MCR for the manual actuation of ESF functions listed in U.S. EPR FSAR Tier 2, Table 7.3-5.

   For the U.S. EPR, protective actions performed by the PS and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. Plant-specific Emergency Operating Procedures (EOPs) and Abnormal Operating Procedures (AOPs) for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a Technical Bases Document (TBD) that will be based on hundreds of safety analyses, which are not yet completed. The emergency operating procedure development process is described in U.S. EPR FSAR Tier 2, Section 13.5.2.1.2, states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the Babcock and Wilcox (B&W) Unit EOP TBD. This document, which represents the vendor Emergency Procedure Guidelines (EPG), provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The SICS does not have variables that have spatial dependence or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, and Tables 8.3-1, Table 8.3-11 and 8.3-12.
- Radiation Zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The SICS is contained with in the Safeguards Building, which is a Seismic Category I structure. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The MCR and RSS will be designed in a way that minimizes human error and incorporates human reliability evaluations to preclude operator error from the SICS. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 18.7.2 and 18.7.4, and in Tier 1, Table 3.4-1.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the SICS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The SICS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

j) The PS performs the protective actions for the U.S. EPR. Reactor trips are listed in U.S. FSAR Tier 2, Table 7.2-1 and reactor trip setpoints are provided in U.S. EPR FSAR Table 15.0-7.

The PS processes both automatic and manual ESF functions. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

Critical points in time, or plant conditions that define the proper completion of a safety function are addressed in plant-specific plant specific EOPs and AOPs. The plant specific EOPs and AOPs for the U.S. EPR design are not yet written. The plant specific EOPs will be developed from a TBD that is based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2, states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information about safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) The controls and indications that are required to be on the SICS are implemented with dedicated, hardwired I&C.

Protection System

Information about the PS is provided in U.S. EPR FSAR Tier 2, 7.1.1.4.1. Specific information for the PS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and PAs requiring protective action by the PS are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in Table 15.0-5. The correlation between each event and specific ESF actuation functions performed by the PS is found in Table 15.0-10.

b) The PS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

- Single detectable failures within the PS.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the AOO or PA that requires the safety function.

The PS is provided to sense conditions that require protective action, and to automatically initiate the safety systems required to mitigate the event.

The PS provides the following safety-related functions:

- Performs automatic initiation of reactor trip functions, listed in U.S. EPR FSAR Tier 2, Table 7.2-1.
- Performs automatic initiation of ESF functions, listed in U.S. EPR FSAR Tier 2, Table 7.3-1.
- Initiates reactor trip manual functions.
- Provides actuation of ESF manual functions.
- Generates permissive signals that authorize the activation or deactivation of certain protective actions according to current plant conditions.
- Generates permissive signals that maintain safety-related interlocks.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.3.2.1.2.

d) The PS processes both automatic and manual reactor trip functions. The PS initiates an automatic reactor trip to mitigate the effects of AOOs and PAs.

The PS automatically initiates a reactor trip when selected variables, provided in U.S. EPR FSAR Tier 2, Table 7.2-1, exceed setpoints that are indicative of conditions that require protective action.

U.S. EPR FSAR Tier 2 Table 7.2-1 provides the protective function and the range of each variable.

The PS automatically initiates ESF functions. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

The analytical limit for reactor trip setpoints is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

U.S. EPR FSAR Tier 2, Section 18.7.4 provides information about the inventory of alarms, displays and controls.

Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.3.2.1.3.

e) The SICS provides a manual actuation of reactor trip in the MCR and RSS.

PS manually actuated functions are listed in U.S. EPR FSAR Tier 2, Table 7.3-5.

For the U.S. EPR, protective actions performed by the PS and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. Plant-specific EOPs and AOPs for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a Technical Bases Document (TBD) that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Chapter 13.5.2.1.2, states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Chapter 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The U.S. EPR design does not use spatially dependent variables as inputs to ESF actuation. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.2.2.1.5.

The self-powered neutron detectors (SPNDs) have spatial dependence required for protective purposes. The minimum number of SPNDs required for protective purposes is provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation Zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70 and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.

- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The PS is contained with in the Safeguards Building which is a Seismic Category I structure. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The MCR and RSS will be designed to minimize human error and incorporate human reliability evaluations to preclude operator error. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 7.1.1.6.5, 18.7.2, 18.7.4, and in Tier 1, Table 3.4-1.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the PS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The PS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Sections 7.1.1.2.1 through 7.1.1.2.2.

Information about the Teleperm XS (TXS) platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S. EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1 and each reactor trip set-point is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

The PS automatically initiates ESF functions. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a Technical Bases Document (TBD) that will be based on hundreds of safety analyses, which are not yet completed. FSAR Section 13.5.2.1.2, Emergency Operating Procedure Development Process, states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4, EOP Development Acceptance Criteria.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in ANP-10304, Revision 4 (Reference 1).

Safety Automation System

Information about the safety automation system (SAS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.4.2. Specific information for the SAS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and postulated accident PAs that require protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The SAS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

   – Single detectable failures within the SAS.

   – Failures caused by the single failure.

   – Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

   Automatic actuation of ESF systems and auxiliary supporting systems is performed by the PS. The SAS performs closed loop automatic controls of certain ESF systems following the actuation by the PS. These controls are described in U.S. EPR FSAR Tier 2, Section 7.3.1.2. The SAS does not perform automatic or manual protective actions. SAS automatic functions are addressed in U.S. EPR FSAR Tier 2, Table 7.1-5, and Sections 7.3 and 7.6.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The PS processes both automatic and manual reactor trip functions. The SAS does not perform automatic or manual protective actions and does not provide any input variables to the PS for control of any protective action.

e) The SAS does not perform automatic or manual protective actions and does not provide any input variables to the PS for control of any protective action.

f) The SAS does not have variables with spatial dependence, or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The SAS is contained within Seismic Category I structures. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The MCR and RSS will be designed to minimize human error and incorporate human reliability evaluations to preclude operator error. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 7.1.1.6.5, 18.7.2, 18.7.4, and in Tier 1, Table 3.4-1.

– Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the SAS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The SAS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Sections 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S. EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1 and each reactor trip set-point is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

The PS processes both automatic and manual ESF functions. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific Emergency Operating Procedures (EOPs) and Abnormal Operating Procedures (AOPs); however the plant specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Priority and Actuator Control System

Information about the priority and actuator control system (PACS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.4.3. Specific information for the PACS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and PAs that require protective action are analyzed in U.S. EPR

FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The PACS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

- Single detectable failures within the PACS.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

Protection system (PS) signals received by each priority module override other signals received by the priority module.

The PS sends a signal to the PACS to automatically initiate each ESF function except the Turbine Trip. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable. The PACS is not utilized for the performance of a Turbine Trip ESF function.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The PS processes both automatic and manual ESF functions. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable. The PS sends a signal to the PACS to automatically initiate each ESF function except the Turbine Trip. The PACS is not utilized for the performance of a Turbine Trip ESF function.

RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) Protection system manually actuated ESF functions are listed in U.S. EPR FSAR Tier 2, Table 7.3-5. The PACS is not utilized for the performance of a Turbine Trip ESF function.

For the U.S. EPR, protective actions are performed by the PS, and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. Plant-specific EOPs and AOPs for the U.S. EPR design needs to be performed; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Chapter 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the

operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The PACS does not have variables with spatial dependence or sensors required for protective purposes. The PS sends a signal to the PACS to automatically initiate each ESF function except the Turbine Trip. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable; however, the PACS is not utilized for the performance of a Turbine Trip ESF function.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in: FSAR Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2 Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The PACS is contained within Seismic Category I structures. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.

- The SICS in the MCR is not normally used by the operator. The SICS is used for controls that are not available on PICS, and when PICS is not available. The U.S. EPR I&C design allows for multiple I&C systems to send requests to a given actuator using priority management. To preclude operator error from the SICS, during normal operation, the operational I&C disable switch on the SICS is set so that PAS can send commands to the PACS, thereby allowing automatic commands from the PAS to override manual commands from the SICS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.5.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the PACS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The PACS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1 and each reactor trip set-point is provided in U.S. EPR FSAR Tier 2, Table 15.0-7. The PS processes both automatic and manual ESF functions.

U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable. The PACS is not utilized for the performance of a turbine trip ESF function.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Incore Instrumentation System

Information about the incore instrumentation system (IIS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.5.2. Specific information for the IIS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and PAs that require protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The IIS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

   – Single detectable failures within the IIS.

   – Failures caused by the single failure.

   – Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

   SPNDs provide input signals to PS for the performance of a reactor trip due to Low DNBR and a reactor trip due to High Linear Power Density (HLPD) reactor trip.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The IIS provides SPND signals to the PS for reactor trip due to Low DNBR and HLPD. The PS processes both automatic and manual reactor trip functions.

   The PS initiates automatic reactor trip to mitigate the effects of AOOs and PAs. The PS automatically initiates a reactor trip when selected variables, provided in U.S. EPR FSAR Tier 2, Table 7.2-1 exceed setpoints that are indicative of conditions that require protective action. U.S. EPR FSAR Tier 2, Table 7.2-1 provides the protective function and the range of each variable.

   The analytical limit for reactor trip setpoints is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

   RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) The SICS provides a manual reactor trip signal to the PS.

   For the U.S. EPR, protective actions are performed by the PS, and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. Plant-specific EOPs and AOPs for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. The emergency operating procedure development is described in U.S. EPR FSAR Tier 2, Chapter 13.5.2.1.2, which states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD.

This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Chapter 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The SPNDs have spatial dependence required for protective purposes. The minimum number of SPNDs required for protective purposes is provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.

- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The IIS is contained within the Seismic Category I structures. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The calculation of Low DNBR and HLPD is performed by the PS. The P2 permissive condition bypasses both the Low DNBR and HLPD reactor trip function at low power levels. To preclude operator error, this bypass is automatically removed as power increase above the P2 permissive setpoint. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 7.2.1.2.1 and 7.2.1.2.2.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the IIS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The IIS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S. EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1, and reactor trip setpoints are provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and

diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Excore Instrumentation System

Information about the excore instrumentation system (EIS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.5.3. Specific information for the EIS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOO or PA that require protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The EIS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

   – Single detectable failures within the EIS.

   – Failures caused by the single failure.

   – Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

   – Intermediate range neutron detector signals are sent to the PS for a Low Doubling Time reactor trip and High Neutron Flux reactor trip.

   – Power range neutron detector signals are sent to the PS for a High Neutron Flux Rate of Change reactor trip.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The EIS provides intermediate range neutron detector signals and power range neutron detector signals to the PS for automatic reactor trips.

   The PS processes both automatic and manual reactor trip functions. The PS initiates automatic reactor trip to mitigate the effects of AOO and PAs. The PS automatically initiates a reactor trip when selected variables, provided in U.S. EPR FSAR Table 7.2-1 exceed setpoints that are indicative of conditions that require protective action. U.S. EPR FSAR Tier 2, Table 7.2-1 provides the protective function and the range of each variable.

   The analytical limit for reactor trip setpoints is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

   RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) The SICS provides a manual reactor trip signal to the PS.

   For the U.S. EPR, protective actions are performed by the PS and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. Plant-specific EOPs and AOPs for the U.S.

EPR design need to be developed. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Chapter 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The EIS does not have variables that have spatial dependence or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.

- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The EIS is contained within the Seismic Category I structures. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The function of a reactor trip on High Neutron Flux and Low Doubling Time is performed by the PS. The P6 permissive condition bypasses both the High Neutron Flux and Low Doubling Time function above a fixed core thermal power level. This bypass is automatically removed when core thermal power decrease below the P6 permissive setpoint to preclude operator error. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 7.2.1.2.8 and 7.2.1.2.9.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the EIS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The EIS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1 and reactor trip setpoints are provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) Distributed control system (DCS) design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design

is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Boron Concentration System

Information about the boron concentration system (BCMS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.5.4. Specific information for the BCMS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2 Chapter 16, Table 3.3.1-1. The AOOs and PAs requiring protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The BCMS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

   – Single detectable failures within the BCMS.

   – Failures caused by the single failure.

   – Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

The BCMS provides boron concentration input signal to the PS for the CVCS Isolation for Anti-Dilution function as listed in U.S. EPR FSAR Tier 2, Table 7.3-1. This function is addressed in U.S. EPR FSAR Tier 2, Section 7.3.1.2.11.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The BCMS provides boron concentration input signal to the PS for the CVCS Isolation for Anti-Dilution function, as listed in U.S. EPR FSAR Tier 2, Table 7.3-1. This function is addressed in U.S. EPR FSAR Tier 2, Section 7.3.1.2.11.

   The PS processes both automatic and manual ESF functions to mitigate the effects of AOO and PA. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

   RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) CVCS Isolation on Anti-Dilution Mitigation may be performed manually as indicated by U.S. EPR FSAR Tier 2, Table 7.3-5.

   Plant-specific EOPs and AOPs for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for

currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The BCMS does not have variables that have spatial dependence for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, and Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.

- The BCMS is contained within a Seismic Category I structure. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- CVCS Isolation on Anti-Dilution Mitigation may be performed manually from the SICS. The MCR and RSS will be designed to minimize human error and incorporate human reliability evaluations as a means to preclude operator error. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 7.1.1.6.5, 18.7.2, 18.7.4, and in Tier 1, Table 3.4-1.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained as a means to prevent failure in a non-safety system from affecting the BCMS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The BCMS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The BCMS provides boron concentration input signal to the PS for the CVCS Isolation for Anti-Dilution function as listed in Table 7.3-1 and the PS performs the protective actions for the U.S. EPR.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Radiation Monitoring System

The radiation monitoring system (RMS) does not perform automatic system actuations.

Information about the RMS is provided in U.S. EPR FSAR Section 7.1.1.5.5. Specific information for the RMS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and postulated accident PAs requiring protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The RMS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

   – Single detectable failures within the RMS.

   – Failures caused by the single failure.

   – Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

   – High Range Containment Radiation monitors provide an input signal to the PS for the Containment Isolation ESF function.

   – MCR air intake duct activity radiation monitors provide an input signal to the PS for the MCR air conditioning system isolation and filtering ESF function.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The RMS provides high range containment radiation monitor signals and MCR air intake duct activity radiation monitor signals to the PS for performance of ESF functions.

   The PS processes both automatic and manual ESF functions to mitigate the effects of AOO and PA. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

   RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) Containment Isolation and CRACS Isolation and Filtering functions may be performed manually as indicated by U.S. EPR FSAR Tier 2, Table 7.3-5.

   For the U.S. EPR, protective actions are performed by the PS and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. EOPs and AOPs for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Chapter 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time

and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The RMS does not have variables that have spatial dependence or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, and Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The safety related portions of the RMS providing input to the PS are contained within a Seismic Category I structure. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.

- Containment Isolation and main control room air conditioning system (CRACS) Isolation and Filtering functions may be performed manually from the SICS. The MCR and RSS will be designed to minimize human error and incorporate human reliability evaluations to preclude operator error. Additional information is provided in U.S. EPR FSAR Tier 2, Sections 7.1.1.6.5, 18.7.2, 18.7.4, and in Tier 1, Table 3.4-1.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the RMS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The RMS will be designed to meet the applicable requirements and guidance necessary to interface with the TXS platform.

   Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The RMS provides radiation monitoring signals to the PS for the Containment Isolation and MCR Air Conditioning System Isolation and Filtering functions as listed in U.S. EPR FSAR Tier 2, Table 7.3-1 and the PS performs the protective actions for the U.S. EPR.

   Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

   The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) The RMS provides input to the SCDS. DCS design principles are addressed in U.S. EPR FSAR Tier 2 Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Hydrogen Monitoring System (HMS)

Information about the HMS is provided in U.S. EPR FSAR Tier 2, Sections 6.2.5 and 7.1.1.5.6. Specific information for the HMS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and PAs requiring protective action are analyzed in U.S. EPR FSAR Tier 2 Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The HMS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

- Single detectable failures within the HMS.
- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

The HMS does not provide any signals to the PS for protective functions.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The HMS does not provide any signals to the PS for protective functions.

e) The HMS does not provide any signals to the PS for protective functions.

f) The HMS does not have variables that have spatial dependence or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, and Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.

i) The HMS will be designed to meet the applicable requirements and guidance necessary to interface with the TXS platform. Information about the TXS platform is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

j) The HMS does not provide any signals to the PS for protective functions. Plant conditions for the operation of the HMS are provided in U.S. EPR FSAR Tier 2, Section 6.2.5.3 and Section 19.2.3.3.2.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) The HMS continuously measures the hydrogen concentration in containment during and after the accident, and remains functional during and after exposure to the accident environmental conditions in accordance with 10 CFR 50.44(c)(4)(ii).

Signal Conditioning and Distribution System

Information about the signal conditioning and distribution system (SCDS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.4.8. Specific information for the SCDS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and postulated accident PAs requiring protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The SCDS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

- Single detectable failures within the SCDS.
- Failures caused by the single failure.

– Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

The SCDS receives hardwired inputs from sensors or black boxes and sends hardwired signal outputs to the PS.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The SCDS receives hardwired inputs from sensors or black boxes and sends hardwired signal outputs to the PS.

The PS processes both automatic and manual reactor trip functions. The PS initiates automatic reactor trip to mitigate the effects of AOOs and PAs. The PS automatically initiates a reactor trip when selected variables, provided in U.S. EPR FSAR Tier 2, Table 7.2-1, exceed setpoints that are indicative of conditions that require protective action. U.S. EPR FSAR Tier 2, Table 7.2-1 provides the protective function and the range of each variable.

The PS processes both automatic and manual ESF functions to mitigate the effects of AOO and PA. U.S. EPR FSAR Tier 2, Table 7.3-1 provides the ESF functions and the range of each variable.

The analytical limit for reactor trip setpoints is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) The list of ESF functions that may be performed manually is provided indicated in U.S. EPR FSAR Tier 2, Table 7.3-5.

For the U.S. EPR, .protective actions are performed by the PS and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. Plant-specific EOPs and AOPs for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The SCDS does not have variables that have spatial dependence or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, and Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The safety-related portions of the SCDS providing input to the PS are contained within a Seismic Category I structure. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The SCDS does not perform actuation functions.
- Independence between safety-related I&C systems and non-safety related I&C systems is maintained as a means to prevent failure in a non-safety system from affecting the SCDS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The SCDS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Section 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S. EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1, and reactor trip setpoints are provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2,Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

Rod Position Measurement System

Information about the rod position measurement system (RPMS) is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.5.14. Specific information for the RPMS for IEEE 603-1998, Clause 4 is as follows:

a) The modes of operation of the U.S. EPR are provided in U.S. EPR FSAR Tier 2, Chapter 16, Table 3.3.1-1. The AOOs and PAs requiring protective action are analyzed in U.S. EPR FSAR Tier 2, Chapter 15. The initiating events analyzed are listed in U.S. EPR FSAR Tier 2, Table 15.0-1. The initial conditions analyzed for each event are presented in U.S. EPR FSAR Tier 2, Table 15.0-5.

b) The RPMS is designed so that safety-related functions required for an AOO or PA are performed in the presence of the following:

- Single detectable failures within the RPMS.

- Failures caused by the single failure.
- Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.

The RPMS provides a RCCA position measurement signal to the PS for the performance of a Low DNBR reactor trip.

c) BISI of safety-related systems is provided by the PICS. BISI is also addressed in U.S. EPR FSAR Tier 2, Sections 7.1.3.1.4, 7.5.2.1.1, 7.5.2.2.4, and 7.5.2.2.5.

d) The RPMS provides a RCCA position measurement signal to the PS for the performance of a Low DNBR reactor trip

The PS processes both automatic and manual reactor trip functions. The PS initiates automatic reactor trip to mitigate the effects of AOOs and PAs. The PS automatically initiates a reactor trip when selected variables, provided in U.S. EPR FSAR Tier 2, Table 7.2-1, exceed setpoints that are indicative of conditions that require protective action. U.S. EPR FSAR Tier 2, Table 7.2-1 provides the protective function and the range of each variable.

The analytical limit for reactor trip setpoints is provided in U.S. EPR FSAR Tier 2, Table 15.0-7.

RAI 414, Question 7.3-30 provides time response information for each variable associated with protective functions of the PS.

e) The SICS provides a manual reactor trip signal to the PS.

For the U.S. EPR, protective actions are performed by the PS and the reactor trips are provided in U.S. EPR FSAR Tier 2, Table 7.2-1. EOPs and AOPs for the U.S. EPR design need to be developed. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Chapter 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system. The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Chapter 13.4.2.1.4. Since EPGs and EOPs have not been developed, the points in time and plant conditions for allowance of manual control are not known, the justification for permitting initiation or control subsequent to initiation solely by manual means is not known, and the expected range of environmental conditions imposed on the operator during normal, abnormal and accident conditions throughout manual operations is not known.

f) The RPMS does not have variables that have spatial dependence or sensors required for protective purposes.

g) Information concerning transient and steady-state motive and control power and environmental conditions during normal, abnormal and accident conditions is for safety systems provided as follows:

- Electrical Information is provided in U.S. EPR FSAR Tier 2, Section 8.2.2.4, and Tables 8.3-1, 8.3-11 and 8.3-12.
- Radiation zone information is provided in U.S. EPR FSAR Tier 2, Figures 12.3-21 through 12.3-29, 12.3-64 through 12.3-66, 12.3-70, and 12.3-81.
- Environmental conditions are provided in: U.S. EPR FSAR Tier 2, Table 9.4.14-1.
- Electromagnetic and radio-frequency interference qualification is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.4.17.
- Seismic and dynamic qualification of electrical and I&C equipment is provided in U.S. EPR FSAR Tier 2, Section 3.10.2.
- Methodology for qualifying safety-related electrical equipment is provided in U.S. EPR FSAR Tier 2, Appendix 3D.
- Seismic qualification techniques are provided in U.S. EPR FSAR Tier 2, Appendix 3E.

h) Information about conditions that have the potential of degrading safety system performance is provided as follows:

- Fire, for which fire protection compliance information is provided in U.S. EPR FSAR Tier 2, Section 3.1.1.3.1.
- Wind and tornado loading, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.3.
- Safeguards Building flooding, for which the analysis is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.4.
- Missile projection, for which protection information is provided in U.S. EPR FSAR Tier 2, Section 3.5.
- Environmental qualification of electrical equipment, which includes fluid system separation, equipment separation and redundancy, is provided in U.S. EPR FSAR Tier 2, Section 3.11.
- Loss of ventilation to electrical equipment, for which information is provided in U.S. EPR FSAR Tier 2, Section 3.11.4.
- The RPMS providing input to the PS are contained within a Seismic Category I structure. Information pertaining to pipe breaks is provided in U.S. EPR FSAR Tier 2, Section 3.4.3.1.
- The calculation of Low DNBR is performed by the PS. The P2 permissive condition bypasses the Low DNBR reactor trip function at low power levels. This bypass is automatically removed as power increase above the P2 permissive setpoint to preclude operator error. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.2.1.2.1.

– Independence between safety-related I&C systems and non-safety related I&C systems is maintained to prevent failure in a non-safety system from affecting the RPMS. Additional information is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

i) The RPMS will be designed to meet the applicable requirements and guidance identified in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1.

Information about the TXS platform design is provided in U.S. EPR FSAR Tier 2, Section 7.1.1.2.1. System design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6.

j) The PS performs the protective actions for the U.S. EPR. Reactor trips are listed in U.S. EPR FSAR Tier 2, Table 7.2-1 and reactor trip setpoints are provided in U.S. EPR FSAR Table 15.0-7.

Critical points in time or plant conditions that define the proper completion of a safety function are addressed in plant-specific EOPs and AOPs; however, the plant-specific EOPs and AOPs for the U.S. EPR design have not yet been written. The plant-specific EOPs will be developed from a TBD that will be based on hundreds of safety analyses, which are not yet completed. U.S. EPR FSAR Tier 2, Section 13.5.2.1.2 states that the EOPs for the U.S. EPR design will be based on the same symptom-based approach and mitigation strategies as the B&W Unit EOP TBD. This document, which represents the vendor EPG, provides the bases that were used to develop the plant-specific EOPs for currently operating plants that have the B&W nuclear steam supply system.

The relevant NRC regulation requirements that will be used as acceptance criteria during the development of the EPGs and EOPs are provided in U.S. EPR FSAR Tier 2, Section 13.4.2.1.4.

k) For safety-related systems, independence is established so that a single failure does not result in the loss of the safety function of the process system. Information for safety-related equipment protective provisions is provided in U.S. EPR FSAR Tier 2, Section 7.1.3.6.10.

l) DCS design principles are addressed in U.S. EPR FSAR Tier 2, Section 7.1.1.6. The other special design basis that is imposed on the I&C systems design is the defense-in-depth and diversity analysis based on a software common cause failure. The overall defense-in-depth and diversity is described in Reference 1.

FSAR Impact:

The U.S. EPR FSAR Tier 2, Section 7.3.1 and Table 7.3-5 will be revised as described in the response and indicated on the enclosed markup.

References:

1. ANP-10304, Revision 4, “U.S. EPR Diversity and Defense-In-Depth Assessment Technical Report,” AREVA NP Inc., June 2011.

U.S. EPR Final Safety Analysis Report Markups

2.4.4 Safety Automation System

1.0 Description

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

The SAS provides the following safety related functions:

- Provides control and monitoring of systems required to transfer the plant to cold shutdown and maintain it in this state following an anticipated operational occurrence (AOO) or postulated accident (PA).
- Provides control and monitoring of safety-related functions of auxiliary support systems.
- Provides safety interlock functions.

2.0 Arrangement

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

2.2 Physical separation exists between ~~the four~~ divisions of the SAS as listed in Table 2.4.4-1.

2.3 Physical separation exists between Class 1E SAS equipment and non-Class 1E equipment.

3.0 Mechanical Design Features

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

4.0 I&C Design Features, Displays and Controls

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

07.01-37

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

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

4.4 The SAS provides the interlocks listed in Table 2.4.4-~~4~~3—Safety Automation System Interlocks.

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

- By introducing and varying, a substitute input of the same nature as the measured variable.
- By cross-checking between channels that bear a known relationship to each other.
- By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.

4.16 Deleted.

4.17 Hardwired disconnects exist between the service unit (SU) and each divisional monitoring and service interface (MSI) of the SAS. The hardwired disconnects prevent the connection of the SU to more than a single division of the SAS.

07.01-37

4.18 The SAS performs the automatic functions listed in Table 2.4.4-~~5~~2—Safety Automation System Automatic Functions and Input Variables.

4.19 During data communication, the SAS function processors receive only the pre-defined messages for that specific function processor. Other messages are ignored.

4.20 SAS self-test features are capable of detecting faults consistent with the requirements of the SAS.

4.21 SAS connections to the SICS are hardwired for manual grouped controls.

4.22 SAS manual grouped controls and indications are available on the SICS in the MCR.

4.23 Permissive P15 provides operating bypass capability for the following SAS functions:

- Safety Injection and Heat Removal System - Automatic Trip of LHSI Pump (in RHR Mode) on Low Delta Psat.
- Safety Injection and Heat Removal System - Automatic Trip of LHSI Pump (in RHR Mode) on Low Loop Level.

5.0 Electrical Power Design Features

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

6.0 Environmental Qualification

6.1 Components listed as Class 1E in Table 2.4.4-1 can perform their function under normal environmental conditions, AOOs, and accident and post-accident environmental conditions.

~~6.0~~7.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.4-~~6~~4 lists the SAS ITAAC.

07.01-37

~~Table 2.4.4-2—Safety Automation System Input Signals~~

~~Item #~~	~~Signal~~	~~Source~~	~~# Divisions~~	~~IEEE Class 1E~~
~~1~~	~~Steam Generator Pressure~~	~~Signal Conditioning and Distribution System (SCDS)~~	~~4~~	~~Yes~~
~~2~~	~~Main Steam Relief Control Valve Position~~	~~Priority and Actuator Control System (PACS)~~	~~4~~	~~Yes~~
~~3~~	~~Neutron Flux from Power Range Detector (PRD) for Nuclear Power Calculation~~	~~SCDS~~	~~4~~	~~Yes~~
~~4~~	~~Main Steam Relief Isolation Valve Position~~	~~PACS~~	~~4~~	~~Yes~~
~~5~~	~~Steam Generator Level (WR)~~	~~SCDS~~	~~4~~	~~Yes~~
~~6~~	~~Emergency Feedwater Flow~~	~~SCDS~~	~~4~~	~~Yes~~

07.01-37

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
Annulus Ventilation System (AVS)	Accident Filtration Train Heater Control	Train 1 Post Heater Temperature
		Train 4 Post Heater Temperature
	Accident Train Switchover	Pressure
		Post Heater Temperature
		Filter Bank Isolation Inlet Damper Position
		Filter Bank Isolation Outlet Damper Position
		Exhaust Fan Signal
Component Cooling Water System (CCWS)	CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2 and Train 2 to Train 1	Train 1 Loss of ESWS Signal
		Train 1 Pump Pressure
		Train 1 Flow Rate
		Train 1 Surge Tank Level
		Train 2 Loss of ESWS Signal
		Train 2 Pump Pressure
		Train 2 Flow Rate
		Train 2 Surge Tank Level
	CCWS Common 2.b Automatic Backup Switchover of Train 3 to Train 4 and Train 4 to Train 3	Train 3 Loss of ESWS Signal
		Train 3 Pump Pressure
		Train 3 Flow Rate
		Train 3 Surge Tank Level
		Train 4 Loss of ESWS Signal
		Train 4 Pump Pressure
		Train 4 Flow Rate
		Train 4 Surge Tank Level
	CCWS Emergency Temperature Control	Heat Exchanger Temp
		Heat Exchanger Bypass Valve Position
	CCWS Emergency Leak Detection	Surge Tank Level
		CCWS Chiller Inlet Flow
		CCWS Chiller Outlet Flow
		Common Supply Outlet Flow

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
		Common Supply Inlet Flow
	CCWS Emergency Leak Detection – Switchover Valves Leakage or Failure	Surge Tank 1 Level
		Surge Tank 2 Level
		Surge Tank 3 Level
		Surge Tank 4 Level
	CCWS Switchover Valves Interlock	Train 1 Common 1a Supply Valve Position
		Train 1 Common 1a Return Valve Position
		Train 1 Common 1b Supply Valve Position
		Train 1 Common 1b Return Valve Position
		Train 2 Common 1a Supply Valve Position
		Train 2 Common 1a Return Valve Position
		Train 2 Common 1b Supply Valve Position
		Train 2 Common 1b Return Valve Position
	CCWS RCP Thermal Barrier Containment Isolation Valve Interlock	Common 1b Return Outer Valve Position
		Common 1b Supply Outer Valve Position
		Common 2b Return Outer Valve Position
		Common 2b Supply Outer Valve Position
		Common 1b Return Inner Valve Position
		Common 1b Supply Inner Valve Position
		Common 2b Return Inner Valve Position
		Common 2b Supply Inner Valve Position

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
	SCWS Condenser Supply Water Flow Control	Condenser Refrigerant Pressure
Emergency Feedwater System (EFWS)	SG Closed Loop Level Control	SG Level
	Pump Flow Protection	Pump Flow Signal
Essential Service Water Pump Building Ventilation System (ESWPBVS)	ESWPBVS ESWS Pump Rooms Temperature Control	Pump Room Temperature
Fuel Building Ventilation System (FBVS)	Safety-Related Room Heater Control	Room Temperature
	FBVS EBS / FPCS Pump Rooms Heat Removal	Recirculation Temperature
Fuel Pool Cooling and Purification System (FPCPS)	FPCPS Pump Trip on Low Spent Fuel Pool (SFP) Level	SFP Level
In-Containment Refueling Water Storage Tank System (IRWST)	IRWST Boundary Isolation for Preserving IRWST Water Inventory Interlock	IRWST Level
Main Control Room Air Conditioning System (CRACS)	Iodine Filtration Train Heater Control	Carbon Filter Isolation Damper Position
		Exhaust Fan Signal
	Heater Control for Outside Inlet Air	Downstream Temperature
		Inlet Damper Position
		Outlet Damper Position
	Pressure Control	MCR Differential Pressure
	Cooler Temperature Control	Supply Air Temperature
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Pressure Control	MSRIV Position
		MSRIV Actuation Signal (from PS)
		MSRT Setpoint (from PS)
		SG Pressure
	Steam Generator MSRCV Regulation during Standby Position Pressure Control	MSRCV Position
		Nuclear Power Calculation (from PS)
Safeguard Building Controlled-Area Ventilation System (SBVS)	SIS/RHRS Pump Rooms Heat Removal	Pump Room Temperature
		SIS/RHR Pump Running Signal

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
		SIS/RHR Pump Stopped Signal
	CCWS/EFWS Valve Rooms Heat Removal	Room Temperature
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply and Recirculation Exhaust Air Flow Control	Supply Air Temperature
		Outside Air Temperature
		Outside Air Damper Open Position Signal
		Outside Air Damper Closed Position Signal
		Exhaust Damper Open Position Signal
		Exhaust Damper Closed Position Signal
		Recirculation Damper Open Position Signal
		Recirculation Damper Closed Position Signal
	Supply Fan Safe Shut-off	Recirc / Exhaust Fan Stopped Signal
		Outside Air Damper Closed Position Signal
		Recirculation Damper Closed Position Signal
	Recirculation Fan Safe Shut-off	Supply Air Fan Stopped Signal
	Exhaust Fan Safe Shut-off	Exhaust Damper Closed Position
	Supply Air Temperature Heater Control	Supply Air Downstream of Heaters Temperature
	Freeze Protection – Supply Air Temperature	Outside Air Temperature
	Supply Air Temperature Control for Supply Air Cooling	Supply Air Downstream of Humidifier Temperature
	Supply Air Temperature Control for Supply Air Heating	Outside Air Temperature
	Battery Room Heater Control	Battery Room Temperature

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
	Battery Room Supply Air Temperature Control	Battery Room Supply Air Temperature
	Emergency Feed Water System (EFWS) Pump Room Heat Removal	EFWS Pump Room Temperature
	Component Cooling Water System (CCWS) Pump Room Heat Removal	CCWS Pump Room Temperature
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow / Chiller Black Box Internal Fault / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure	Train 1 Chiller Evaporator Outlet Temperature
		Train 1 Chiller Compressor Oil Pressure
		Train 1 Condenser Refrigerant Pressure
		Train 1 Chiller Evaporator Flow Signal
		Train 1 Cross-Tie Valves Position Signal
		Train 2 Cross-Tie Valves Position Signal
		Train 2 Circulating Pump 1 Running Signal
		Train 2 Circulating Pump 2 Running Signal
		Train 2 Evaporator ΔP Signal
		Train 2 Chiller Evaporator Flow Signal
	SCWS Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow / Chiller Black Box Internal Fault / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure	Train 1 Circulating Pump 1 Running Signal
		Train 1 Circulating Pump 2 Running Signal
		Train 1 Evaporator ΔP Signal
		Train 1 Chiller Evaporator Flow Signal
		Train 1 Cross-Tie Valves Position Signal

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
		Train 2 Cross-Tie Valves Position Signal
		Train 2 Chiller Evaporator Flow Signal
		Train 2 Condenser Refrigerant Pressure
		Train 2 Chiller Compressor Oil Pressure
		Train 2 Chiller Evaporator Outlet Temperature
		Train 2 Condenser Flow Rate Signal
	SCWS Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow / Chiller Black Box Internal Fault / Loss of UHS-CCWS / SCWS Chiller Evaporator Water Flow Control / LOOP Re-start Failure	Train 3 Condenser Flow Rate Signal
		Train 3 Chiller Evaporator Outlet Temperature
		Train 3 Chiller Compressor Oil Pressure
		Train 3 Condenser Refrigerant Pressure
		Train 3 Chiller Evaporator Flow Signal
		Train 3 Cross-Tie Valves Position Signal
		Train 4 Cross-Tie Valves Position Signal
		Train 4 Circulating Pump 1 Running Signal
		Train 4 Circulating Pump 2 Running Signal
		Train 4 Evaporator ΔP Signal
		Train 4 Chiller Evaporator Flow Signal
	SCWS Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow / Chiller Black Box Internal Fault / SCWS	Train 3 Circulating Pump 1 Running Signal
		Train 3 Circulating Pump 2 Running Signal

07.01-37

Table 2.4.4-2— Safety Automation System Automatic Functions and Input Variables (7 Sheets)

Table System	Function Name	Input Variable
	Chiller Evaporator Water Flow Control / LOOP Re-start Failure	Train 3 Evaporator ΔP Signal
		Train 3 Chiller Evaporator Flow Signal
		Train 3 Cross-Tie Valves Position Signal
		Train 4 Cross-Tie Valves Position Signal
		Train 4 Chiller Evaporator Flow Signal
		Train 4 Condenser Refrigerant Pressure
		Train 4 Chiller Compressor Oil Pressure
		Train 4 Chiller Evaporator Outlet Temperature
Safety Injection and Residual Heat Removal System (SIS/RHRS)	Automatic RHRS Flow Rate Control	RHRS Flow Rate Signal
		RHRS Temperature
		LHSI Pump Pressure
	Automatic Trip of LHSI Pump (in RHR Mode) on Low ΔPsat	Hot Leg Temperature (WR)
		Hot Leg Pressure (WR)
	Automatic Trip of LHSI Pump (in RHR Mode) on Low Loop Level	Hot Leg Loop Level
	LHSI Valves Actuation Based on RHRS Alignment	RHR 1st RCPB Isolation Valve Position
		RHR 2nd RCPB Isolation Valve Position
		Outside Containment Isolation Valve Position

~~Table 2.4.4-3—Safety Automation System Output Signals~~

~~Item #~~	~~Output Signal~~	~~Recipient~~	~~# Divisions~~
~~1~~	~~EFW Flow Control Valve Position Signal~~	~~PACS~~	~~4~~
~~2~~	~~EFW SG Level Control Valve Position Signal~~	~~PACS~~	~~4~~
~~3~~	~~Main Steam Relief Control Valve Signal~~	~~PACS~~	~~4~~

07.01-37

07.01-37

Table 2.4.4-43—Safety Automation System Interlocks

Isolation of Component Cooling Water System (CCWS) Trains

07.01-37

Table 2.4.4-5—Safety Automation System Automatic Functions (4 Sheets)

System	Function Name
Annulus Ventilation System (AVS)	Accident Filtration Train Heater Control
Annulus Ventilation System (AVS)	Accident Train Switchover
Component Cooling Water System (CCWS)	CCWS Common 1.b Automatic Backup Switchover of Train 1 to Train 2
Component Cooling Water System (CCWS)	CCWS Common 1.b Automatic Backup Switchover of Train 2 to Train 1
Component Cooling Water System (CCWS)	CCWS Common 2.b Automatic Backup Switchover of Train 3 to Train 4
Component Cooling Water System (CCWS)	CCWS Common 2.b Automatic Backup Switchover of Train 4 to Train 3
Component Cooling Water System (CCWS)	CCWS Emergency Temperature Control
Component Cooling Water System (CCWS)	CCWS Emergency Leak Detection
Component Cooling Water System (CCWS)	CCWS Switchover Valve Interlock
Component Cooling Water System (CCWS)	CCWS RCP Thermal Barrier Containment Isolation Valve Interlock
Component Cooling Water System (CCWS)	CCWS Switchover Valves Leakage or Failure
Component Cooling Water System (CCWS)	CCWS Condenser Supply Water Flow Control
Emergency Feedwater System (EFWS)	SG Closed Loop Level Control
Emergency Feedwater System (EFWS)	EFW Pump Flow Control
Essential Service Water System (ESWS)	Automatic ESWS Actuation from CCWS Start
Essential Service Water Pump Building Ventilation System (ESWPBVS)	Remove Heat Generated by Essential Service Water Equipment
Fuel Building Ventilation System (FBVS)	Safety-related Room Heater Control

07.01-37

Table 2.4.4-5—Safety Automation System Automatic Functions (4 Sheets)

System	Function Name
Fuel Building Ventilation System (FBVS)	Maintain Ambient Conditions for EBS and FPCS pump rooms (Recirculation Coolers)
Fuel Pool Cooling and Purification System (FPCPS)	Fuel Pool Cooling Pump Trip On Low SFP Level
In-Containment Refueling Water Storage Tank System (IRWST)	IRWST Boundary Isolation for Preserving IRWST Water Inventory
Main Control Room Air Conditioning System (CRACS)	Iodine Filtration Train Heater Control
Main Control Room Air Conditioning System (CRACS)	Heater Control for Outside Inlet Air
Main Control Room Air Conditioning System (CRACS)	Pressure Control
Main Control Room Air Conditioning System (CRACS)	Cooler Temperature Control
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Standby Position Control
Main Steam System (MSS)	Steam Generator MSRCV Regulation during Pressure Control
Safeguard Building Controlled Area Ventilation System (SBVS)	SIS/RHRS Pump Rooms Heat Removal
Safeguard Building Controlled Area Ventilation System (SBVS)	SIS/RHRS Valve Rooms Heat Removal
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply and Recirculation Exhaust Air Flow Control
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Fan Safe Shut-off
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Recirculation/Exhaust Fan Safe Shut-off
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Exhaust Fan Safe Shut-off

07.01-37

Table 2.4.4-5—Safety Automation System Automatic Functions (4 Sheets)

System	Function Name
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Air Temperature
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Freeze Protection—Supply Air Temperature
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Freeze Protection—Heat Tracing
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Air Temperature Control for Cooling
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Supply Air Temperature Control for Supply Air Heating
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Battery Room Temperature Control
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Battery Room Supply Air Temperature
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Emergency Feedwater Pump Room Heat Removal
Electrical Division of Safeguard Building Ventilation System (SBVSE)	Component Cooling Water System Rooms Heat Removal
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on Train 1 Low Evaporator Flow
Safety Chilled Water System (SCWS)	SCWS Train 2 to Train 1 Switchover on Train 2 Low Evaporator Flow
Safety Chilled Water System (SCWS)	SCWS Train 3 to Train 4 Switchover on Train 3 Low Evaporator Flow
Safety Chilled Water System (SCWS)	SCWS Train 4 to Train 3 Switchover on Train 4 Low Evaporator Flow
Safety Chilled Water System (SCWS)	SCWS Train 1 to Train 2 Switchover on Train 1 Chiller Black Box Internal Fault
Safety Chilled Water System (SCWS)	SCWS Train 2 to Train 1 Switchover on Train 2 Chiller Black Box Internal Fault

07.01-37

~~Table 2.4.4-5—Safety Automation System Automatic Functions (4 Sheets)~~

~~System~~	~~Function Name~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 3 to Train 4 Switchover on Train 3 Chiller Black Box Internal Fault~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 4 to Train 3 Switchover on Train 4 Chiller Black Box Internal Fault~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 2 to Train 1 Switchover on Loss of Ultimate Heat Sink (LUHS)/CCWS~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 3 to Train 4 Switchover on Loss of Ultimate Heat Sink (LUHS)/CCWS~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 1 to Train 2 Switchover on LOOP Re-start Failure~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 2 to Train 1 Switchover on LOOP Re-start Failure~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 3 to Train 4 Switchover on LOOP Re-start Failure~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Train 4 to Train 3 Switchover on LOOP Re-start Failure~~
~~Safety Chilled Water System (SCWS)~~	~~SCWS Chiller Evaporator Water Flow Control (Trains 1 and 4)~~
~~Safety Injection and Residual Heat Removal System (SIS/RHRS)~~	~~Automatic RHRS Flow Rate Control~~
~~Safety Injection and Residual Heat Removal System (SIS/RHRS)~~	~~Automatic Trip of LHSI Pump (in RHR Mode) on Low ΔPsat~~
~~Safety Injection and Residual Heat Removal System (SIS/RHRS)~~	~~Automatic Trip of LHSI Pump (in RHR Mode) on Low Loop Level~~
~~Safety Injection and Residual Heat Removal System (SIS/RHRS)~~	~~LHSI Valves Actuation Based on RHRS Alignment~~

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
2.1	The location of the SAS equipment is ~~located~~ as listed in Table 2.4.4-1.	~~Inspections~~ An inspection will be performed ~~of the location of the SAS equipment~~.	The SAS equipment listed in Table 2.4.4-1 is located as listed in Table 2.4.4-1.
2.2	Physical separation exists between ~~the four~~ divisions of the SAS as listed in Table 2.4.4-1.	~~Inspections~~ An inspection will be performed ~~to verify that the divisions of the SAS are located in separate Safeguard Buildings~~.	The ~~four~~ divisions of the SAS are located in separate Safeguard Buildings as listed in Table 2.4.4-1.
2.3	Physical separation exists between Class 1E SAS equipment and non-Class 1E equipment.	a. ~~Design analyses~~An analysis will be performed to determine the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E SAS equipment and non-Class 1E equipment. b. ~~Inspections~~ An inspection and analysis will be performed to verify that the required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SAS equipment and non-Class 1E equipment.	a. A report exists ~~and~~ that defines the required safety-related structures, separation distance, barriers, or any combination thereof to achieve adequate physical separation between Class 1E SAS equipment and non-Class 1E equipment. b. The required safety-related structures, separation distance, barriers, or any combination thereof exist between Class 1E SAS equipment and non-Class 1E equipment. Reconciliation is performed of any deviations to the ~~design~~analysis.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
3.1	Equipment identified as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses, or a combination of type tests and analyses will be performed on the equipment listed as Seismic Category I in Table 2.4.4-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements. b. Inspections will be performed of the Seismic Category I equipment listed in Table 2.4.4-1 to verify that the equipment including anchorage is installed per seismic qualification report (SQDP, EQDP, or analyses) requirements~~as specified on the construction drawings~~.	a. Tests/analysis reports ~~exist and~~ conclude that the equipment listed as Seismic Category I in Table 2.4.4-1 can withstand seismic design basis loads without loss of safety function. b. Inspection reports ~~exist and~~ conclude that the Seismic Category I equipment listed in Table 2.4.4-1 including anchorage is installed per seismic qualification report (SQDP, EQDP, or analyses) requirements~~as specified on the construction drawings~~.
4.1	Class 1E SAS equipment listed in Table 2.4.4-1 can ~~perform its safety~~ function when subjected to EMI, RFI, ESD, and power surges.	Type tests or type tests and analysis ~~of these~~ will be performed ~~for the Class 1E equipment listed in Table 2.4.4-1~~.	~~A report exists and concludes that the e~~Equipment identified as Class 1E in Table 2.4.4-1 can ~~perform its safety~~ function when subjected to electromagnetic interference EMI, RFI, ESD, and power surges.
4.2	The SAS receives input signals from the sources listed in Table 2.4.4-2.	~~Tests~~ A test will be performed using test signals.~~to verify the existence of input signals.~~	The SAS receives input signals from the sources listed in Table 2.4.4-2.
4.3	Deleted.~~The SAS provides the output signals to the recipients listed in Table 2.4.4-3.~~	Deleted.~~Tests A test will be performed using test signals.to verify the existence of output signals.~~	Deleted.~~The SAS provides output signals to the recipients listed in Table 2.4.4-3.~~
4.4	The SAS provides the interlocks listed in Table 2.4.4-~~4~~3.	Tests will be performed using test signals ~~to verify the operation of the interlocks listed in Table 2.4.4-4~~.	The interlocks listed in Table 2.4.4-~~4~~3 respond as specified when activated by a test signal.

07.01-37

07.01-37

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.5	The SAS system design and application software are developed using a process composed of six lifecycle phases, with each phase having outputs which must conform to the requirements of that phase. The six lifecycle phases are the following: 1) Basic Design Phase. 2) Detailed Design Phase. 3) Manufacturing Phase. 4) System Integration and Testing Phase 5) Installation and Commissioning Phase. 6) Final Documentation Phase.	a. Analyses will be performed to verify that the outputs for the SAS basic design phase conform to the requirements of that phase.	a. A report ~~exists and~~ concludes that the outputs conform to requirements of the basic design phase of the SAS.
		b. Analyses will be performed to verify that the outputs for the SAS detailed design phase conform to the requirements of that phase.	b. A report ~~exists and~~ concludes that the outputs conform to requirements of the detailed design phase of the SAS.
		c. Analyses will be performed to verify that the outputs for the SAS manufacturing phase conform to the requirements of that phase.	c. A report ~~exists and~~ concludes that the outputs conform to the requirements of the manufacturing phase of the SAS.
		d. Analyses will be performed to verify that the outputs for the SAS system integration and testing phase conform to the requirements of that phase.	d. A report ~~exists and~~ concludes that the outputs conform to the requirements of the system integration and testing phase of the SAS.
		e. Analyses will be performed to verify that the outputs for the SAS installation and commissioning phase conform to the requirements of that phase.	e. A report ~~exists and~~ concludes that the outputs conform to the requirements of the installation and commissioning phase of the SAS.
		f. Analyses will be performed to verify that the outputs for the SAS final documentation phase conform to the requirements of that phase.	f. A report ~~exists and~~ concludes that the outputs conform to the requirements of the final documentation phase of the SAS.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

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

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

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

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.9	Communications independence is provided between SAS equipment and non-Class 1E equipment.	Tests using test signals, analyses, or a combination of tests using test signals and analyses will be performed ~~on the SAS equipment~~.	Communications independence between SAS equipment and non-Class 1E equipment is provided by ~~A report exists and concludes that~~: • Data communications between SAS function processors and non-Class 1E equipment is through a Monitoring and Service Interface (MSI). • The MSI do not interface directly with a network. Separate communication modules interface directly with the network. • Separate send and receive data channels are used in both the communications modules and the MSI. • The MSI operates in a strictly cyclic manner. • The MSI operates asynchronously from the communications modules. • The SAS uses a Class 1E hardware device to ~~ensure that~~ send unidirectional signals ~~are sent~~ to non-safety-related I&C systems.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.10	The SAS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the following: • Single detectable failures within the SAS. • Failures caused by the single failure. • Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.	A failure modes and effects analysis will be performed on the SAS at the level of replaceable modules and components.	A report ~~exists and~~ concludes that the SAS is designed so that safety-related functions required for AOOs or PAs are performed in the presence of the following: • Single detectable failures within the SAS ~~concurrent with identifiable but non-detectable failures~~. • Failures caused by the single failure. • Failures and spurious system actions that cause or are caused by the AOO or PA requiring the safety function.
4.11	The equipment for each SAS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.	Inspections will be performed on the SAS equipment to verify that the equipment for each SAS division is distinctly identified and distinguishable from other markings placed on the equipment and that the identifications do not require frequent use of reference material.	The equipment for each SAS division is distinctly identified and distinguishable from other identifying markings placed on the equipment, and the identifications do not require frequent use of reference material.
4.12	Locking mechanisms are provided on the SAS cabinet doors. Opened SAS cabinet doors are indicated in the MCR.	a. ~~Inspections~~ An inspection will be performed ~~to verify the existence of locking mechanisms on the SAS cabinet doors~~. b. ~~Tests~~ A test will be performed ~~to verify the proper operation of the locking mechanisms on the SAS cabinet doors~~. c. ~~Tests~~ A test ~~and inspections~~ will be performed ~~to verify an indication exists in the MCR when a SAS cabinet door is in the open position~~.	a. Locking mechanisms exist on the SAS cabinet doors. b. The locking mechanisms on the SAS cabinet doors operate properly. c. Opened SAS cabinet doors are indicated in the MCR with an SAS cabinet door is in the open position.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.13	CPU state switches are present at the SAS cabinets to restrict modifications to the SAS software.	a. Inspections will be performed ~~to verify the existence of CPU state switches that restrict modifications to the SAS software~~. b. Tests will be performed ~~to verify that the CPU state switches restrict modifications to the SAS software~~.	a. CPU state switches are provided at the SAS cabinets. b. CPU state switches at the SAS cabinets restrict modifications to the SAS software.
4.14	The SAS is capable of performing its safety function when SAS equipment is in maintenance~~one of the SAS divisions is out of service~~. Bypassed SAS equipment is ~~Out of service divisions of SAS are~~ indicated in the MCR.	a. A test of the SAS will be performed using test signals to verify the maintenance bypass functionality.~~the SAS can perform its safety function when one of the SAS divisions is out of service~~. b. ~~Inspections~~ A test will be performed using test signals to verify the existence of indication in the MCR when ~~a~~ SAS equipment is in maintenance bypass (inoperable).~~division is placed out of service.~~	a. The SAS can perform its safety functions when ~~one of the~~ SAS equipment is in maintenance bypass. ~~divisions is out of service.~~ b. Bypassed SAS equipment is ~~Out of service divisions of SAS are~~ indicated in the MCR.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.15	The operational availability of each input variable listed in Table 2.4.4-2 can be confirmed during reactor operation including post-accident periods by one of the following methods: • By perturbing the monitored variable. • By introducing and varying, a substitute input of the same nature as the measured variable. • By cross-checking between channels that bear a known relationship to each other. • By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.	Analysis will be performed to demonstrate that the operational availability of each input variable listed in Table 2.4.4-2 can be confirmed during reactor operation including post-accident periods. ~~by one of the following methods:~~ ~~•By perturbing the monitored variable.~~ ~~•By introducing and varying, a substitute input of the same nature as the measured variable.~~ ~~•By cross-checking between channels that bear a known relationship to each other.~~ ~~• By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.~~	A report ~~exists and~~ concludes that the operational availability of each input variable listed in Table 2.4.4-2 can be confirmed during reactor operation including post-accident periods by one of the following methods: • By perturbing the monitored variable. • By introducing and varying, a substitute input of the same nature as the measured variable. • By cross-checking between channels that bear a known relationship to each other. • By specifying equipment that is stable and the period of time it retains its calibration during post-accident conditions.
4.16	Deleted.	Deleted.	Deleted.
4.17	Hardwired disconnects exist between the SU and each divisional MSI of the SAS. The hardwired disconnects prevent the connection of the SU to more than a single division of the SAS.	a. Inspections will be performed. ~~on the SAS to verify the existence of hardwired disconnects between the SU and each divisional MSI of SAS.~~ b. Tests will be performed. ~~on the SAS to verify that the hardwired disconnects prevent the connection of the SU to more than a single division of the SAS.~~	a. Hardwired disconnects exist between the SU and each divisional MSI of the SAS. b. The hardwired disconnects prevent the connection of the SU to more than a single division of the SAS.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
4.18	The SAS performs ESF and Essential Auxiliary Support (EAS) automatic functions for the input variables listed in Table 2.4.4-2.~~The SAS performs automatic functions listed in Table 2.4.4-5.~~	A test will be performed on the SAS using test signals.~~Tests A test will be performed using test signals to verify the operation of automatic functions listed in Table 2.4.4-5.~~	The SAS generates ESF and EAS output signals after the application of a test signal for the input variables listed in Table 2.4.4-2. Upon removal of the test signal the ESF and EAS output signals shall reflect the current plant conditions. Deliberate manual action is required to return the SAS to normal.~~The SAS generates the correct output signals for each automatic function listed in Table 2.4.4-5.~~
4.19	During data communication, the SAS function processors receive only the pre-defined messages for that specific function processor. Other messages are ignored.	a. An analysis will be performed. b. A test will be performed.	a. A report determines the test specification for the SAS function processors to verify that only pre-defined messages for that specific function processor and other messages are ignored. b. A report concludes that the SAS function processors receive only the pre-defined messages for that specific function processor. Other messages are ignored.
4.20	SAS self-test features are capable of detecting faults consistent with the requirements of the SAS.	a. Analyses will be performed to determine the faults that require detection through self-test features. b. Type tests, analyses or a combination of type tests and analyses will be performed to verify that faults requiring detection through self-test features are detected by the SAS equipment.	a. A report identifies the faults that require detection through self-test features. b. A report concludes that the SAS equipment is capable of detecting faults required to be detected by self-test features.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
4.21	SAS connections to the SICS are hardwired for manual grouped controls.	Inspections will be performed.	SAS connections to the SICS are hardwired for manual grouped controls.
4.22	SAS manual grouped controls and indications are available on the SICS in the MCR.	a. Inspections will be performed. b. Tests will be performed using test signals.	a. SAS manual grouped controls and indications are available on the SICS in the MCR. b. SAS equipment is capable of operating manual grouped control functions from the SICS in the MCR.
4.23	Permissive P15 provides operating bypass capability for the following SAS functions: • Safety Injection and Heat Removal System - Automatic Trip of LHSI Pump (in RHR Mode) on Low Delta Psat. • Safety Injection and Heat Removal System - Automatic Trip of LHSI Pump (in RHR Mode) on Low Loop Level.	A test will be performed using test signals.	A report concludes that Permissive P15 provides operating bypass capability for the following SAS functions: • Safety Injection and Heat Removal System - Automatic Trip of LHSI Pump (in RHR Mode) on Low Delta Psat. • Safety Injection and Heat Removal System - Automatic Trip of LHSI Pump (in RHR Mode) on Low Loop Level.
5.1	~~Class 1E SAS~~ The components designated as Class 1E in Table 2.4.4-1 are powered from a Class 1E division as listed in Table 2.4.4-1 in a normal or alternate feed condition.	a. Testing will be performed ~~for components identified as Class 1E in Table 2.4.4-1~~ by providing a test signal in each normally aligned division. b. Testing will be performed ~~for components identified as Class 1E in Table 2.4.4-1~~ by providing a test signal in each division with the alternate feed aligned to the divisional pair.	a. The test signal provided in the normally aligned division is present at the respective Class 1E components identified in Table 2.4.4-1. b. The test signal provided in each division with the alternate feed aligned to the divisional pair is present at the respective Class 1E components identified in Table 2.4.4-1.

07.01-37

Table 2.4.4-~~6~~4—Safety Automation System ITAAC (11 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
6.1	Components listed as Class 1E in Table 2.4.4-1 can perform their function under normal environmental conditions, AOOs, and accident and post-accident environmental conditions.	a. Type tests or type tests and analysis will be performed to demonstrate the ability of the components listed as Class 1E in Table 2.4.4-1 to perform their function under normal environmental conditions, AOOs, and accident and post-accident environmental conditions.	a. Environmental Qualification Data Packages (EQDP) conclude that components listed as Class 1E in Table 2.4.4-1 can perform their function under normal environmental conditions, AOOs, and accident and post-accident environmental conditions including the time required to perform their function.
		b. Components listed as Class 1E in Table 2.4.4-1 will be inspected to verify installation in accordance with the EQDP requirements.	b. Inspection reports conclude that components listed as Class 1E in Table 2.4.4-1 are installed per the EQDP requirements.

Next File

7.3 Engineered Safety Features Systems

7.3.1 Description

The U.S. EPR provides safety-related instrumentation and controls to sense accident conditions and automatically initiate the engineered safety features (ESF) systems. ESF systems are automatically actuated when selected variables exceed setpoints that are indicative of conditions that require protective action. Additionally, the ability to manually initiate ESF systems is provided in the main control room (MCR). Manual system-level actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions. The SICS provides controls in the MCR for the manual actuation of the ESF functions listed in Table 7.3-5—Protection System Manually Actuated Functions. Component-level control ESF system actuators is also provided in the MCR.

07.03-38

7.3.1.1 System Description

Automatic actuation of ESF systems and auxiliary supporting systems is performed by the protection system (PS) when selected plant parameters reach the appropriate setpoints. These automatic actuation orders are sent to the priority and actuator control system (PACS) for prioritization and interface to the actuators. An example of an ESF actuation sequence actuated by four divisions of the PS is illustrated in Figure 7.3-1 (Sheet 1), and is described as follows:

- An acquisition and processing unit (APU) in each division acquires one-fourth of the redundant sensor measurements through the signal conditioning and distribution system (SCDS) that are inputs to a given ESF actuation function.
- The APU in each division performs any required processing using the measurements acquired by that division (e.g., filtering, range conversion, calculations). The resulting variable is compared to a relevant actuation setpoint in each division. If a setpoint is breached, the APU in that division generates a partial trigger signal for the appropriate ESF function.
- The partial trigger signals from each division are sent to redundant actuation logic units (ALU) in the PS division responsible for the associated actuation. Two out of four voting is performed in each ALU on the partial trigger signals from all four divisions. If the voting logic is satisfied, an actuation order is generated.
- The actuation signals of the redundant ALU in each subsystem are combined in a hardwired "functional OR" configuration so that either redundant ALU can actuate the function.

ESF functions actuated by less than four divisions are illustrated in Figure 7.3-1 (Sheets 3 through 5).

modified to disregard the input being tested. The ESF actuation functions are still performed using the redundant input channels.

07.01-41

The connections between the PS output circuits and the PACS priority modules can be tested during power operation. One function of one division of the PS is tested at a time and the outputs of the PACS priority modules are disabled (no actuation signals can be sent) so that the actuators are not affected by the test. The PACS priority modules are disabled for five seconds and then they automatically exit the test mode and enable (allows actuation signals to be sent) their outputs. If an ESF actuation order is generated during the time that a PACS priority module is in test mode, the outputs of the PACS priority module remain disabled until the PACS priority module exits the test mode. The ESF actuation functions are still performed using the other PS divisions.

The testing of the PS is described in the U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report (ANP-10315P) (Reference 7).

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

The automatic ESF actuation functions are implemented using the TELEPERM XS platform (Reference 2) which is approved for use in safety-related systems of nuclear power generating stations in the United States. The ESF actuation functions are implemented in an architecture designed to satisfy requirements applicable to all safety-related I&C systems.

Implementation of safety-related I&C systems is governed by the requirements of IEEE Std 603-1998 (Reference 5). Compliance with this requirement is described in Section 7.1. Guidance on the use of digital computers in safety-related systems is provided by IEEE Std 7-4.3.2-2003 (Reference 6). Conformance to this guidance is described in Section 7.1.

7.3.2.3.8 Compliance with Requirements for ESF Actuation Setpoint Determination (Clause 6.8 of IEEE Std 603-1998)

Each setpoint used to actuate an ESF system is selected based on the safety limits assumed in the plant accident analysis. The ESF actuation setpoints provide margin to the safety limit and take into account measurement uncertainties. The methodology to determine setpoints for ESF actuation functions is documented in the U.S. EPR Instrument Setpoint Topical Report (ANP-10275P-A) (Reference 4). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

Table 7.3-5—Protection System Manually Actuated Functions

Reactor Trip
Containment Isolation (Stage 1)
Containment Isolation (Stage 2)
CVCS Charging Isolation
CVCS Isolation on Anti-Dilution Mitigation
EDG Actuation
EFWS Actuation
EFWS Isolation
Extra Borating System Isolation
Hydrogen Mixing Dampers Opening
CRACS Isolation and Filtering
Main Feedwater (MFW) Full Load Isolation
Main Steam Isolation
MSRIV Opening
MSRT Isolation
Partial Cooldown Actuation
PSRV Opening
RCP Trip
SG Isolation
SIS Actuation
Turbine Trip

07.03-38

07.01-41

Above a predetermined power level, the AO control can be enabled~~activated~~. If the AO exceeds a power dependant positive value, a dilution batch will be requested. This effectively raises the core-wide power and average coolant temperature, which causes the ACT control to insert rods, thereby correcting the AO. If the AO exceeds a power dependant negative value, a boration batch will be requested. This effectively lowers the core-wide power and average coolant temperature, which causes the ACT control to withdraw rods and correct the AO.

7.7.2.2 Operational Plant Control Functions

7.7.2.2.1 RCS Pressure Control

The RCS pressure control maintains the RCS pressure within allowable limits during Mode 1 through Mode 5. When in the automatic control mode, the RCS pressure control maintains the primary pressure at a setpoint value in steady-state operation and within an allowable range around its setpoint (i.e., control band) during transients, including startup and cooldown operations. Figure 7.7-3—RCS Pressure Setpoints indicates the control band relative to other RCS pressure setpoints.

When the automatic heatup and cooldown mode is selected, the RCS pressure control has an automatically generated temperature dependent setpoint. The automatic heatup and cooldown mode is selected during plant Mode 2 and Mode 3. The primary pressure is required to stay in an allowable range around the automatically generated setpoint. If the pressure drifts from the limits of the setpoint, the Max2 sliding pressure limitation function described in Section 7.7.2.3.11 is actuated. If the pressure progresses further from the temperature dependent setpoint to the high pressure (HP) or low pressure (LP) locking setpoints, the automatic heatup and cooldown is interrupted, and an alarm is sent to PICS.

RCS pressure control is performed by actuating pressurizer (PZR) heaters or PZR normal spray.

A manual control mode allows manual setpoint control and manual control of the actuators.

7.7.2.2.2 Pressurizer Level Control

The PZR level control provides:

- Sufficient RCS water inventory for cooling and for proper control of RCS pressure.
- A sufficient steam volume in the PZR to accommodate in-surges in the PZR from the RCS without causing an excessive pressure increase for normal operating transients. There is also sufficient water mass to accommodate out-surges from the PZR to the RCS without causing an excessive pressure decrease.

The function of the PZR level control is to maintain the PZR level at a setpoint value in steady-state operation and within the allowable range around its setpoints during normal operational situations, including startup and cooldown. When in automatic control mode, PZR level control channel makes sure that the PZR level remains within given limits (i.e., control band) around the setpoint. Figure 7.7-4—Pressurizer Level Setpoints indicates the control band relative to other PZR level setpoints.

The PZR level control monitors the PZR level for deviations from its setpoint during Mode 1 through Mode 4, and based on mode changes, actuates different control valves at the pressure reducing stations located in the CVCS letdown lines.

A manual control mode allows manual setpoint control and manual control of the pressure reducing valve actuators.

7.7.2.2.3 RCS Loop Level Control

The RCS loop level control function provides an automatic and continuous control of the RCS water inventory during mid-loop operation. In case of primary system inventory changes, the control function limits the resulting mid-loop operation level deviations within the specified control band.

The loop level control function provides an automatic control of RCS water inventory by continuously monitoring the RCS loop level and controlling the coolant letdown flowrate.

RCS loop level control is maintained by a closed-loop control I&C function, which is put in service manually at cold shutdown conditions.

07.01-41

RCS loop level control is manually enabled~~activated~~ at cold shutdown conditions. Control actions are only effective when an HP charging pump is in operation and the volume control tank (VCT) bypass line is not opened.

7.7.2.2.4 Steam Generator Level Control

The steam generator (SG) water level control automatically maintains SG level by matching feedwater flow to steam demand. The level can also be controlled manually.

This SG level control I&C function provide the following:

- Sufficient water level for heat removal from the primary to secondary side.
- Minimizes moisture carryover to the turbine.

The SG level control I&C function maintains the SG level at a setpoint value in steady-state operation during heatup and cooldown (Mode 1 through Mode 4), and within allowable limits (called the control band) during normal operational transients.

Loss of One MFW Pump (if standby pump not available)

This limitation function deals with the loss of one MFW pump (if standby pump not available) by initiating a PT and a turbine load reduction. An imbalance between MFW flowrate and a nominal MFW flowrate (according to feedwater temperature and reactor power) initiates~~activates~~ a PT and a generator power reduction to a power level corresponding to operation with two MFW pumps.

07.01-41

Loss of All MFW Pumps

A low MFW flowrate combined with a high reactor power level is the criteria for the detection of the loss of all MFW pumps. In this case the limitation function will initiate a non-safety-related reactor trip, initiates~~activate~~ turbine trip, and close all FW FLCVs. The reactor trip signal resets this actuation.

Imbalance of Feedwater Flowrate and Reactor Power During Startup Phase

Indications of a low enough feedwater flowrate and a high enough reactor power leads to blocking the withdrawal of any RCCA. This prevents an increase of the reactor power without an increase of the MFW flowrate during the startup phase.

7.7.2.3.4 Reactor Power Limitation with respect to Generator Power

This limitation function limits reactor power after loss of generator load events. The objective is to limit the energy level of the primary system in case of load rejections or turbine trip in order to avoid reaching the RT criteria. This will be done by initiating a PT. The target reactor power level is determined by:

- The maximum of generator power.
- The minimum PT target power.

In case of turbine trip or load rejection to house load, the plant is first stabilized at minimum PT target power while heat removal is performed via the turbine bypass valves. A further controlled reduction to the minimum load reactor power will then be done by ACT control.

7.7.2.3.5 Reactor Power Limitation with respect to Thermal Power

The reactor power limitation with respect to thermal power function is designed to maintain reactor power below 100 percent rated thermal power. This function provides the capability to adjust turbine power and indirectly reactor power due to cooling tower temperature changes that affect overall plant efficiencies. The reactor power signal is selected from the highest of the following:

- Continuous secondary calorimetric calculation (i.e., above 25 percent power).

interface, where it is compared to the permissible shutdown state boron concentration. The low concentration limitation threshold is generated in the RCSL at a higher threshold than the antidilution at a shutdown condition state protection criterion. When the limitation signals are generated in two out of four RCSL divisions, the following actions are initiated:

- Boron addition with maximum injection rate.
- Isolation of demineralized water injection lines of the reactor boron and water makeup system (RBWMS). Both demineralized water injection pumps are shut off and both control valves are closed with highest priority.

The second sub-function is enabled~~activated~~ when shutdown conditions are detected (reactor trip or no RCPs running). In this sub-function, boron concentration injected by RBWMS is measured. If the injected concentration is below the permissible value then the demineralized water injection lines will be isolated.

07.01-41

7.7.2.3.11 Reactor Coolant System Pressure Limitations

When the RCS pressure goes out of the normal operating range, the following RCS pressure limitation functions are enabled~~can be activated~~. These functions are designed to correct RCS pressure transients before a RT setpoint is reached, or to protect equipment. These functions have a more stringent action than the RCS pressure control function as described in Section 7.7.2.2.1. A graphical presentation of the RCS pressure limitation setpoints in relation to protective function setpoints and the control band is presented in Figure 7.7-3.

In case of post-accident operations, the operator is able to inhibit the activation of the RCS pressure limitation functions from PICS.

Max2 Pressure Function

The Max2 pressure function improves the availability of the plant by avoiding an RT on the Max2p setpoint (i.e., high PZR pressure). When the RCS pressure measurement reaches the setpoint, this function de-energizes the PZR heaters and actuates the normal spray. If the normal spray is not functional, auxiliary spray is actuated. The normal spray availability is determined based on RCP speed or the loop flowrate.

This function is operational in Mode 1 through Mode 3.

Max2 Sliding Pressure Function

The Max2 sliding pressure function improves plant availability by preventing a lock of the automatic heatup and cooldown on Max2p and limits the temperature differences between the PZR and RCS loops. The Max2 sliding pressure function is similar to the

In case of post-accident operations, the operator is able to inhibit the activation of this function from PICS.

Min3 Level Function

The Min3 level function protects the PZR heaters from being uncovered and is designed to prevent severe damage to the PZR heaters and also a potential breach of the RCS. When the PZR level reaches the Min3 function level setpoint, the PZR heaters are de-energized. An alarm on PICS indicates that the Min3 level function has been actuated. When the PZR level returns above the Min3 level setpoint, the PZR heaters are automatically switched back to RCS pressure control.

This function is operational during all plant modes.

The Min3 level function cannot be inhibited.

7.7.2.3.13 Reactor Coolant System Loop Level Limitation

The RCS loop level limitation function continuously monitors the loop level during mid-loop operation.

The RCS loop level limitation function makes sure that the minimum and maximum admissible water levels are in the RCS loops in case of transients. This limitation function acts when an overshoot of the control band limit occurs. This function prevents the actuation of safety functions by the PS.

The RCS loop level limitation function considers the water level required to protect the low head safety injection (LHSI) pumps from cavitation during mid loop operation.

This limitation function also prevents inadvertent filling of the loops. Filling the loops interrupts the flow area for the purge gas in the loop and the necessary free water surface for removal of noble gas. This could endanger personnel working in the SG bowls, and could potentially discharge coolant to the containment via open SG man-ways.

The RCS loop level limitation function fully closes the LP and HP reducing station of the CVCS letdown line when the RCS water level falls below a dedicated threshold that is below the lower control band limit of the RCS loop level control function. This limitation function fully opens the LP reducing stations to increase the coolant letdown flowrate when the water level exceeds a dedicated threshold above the upper control band limit of the RCS loop level control function. Both the upper and lower thresholds of this function are constant.

07.01-41

The limitation function is automatically enabled~~activated~~ during the plant shutdown procedure when the operating range of the LHSI RHRS is reached.

Low SG Level Limitation Function

The low SG level limitation function avoids RT at Min1p and returns the SG level to its normal operating range. This function has higher priority over the SG level control function described in Section 7.7.2.2.4.

This function is operable in Mode 1 through Mode 4.

This function receives input from SG level (NR) and reactor power.

The low SG level limitation function defines a movable setpoint Min c1, set at a constant distance below the SG level control function setpoint and above the safety setpoint Min1p. The Min c1 setpoint is designed to be movable at a constant distance from the SG level control function setpoint to prevent undesired actuation of the low SG level safety function during SG level setpoint reduction before an RCP restart.

When the SG level is less than Min c1 and reactor power is less than 20 percent, an open order is sent to the LLCV. SG level is controlled by the LLCV at this power level. The open order to the LLCV is maintained as long as the water level is less than the Min c1 setpoint. Once the level increases above than Min c1 setpoint, the control of the LLCV returns back to the automatic control mode.

When the SG level is less than Min c1 and reactor power is greater than 20 percent, an open order is sent to the FLCV and the LLCV. The open orders are maintained to both valves as long as the water level is less than the Min c1 setpoint. Once the level increases above than Min c1 setpoint, the control of the FLCV and the LLCV return back to the automatic control mode.

Very Low Flow SG Level Limitation Function

07.01-41

The very low flow SG level limitation function disables~~deactivates~~ the VLLCV signal stop and returns the SG level to the normal operating range. It has higher priority over the SG level control function described in Section 7.7.2.2.4.

This function is operable in Mode 2 and Mode 3.

The very low flow SG level limitation function disables~~deactivates~~ the VLLCV signal stop, which provides the minimum position limitation during the startup and shutdown phases. The FLCV and LLCV are manually closed during Mode 2 and Mode 3 and therefore the FLCV and LLCV are not controlled by this limitation function.

To prevent water hammer and thermal stratification phenomena on the SG feedwater nozzle, the VLLCV signal stop guarantees a minimum continuous feedwater flowrate by preventing the VLLCV from closing below the minimum flow position. However, this could potentially cause a high water level in the SG.

07.01-41

When the SG level is greater than the Max c1 setpoint, the VLLCV signal stop is disabled~~deactivated~~ and close orders are sent to the VLLCV. Once the SG level drops below the Max c1 setpoint, the VLLCV returns to the automatic control mode.

7.7.2.4 Non-Safety Control Systems Described in Other Sections

Table 7.7-1 provides a cross-reference to other sections of the final safety analysis report (FSAR) that contain information on I&C that support non-safety-related functions. The functions listed in Table 7.7-1 do not have direct influence on the process of nuclear power generation.

7.7.2.5 Safety Classification

With the exception of the SCDS, the I&C systems described in Section 7.7.1.1 and Section 7.7.1.2 are non-safety-related. The functions that these systems implement provide control of important parameters, but are not necessary to provide protection against AOOs and PAs. The SCDS serves only as the instrumentation interface and does not perform core control and plant control functions.

7.7.2.6 Effects of Control System Operation Upon Accidents

The effects of non-safety-related control system action and inaction on the transient response of the plant for AOOs and PAs are considered in the safety analysis addressed in Chapter 15.

The non-safety-related control functions maintain the major process variables of the NSSS in predefined and allowed ranges during normal power operation. The proper operation of the non-safety-related control functions is not necessary to provide protection against accidents.

7.7.2.7 Effects of Control System Failures

The effects of control system failures are minimized by the features described in this section.

Functions assigned to RCSL and PAS are redundant in more than one division. The failure of a function in one division is backed up by a redundant function in another division. The redundant functions and their associated equipment, including support systems are independent of each other. Independence is achieved by the following:

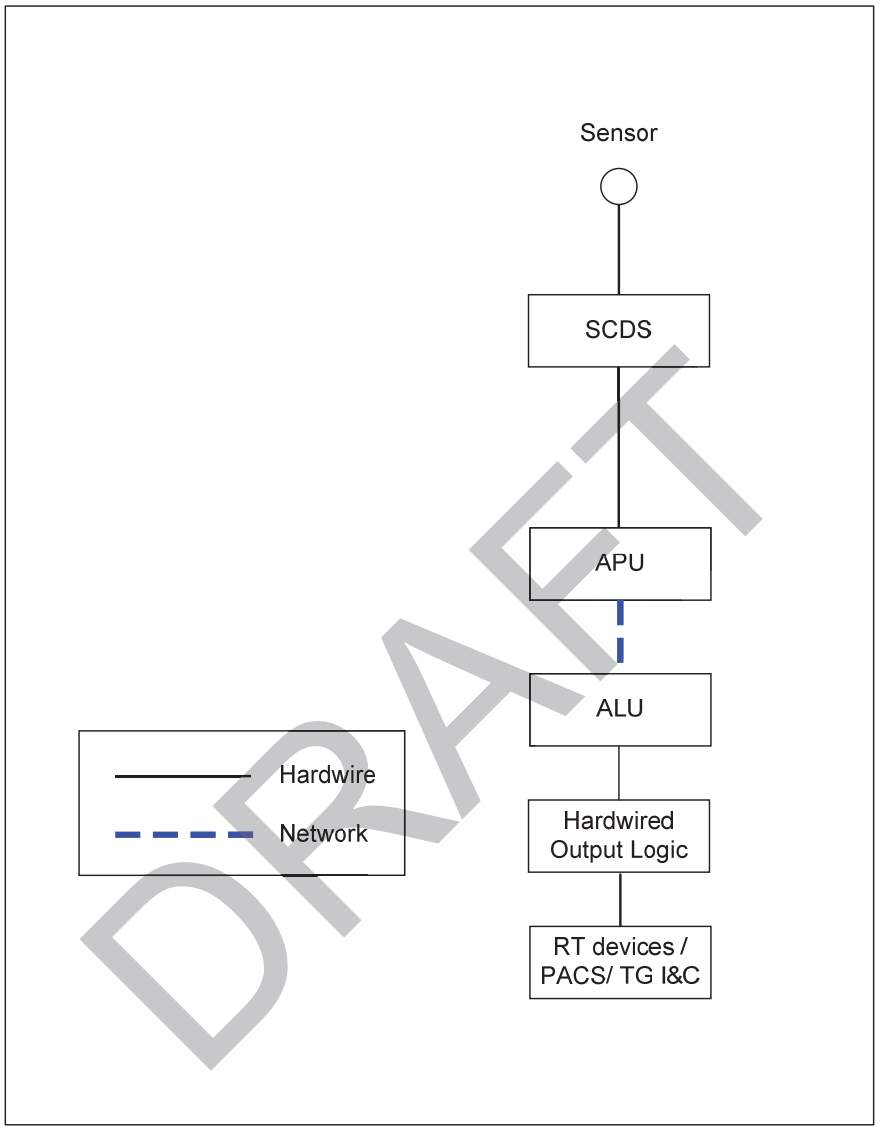
- Redundant functions are allocated to physically separated divisions.
- Electrical isolation between divisions.
- Erroneous signals or messages from one faulty division do not impair the functionality of the remaining divisions.

U.S. EPR™ Protection System

Technical Report ANP-10309

MARKUPS

Figure A.1—PS Component Interface



Consideration of Maintenance

GDC 21 (Reference 2) requires, in part, that "removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated." For this reason, the FMEA of the PS is performed considering inoperable (see U.S. EPR FSAR Tier 2, Table 7.1-6, for functional processor operational states) components due to preventative or corrective maintenance. The

07.01-41

A.3.3 Permissive Functions Results

The results of the U.S. EPR™ PS Permissive Functions FMEA are shown in Tables A.3-2 through A.3-14.

Permissive P8

The Permissive P8 function has failure modes that allow the permissive to be in the incorrect state during certain plant conditions.

These failure modes have been reviewed by safety analysis to verify that they force the affected protection functions in the conservative direction. The results of this assessment are as follows:

The worst case failure results in one half of the sensors not providing input into the permissive status. This does not result in the permissive having the incorrect state during operation with rods out. However, when rods are in the process of inserting, a situation may occur when the P8 validated signal is sent (indicating all shutdown RCCA are in), but some shutdown RCCA are not fully inserted.

Permissive P8 provides input to the selection of the setpoint for the CVCS isolation for anti-dilution isolation function. In this case it selects between power and shutdown conditions based on rod insertion. Based on the above FMEA result, it is possible to have a situation where not all rods are in but the appearance is given to enable~~activate~~ the anti-dilution shutdown state. The anti-dilution shutdown state setpoint is further selected based on RCPs running or not running (see permissive P7). With the RCPs running (at power and shutdown) the anti-dilution setpoint is based on assuming the most reactive rod is stuck out of the core. At power, the setpoint is based on when shutdown margin is lost and the rods can no longer shutdown the reactor. In the shutdown mode, the setpoint is based on the approach to critical. If rods are in the process of being inserted then the reactor is actually in the shutdown state. As long as no more than one rod is out of the core the analysis remains valid and the failure mode

07.01-41

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

Technical Report ANP-10315

MARKUPS

Different methods are used to perform ADOT for ~~ESFAS~~ ESF (ESFAS and ESF control) functions and RT functions.

2.2.5.1 *ADOT for ESFAS Actuators*

07.01-41

For ESF~~AS~~ actuators, two overlapping tests (i.e., no-go test and go test) are used to provide test coverage of each component between the PS and SAS outputs and the actuator. In a no-go test, the PS and SAS outputs are activated (actuation signals are sent) and acquired by the PACS priority module, but the outputs of the priority module are blocked to prevent the actuator from responding. In a go test, the non-safety-related I&C is used to exercise the actuator via the PACS priority module. The ADOT confirms both the functional capability and response time of the equipment between the PS outputs and the actuator. The ADOT confirms the functional capability of the equipment between the SAS outputs and the actuator.

2.2.5.1.1 ESF~~AS~~ "No-Go" ADOT

Each ESF~~AS~~ actuator has a dedicated PACS priority module. For a given ESF~~AS~~ function, the PS or SAS sends actuation signals to the priority modules corresponding to the actuators required for that function. The no-go test duplicates this functionality by prompting the PS or SAS to send actuation outputs to all priority modules involved in a particular ESF~~AS~~ function. Priority modules receiving ESF~~AS~~ signals are tested functionally on a single processor in a single division. A single input function and all related outputs from the processor are verified in a single test. The test is initiated via the respective system's SU and performed by dedicated logic in the ALU or CU application software.

Figure 2-5 shows logic that could be used to perform a no-go test. The example in Figure 2-5 (Sheet 1) is for an ESFAS function that includes three actuators. When the test release parameter has been set to "1," the test is initiated. A dedicated ALU output is generated to block the output of the priority module to prevent the actuator from responding. The blocking signal from the ALU output initiates a 5 second test mode in the priority module of the PACS, where the outputs of the priority module of the PACS

are blocked (via a logic AND). If a legitimate protection function is initiated during this 5 second test mode, the outputs of the priority module of the PACS remain blocked. After the 5 seconds, the priority module of the PACS automatically exits the test mode, and the outputs of the priority module become enabled (actuation signals can be sent). One function of one division of the PS is tested at a time. If a legitimate protection function is initiated during a test, then the other PS divisions will execute the protection function. One second after the test is initiated, the ALU actuation outputs for the ESFAS function are activated (actuation signals are sent) for three seconds and sent to the group of priority modules involved in the function being tested. This results in 1 second between when the priority module of the PACS enters test mode, and the ALU actuation outputs for the ESFAS function are activated. This also results in 1 second between when the ALU actuation outputs for the ESFAS function are deactivated (actuation signals are removed), and the priority module of the PACS exits test mode. This ALU output is acquired by ~~a~~ the test machine, via a permanently installed test connection, to verify that the ALU output is generated and to start a timer. The output of each priority module is also acquired by the test machine, via a permanently installed test connection, to verify that the signal was processed correctly by the priority logic and to stop the timer. In this way, the functionality of the ALU output module, wiring between the ALU and priority module, and the priority logic are verified. The response time of each priority module is also verified.

07.01-41

The primary reason a test machine is needed for this test is to verify the response time of the priority logic. ~~A COL applicant referencing the U.S. EPR standard design may propose to exclude the priority logic from periodic response time testing. This would require the applicant to submit a topical report justifying that approach.~~

If the priority logic is excluded from response time testing because there is no response time requirement for this equipment, then the priority logic outputs can be wired to the monitoring service interface (MSI), and the functionality verified via the SU. The SAS does not have any response time surveillance requirements, therefore for the ESF control functions' "No-Go" test, the test machine is not utilized. This configuration is shown in Figure 2-5 (Sheet 2).~~If the priority logic is excluded from response time testing~~

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

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

2.2.6.3 *Exception-Handler (Inherent)*

The exception-~~-~~handler is activated when exceptional situations are encountered during runtime (also in case of a fault detected by the cyclic self-test). After activation, the exception-handler deactivates all output boards through driver calls (provides no outputs), and cyclic communication is stopped. Self monitoring result information is saved, which includes: exception type, exception number, exception address, memory dump and stack dump.

07.01-41

Depending on the type of fault, the exception-handler either resets or halts (the processor enters a defined fault state and all output signals are set to predetermined safe states. See Technical Report ANP-10309P for information associated with failure states) the function processor, as indicated. If a second exceptional situation occurs within a specified period after a reset (depends on cycle time: e.g., 5 minutes for a 50 ms cycle), the function processor is ~~deactivated~~shutdown. Tables 2-2, 2-3, and 2-4 show the exceptional situations that activate the exception-~~-~~handler.