ArevaEPRDCPEm Resource

From: WELLS Russell (AREVA) [Russell.Wells@areva.com]
Sent: Monday, March 21, 2011 4:28 PM
To: Tesfaye, Getachew
Cc: HUDSON Greg (AREVA); BUDZIK Dennis (AREVA); BENNETT Kathy (AREVA); DELANO Karen (AREVA); HALLINGER Pat (EXTERNAL AREVA); ROMINE Judy (AREVA); RYAN Tom (AREVA); WILLIFORD Dennis (AREVA)
Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Question 7.1-26
Attachments: RAI 442 Question 07.01-26 Response US EPR DC - DRAFT.pdf

Getachew,

Attached is a draft response for RAI No. 442, FSAR Ch. 7, Question 7.1-26 as shown below in advance of the April 21, 2011 final date. Proposed changes to the instrumentation and controls (I&C) architecture were communicated to the NRC staff in the February 15, 2011 public meeting. U.S. EPR FSAR Tier 2, Section 7.1 attached to this response incorporate the revised I&C architecture. This section is provided in its entirety with this response to facilitate NRC review.

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

Thanks,

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

From: WELLS Russell (RS/NB)
Sent: Tuesday, March 15, 2011 12:51 PM
To: 'Tesfaye, Getachew'
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Supplement 6

Getachew,

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

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

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

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

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

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

Sincerely,

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

From: WELLS Russell (RS/NB)
Sent: Wednesday, March 02, 2011 4:52 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Supplement 5

Getachew,

On November 19, 2010, AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to the questions in RAI 442. Supplement 1 response was sent on January 7, 2011 to provide a revised schedule for four of the questions. Supplement 2 response was sent on February 9, 2011 to provide a revised schedule. Supplement 3 response was sent on February 18, 2011 to provide technically correct and complete responses to four questions. Supplement 4 response was sent on February 25, 2011 to provide technically correct and complete response to one question. Based on discussions with NRC, the attached file, "RAI 442 Supplement 5 Response US EPR DC.pdf" provides technically correct and complete responses to three of the 12 questions, as committed.

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

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

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

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

Sincerely,

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

From: WELLS Russell (RS/NB)
Sent: Friday, February 25, 2011 8:07 AM
To: Tesfaye, Getachew
Cc: BRYAN Martin (External RS/NB); BENNETT Kathy (RS/NB); DELANO Karen (RS/NB); ROMINE Judy (RS/NB); RYAN Tom (RS/NB)
Subject: Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Supplement 4

Getachew,

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

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

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

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

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

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

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

Sincerely,

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

Russell.Wells@Areva.com

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

Getachew,

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

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

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

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

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

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

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

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

Sincerely,

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

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

Getachew,

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

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

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

Sincerely,

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

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

Getachew,

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

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

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

Sincerely,

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

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

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

Getachew,

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

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

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

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

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

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

Sincerely,

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

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

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

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 2727

Mail Envelope Properties (1F1CC1BBDC66B842A46CAC03D6B1CD410420F9B0)

Subject: DRAFT Response to U.S. EPR Design Certification Application RAI No. 442, FSAR Ch. 7, Question 7.1-26
Sent Date: 3/21/2011 4:28:24 PM
Received Date: 3/21/2011 4:28:48 PM
From: WELLS Russell (AREVA)

Created By: Russell.Wells@areva.com

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

Post Office: AUSLYNCMX02.adom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	18415	3/21/2011 4:28:48 PM
RAI 442 Question 07.01-26 Response US EPR DC - DRAFT.pdf	1100988	

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

Response to

Request for Additional Information No. 442, Question 07.01-26

10/20/2010

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.01 - Instrumentation and Controls - Introduction
SRP Section: 07.03 - Engineered Safety Features Systems
SRP Section: 07.09 - Data Communication Systems

Application Section: FSAR Ch 7

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

Question 07.01-26:

Provide sufficient information for the staff to conclude that the safety-related standalone or packaged systems provide sufficient independence between those standalone systems and other safety or non-safety systems.

10 CFR 50.55a(h) (Clause 5.6 of IEEE Std. 603-1991) requires addressing the independence between safety systems and other systems. U.S. EPR FSAR Subsection 7.1.1.5 states that Level 0 interface level includes components such as sensors, actuators, and switchgear. However, in this subsection there are also a few safety standalone or packaged systems. The staff requests the applicant to include sufficient design information to address all aspects of independence for those standalone I&C systems. In addition, clarify how those standalone I&C systems are connected in Figure 7.1-2 of the FSAR and what kind of platform or system interfaces will be used for the safety-related standalone systems to achieve the necessary independence.

Response to Question 07.01-26:

In the revised instrumentation and controls (I&C) architecture, Level 0 systems have been renamed as “Dedicated I&C Systems.” These systems are not part of the distributed control system (DCS), but they interface with the DCS as shown in U.S. EPR FSAR Tier 2, Figure 7.1-2. The equipment used in the safety-related I&C systems is qualified to withstand the effects of design basis events (DBEs).

The signal conditioning and distribution system (SCDS) is a safety-related system that contains both safety-related and non-safety-related components. The function of the SCDS is to receive input signals from dedicated I&C systems and provide conditioned, standard analog output signals to multiple DCS subsystems. This signal conditioning is performed with conventional, non-digital, non-microprocessor based modules. The SCDS is organized into four divisions, and each division is located in a separate Safeguards Building.

Inputs to the SCDS from dedicated I&C systems are hardwired connections. Outputs from the SCDS to multiple DCS subsystems are sent through hardwired connections. The SCDS utilizes qualified isolation devices to verify that IEEE 603-1991, Clause 5.6 requirements for separation between safety-related and non-safety-related equipment is maintained.

The SCDS does not share signals between divisions, and there is no interdivisional communication.

The following standalone systems perform safety-related functions and interface with the DCS:

1. Control rod drive control system (CRDCS):

   The CRDCS contactor modules receive electrically isolated, hardwired reactor trip (RT) signals from the protection system (PS) to open the trip contactors.

   The contactor modules in the CRDCS are qualified to Class 1E standards and are physically separated and electrically isolated from the non-safety-related portions of the CRDCS.

The CRDCS does not share signals between divisions, and there is no interdivisional communication.

2. Incore instrumentation system:

   The incore instrumentation cabinets are organized into four redundant divisions located in separate Safeguards Buildings and send 72 self-powered neutron detector (SPND) output signals and 36 core outlet thermocouples signals to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

   The safety-related portions of the incore instrumentation system are electrically isolated from the non-safety-related portions of the incore instrumentation system.

   The incore instrumentation system does not share signals between divisions, and there is no interdivisional communication.

   An alternative request to use a conservative setpoint methodology to satisfy single failure considerations as an alternative for independence between redundant divisions in IEEE 603-1991, Clause 5.6.1 will be submitted under separate letter.

3. Excore instrumentation system:

   The excore instrumentation system cabinets are organized into four redundant divisions located in separate Safeguards Buildings and send intermediate range and power range detector signals to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

   The excore instrumentation system does not share signals between divisions, and there is no interdivisional communication.

4. Rod position measurement system (RPMS):

   The RMPS cabinets are organized into four redundant divisions located in separate Safeguards Buildings and contain the rod position measurement units (RPMU) located in the RPMS cabinets. Rod position measurement signals are sent to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

   The RMPS does not share signals between divisions, and there is no interdivisional communication.

5. Boron concentration measurement system (BCMS):

   The BCMS cabinets are organized into four redundant divisions located in separate Safeguards Buildings and send boron concentration measurement signals to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

   The BCMS does not share signals between divisions, and there is no interdivisional communication.

6. Radiation monitoring system (RMS):

   The RMS consists of multiple types of radiation monitors located throughout the footprint of the plant, depending on their required application for local radiation measurement.

Redundant safety-related monitors are independent of and physically separate from each other.

Radiation measurement signals are sent to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

The safety-related portions of the RMS are electrically isolated from the non-safety-related portions of the RMS.

The RMS does not share signals between monitors, and there is no interdivisional communication.

7. Hydrogen monitoring system (HMS):

   The HMS cabinets are organized into two redundant divisions located in Safeguards Buildings 1 and 4. The HMS sends signals of the containment atmosphere hydrogen concentration to the SCDS for distribution to the DCS through electrically isolated, hardwired connections.

   The safety-related portions of the RMS are electrically isolated from the non-safety-related portions of the RMS.

   The HMS does not share signals between divisions, and there is no interdivisional communication.

Proposed changes to the I&C architecture were communicated to the NRC staff in the February 15, 2011 public meeting. U.S. EPR FSAR Tier 2, Section 7.1 will be revised to incorporate the revised I&C architecture. This section is provided in its entirety with this response to facilitate NRC review.

FSAR Impact:

U.S. EPR FSAR Tier 2, Section 7.1 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

Table 1.1-1—U.S. EPR FSAR Acronyms and Descriptions
Sheet 4 of 20

Acronym	Description
CRDMPSS	Control Rod Drive Mechanism Power Supply System
CRE	Control Room Envelope
CREF	Control Room Emergency Filtration
CRGA	Control Rod Guide Assembly
CS	Conventional Seismic
CSDRS	Certified Seismic Design Response Spectra
CSSS	Coolant Supply and Storage System
CT	Compact Tension
CTCS	Condenser Tube Cleaning System
CTS	Coolant Treatment System
CU	Control Unit
CVCS	Chemical and Volume Control System
CWPB	Circulating Water Pump Building
CWS	Circulating Water System
D-RAP	Design-Reliability Assurance Program
DAC	Design Acceptance Criteria
DAS	Diverse Actuation System
DBA	Design Basis Accident
DBE	Design Basis Event
DBT	Design Basis Threat
DCH	Direct Containment Heating
DCS	Distributed Control System 07.01-26
DDT	Deflagration-to-Detonation Transition
DE	Dose Equivalent
DET	Decomposition Event Tree
DGAIES	Diesel Generator Air Intake and Exhaust System
DGCWS	Diesel Generator Cooling Water System
DGFOSTS	Diesel Generator Fuel Oil Storage and Transfer System
DGLS	Diesel Generator Lubricating (Oil) System
DGSAS	Diesel Generator Starting Air System
DLF	Dynamic Load Factor
DLS	Diesel Load Steps
DNB	Departure from Nucleate Boiling

Table 1.1-1—U.S. EPR FSAR Acronyms and Descriptions
Sheet 15 of 20

Acronym	Description
RAP	Reliability Assurance Program
RAU	Remote Acquisition Units
RAW	Risk Achievement Worth
RB	Reactor Building
RBIS	Reactor Building Internal Structures
RBWMS	Reactor Boron and Water Makeup System
RC	Release Category
RCA	Radiologically Controlled Area
RCB	Reactor Containment Building
RCCA	Rod Cluster Control Assembly
RCDT	Reactor Coolant Drain Tank
RCL	Reactor Coolant Loop
RCP	Reactor Coolant Pump
RCPB	Reactor Coolant Pressure Boundary
RCS	Reactor Coolant System
RCSL	Reactor Control, Surveillance and Limitation
RFI	Radio Frequency Interference
RG	Regulatory Guide
RHR	Residual Heat Removal
RHRS	Residual Heat Removal System
RLE	Review Level Earthquake
RM	Refueling Machine
RMI	Reflective Metallic Insulation
$RMS_{(EQUATIONS)}$	Root Mean Square
$RMS_{(TEXT)}$	Radiation Monitoring System
RPMS	Rod Position Measurement System
RPS	Reactor Protection System
RPV	Reactor Pressure Vessel
RPVDT	Reactor Pressure Vessel Dome Temperature
RPVL	Reactor Pressure Vessel Level
RR	Rod Return
RRS	Required Response Spectra
RS	Radwaste Seismic

07.01-26

Table 1.1-1—U.S. EPR FSAR Acronyms and Descriptions
Sheet 16 of 20

Acronym	Description
RSB	Reactor Shield Building
RSS	Remote Shutdown Station
RT	Reactor Trip
RT_{NDT}	Reference Temperature
RTNSS	Regulatory Treatment of Non-Safety Systems
RTP	Rated Thermal Power
RV	Reactor Vessel
RWB	Radioactive Waste (Processing) Building
RWBVS	Radioactive Waste Building Ventilation System
RWSS	Raw Water Supply System
SA	Severe Accident
SADV	Severe Accident Depressurization Valves
SAFDL	Specified Acceptable Fuel Design Limits
SAHRS	Severe Accident Heat Removal System
SAM	Severe Accident Management
SAMDA	Severe Accident Mitigation Design Alternatives
SAMG	Severe Accident Mitigation Guideline
SAMS	Sampling Activity Monitoring System
SAS	Safety Automation System
SASS	Severe Accident Sampling System
SAT	Systematic Approach to Training
SB	Safeguard Building
SBA	Small Pipe Break Accident
SBLOCA	Small Break Loss of Coolant Accident
SBO	Station Blackout
SBODG	Station Blackout Diesel Generator
SBORVS	Station Blackout Room Ventilation System
SBVS	Safeguard Building (Controlled Area) Ventilation System
SBVSE	Safeguard Building Ventilation System (Electrical)
SCBA	Self-Contained Breathing Apparatus
SCC	Stress Corrosion Cracking
SCCA	Stationary Control Component Assembly
SCDS	Signal Conditioning and Distribution System

07.01-26

7.0 Instrumentation and Controls

07.01-26

7.1 Introduction

Chapter 7 describes the instrumentation and controls (I&C) systems for the U.S. EPR systems. The description of the I&C systems includes system classifications, functional requirements and assignment, and system architecture. The information provided emphasizes those instruments and associated equipment that constitutes the safety systems as defined in IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std 603-1998) (Reference 1), which meets or exceeds the requirements of IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations (IEEE Std 603-1991) (Reference 2).

The I&C systems provide proper control of plant processes to protect against unsafe and improper reactor operations during steady-state and transient power operations. The I&C systems also provide initiating signals to mitigate the consequences of accident conditions.

This section describes the U.S. EPR I&C systems that comprise the U.S. EPR I&C architecture and the design features associated with these systems.

Figure 7.1-1—Chapter 7 Symbol Legend is provided to illustrate the symbols used in the figures provided in this chapter.

Definitions

The terminology used in this chapter reflects those used in IEEE Std 603-1998 (Reference 1):

Actuated Equipment – the assembly of prime movers and driven equipment used to accomplish a protective function, such as solenoids, shutdown rods, and valves.

Actuation Device – a component or assembly of components that directly controls the motive power for actuated equipment.

Anticipated Operational Occurrence (AOO) - Anticipated operational occurrences mean those conditions of normal operation which are expected to occur one or more times during the life of the nuclear power unit and include but are not limited to loss of power to the recirculation pumps, tripping of the turbine generator (TG) set, isolation of the main condenser, and loss of offsite power.

Application Software – software that is developed using a set of engineering tools associated with a generic I&C platform and is specific to a particular set of functional requirements.

07.01-26

Beyond Design Basis Event (BDBE) – postulated event that is excluded from the deterministic design basis based on the low probability of occurrence. BDBEs are considered in the design of the plant based on specific regulatory requirements or guidance, or based on results from the probabilistic risk assessment.

Communication Module – A device that is used to transmit digital information from one device to another over one or several data communication links using a predetermined protocol.

Control Unit (CU) - a functional unit in an Instrumentation and Control system that contains a function processor. A Control Unit is a generic functional term and is neither system nor technology specific. Generally, a CU consists of microprocessors, firmware, hardware, and software necessary to implement its functions. However, specific details of each system design are unique to the technology chosen to implement its functions.

Channel – an arrangement of components and modules as required to generate a single protective action signal when required by a generating station condition. A channel loses its identity where single protective action signals are combined.

Class 1E – the safety classification of the electrical equipment and systems that are essential to emergency reactor shutdown, containment isolation, reactor core cooling, and containment and reactor heat removal, or are otherwise essential in preventing significant release of radioactive material to the environment.

Component Level – actuation or control of a single actuation device (component).

Credited – designation for a system that can perform a safety function, and is qualified and relied upon to do so.

Data Communication – a method of sharing information between devices that involves a set of rules, formats, encodings, specifications, and conventions for transmitting data over a communication path, known as a protocol.

Division – the designation applied to a given system or set of components that enables the establishment and maintenance of physical, electrical, and functional independence from other redundant sets of components.

07.01-26

Design Basis Event (DBE) – postulated events used in the design to establish the acceptable requirements for the structures, systems, and components.

Function Processor – a device that contains hardware, system software, and application software that executes instrumentation and control functions.

Functional Unit – a set of assembled components within a system that perform specific functions to support overall system operation.

I&C Platform – a generic set of system hardware, system software, and engineering tools that can be configuration for a wide variety of instrumentation and control functions.

Hardwired I&C – operator controls and indicators that are connected with other I&C equipment using an analog signal path. This includes devices such as buttons, switches, analog indicators, or standalone digital indicators.

Hardwired Signal – an analog or discrete digital signal that does not use a data communications protocol.

Input/Output (I/O) Module – a module that converts signals from a hardwired to digital form (or vice versa).

Non-Credited – designation for a system that can perform a safety function, but is not qualified or relied upon to do so.

07.01-26

Optical link module – a device that converts an electrical signal to an optical signal.

Postulated accident (PA) - unanticipated occurrences that are postulated to occur but are not expected to occur during the life of the nuclear plant unit.

Protective action – the initiation of a signal within the sense and command features or the operation of equipment within the execute features for the purpose of accomplishing a safety function.

Protection system – That part of the sense and command features involved in generating those signals used primarily for the reactor trip system and engineered safety features.

Safety function – one of the processes or conditions (e.g., emergency negative reactivity insertion, post-accident heat removal, emergency core cooling, post-accident radioactivity removal, and containment isolation) essential to maintain plant parameters within acceptable limits established for a DBE.

Safety system – a system that is relied upon to remain functional during and following design events to maintain: (A) the integrity of the reactor coolant pressure boundary (RCPB), (B) the capability to shut down the reactor and maintain it in a safe shutdown condition, or (C) the capability to prevent or mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR 100 guidelines.

Sensor – the portion of a channel that responds to changes in a plant variable or condition and converts the measured process variable into an electrical, optical or pneumatic signal.

System level – actuation or control of a sufficient number of components to achieve a desired function.

System Hardware – hardware associated with a generic I&C platform, including function processors, I/O modules, communication modules, subracks and other hardware devices associated with a generic I&C platform.

System software – The layers of software that are not configured uniquely for a specific I&C application. System software has a different functional purpose compared to “application software” (defined above) and is the same on all TXS processors. In contrast, application software is configured to reflect a nuclear power plant’s specific safety system functional requirements, different application software functions reside on individual TXS processors within the overall TXS system. For TELEPERM XS, system software is defined as the operating system and platform software layers shown in Figure 3.5 of Reference 3.

07.01-26

7.1.1 U.S. EPR I&C ~~Architecture~~Systems

7.1.1.1 Overview

The U.S. EPR implements a modern digital I&C design based on experience gained internationally from new plant designs and retrofits to existing plants using digital I&C equipment. The U.S. EPR I&C ~~architecture~~systems implement~~s~~ these design features to optimize overall plant safety:

- Use of digital technology:

  The I&C design maximizes the use of digital I&C platforms. Many features of digital I&C provide overall improvements in plant safety. These features include continuous online self-testing and diagnostics that allow early detection of failures and improved human-machine interfaces (HMI) using video display units that provide an integrated view of process systems status to the operators.

- Robust I&C architecture design:

  The I&C architecture implements several design principles such as defense-in-depth, diversity, redundancy, independence and priority to optimize plant safety. These principles are applied so that the impact of failures is minimized and the required safety functions are executed when required.

- Automation of plant operation:

A high degree of automation is implemented to improve plant operation, reduce operator burden, and improve situational awareness during normal and accident conditions. For DBEs, safety functions required during the first 30 minutes are automated.

- State of the art design for human factors:

07.01-26

The I&C systems design is integrated with the human factors engineering (HFE) principles addressed in Chapter 18 for improved human reliability and overall plant safety.

The primary I&C systems used for control and monitoring in the plant are collectively referred to as the distributed control system (DCS). The DCS performs the majority of signal input processing, automation, operator interface, annunciation of abnormal process conditions, and actuator output functions in the plant. Section 7.1.1.3 and Section 7.1.1.4 describe the DCS and its constituent subsystems. Section 7.1.1.6 describes the design principles of the DCS . Figure 7.1-2—Distributed Control System Functional Architecture and Figure 7.1-22—Distributed Control System Physical Architecture show the U.S. EPR DCS design.

The DCS implements functional requirements specified by the various plant mechanical and electrical systems, provided in the following list. The allocation of these functional requirements within the DCS is shown in Table 7.1-3—DCS Functional Requirements Allocation Matrix:

- The process control functions are described in Section 7.7.
- The process limitation functions are described in Section 7.7.
- The reactor trip functions are described in Section 7.2.
- The engineered safety feature (ESF) actuation functions are described in Section 7.3.
- The safety control functions are described in the following sections:
  - The control of safety systems in continuous operation is described in Chapter 8 and Chapter 9.
  - The control of safety systems following ESF actuation is described in Section 7.3.
  - The control of safety systems to reach and maintain safe shutdown is described in Section 7.4.
- The safety interlock functions are described in Section 7.6.
- The severe accident control functions are described in Chapter 19.

07.01-26

- The diverse reactor trip functions are described in Section 7.8.
- The diverse ESF actuation functions are described in Section 7.8.
- The process indications are described in Chapters 5, 6, 8, 9, 10, and 11.
- The post-accident monitoring (PAM) indications are described in Section 7.5.
- The severe accident indications are described in Chapter 19.
- The alarms are described in Section 7.5.

Other I&C systems in the plant include dedicated systems for specific functions, such as acquisition and processing of neutron flux measurements. Section 7.1.1.5 describes these systems.

I&C equipment is also contained in mechanical and electrical systems. This equipment includes instrumentation and black boxes for packaged equipment, such as emergency diesel generators (EDGs). I&C equipment contained in mechanical and electrical systems are described in Chapters 5, 6, 8, 9, 10, and 11.

~~The U.S. EPR I&C architecture is represented in Figure 7.1-2—U.S. EPR I&C ArchitectureDistributed Control System Functional Architecture. The overall I&C architecture is categorized into four levels:~~

- ~~Level 3: business management systems—These consist of plant information management systems. Other than interfaces provided from Level 2, these systems are not within the scope of this document and are not shown on Figure 7.1-2.~~
- ~~Level 2: unit supervision and control—These I&C systems are provided as an interface between the operator and the automation systems. Typical functions include monitoring plant processes and manual control of plant components.~~
- ~~Level 1: system automation—These I&C systems acquire and process sensor information to perform automatic system control functions and transmit information for display to the operator. These systems also process manual commands to operate plant equipment.~~
- ~~Level 0: process interface—These I&C systems act as the coupling between the physical process and the I&C systems. They include sensing components, actuation devices, and actuated equipment such as pressure sensors, thermocouples, switchgear, pumps and valves.~~

7.1.1.2 Use of TELEPERM XS and Qualified Display System in the U.S. EPR

TELEPERM XS (TXS) is a digital I&C platform that has been specifically designed and qualified for use in nuclear safety-related applications.

07.01-26

The qualified display system (QDS) is a digital human machine interface (HMI) that is qualified for use in safety-related applications through a commercial grade dedication process.

7.1.1.2.1 TXS Platform Design

The TXS platform is described in the Reactor Protection System Topical Report (EMF-2110(NP)(A) (Reference 3). Because of advances in technology and rapid obsolescence of components, the various modules described in EMF-2110(NP)(A) (Reference 3) will be modified and upgraded over time, and new modules will be developed. The design and qualification of new or upgraded TXS hardware and system software used in U.S. EPR plants will be performed consistent with the methods described in Reference 3.

The aspects of the TXS platform discussed in EMF-2110(NP)(A) can be classified in three broad categories:

1. Hardware design and qualification.
2. System software design and qualification.
3. Various configurations and arrangements of hardware and software to form a project-specific system architecture.

Modified, upgraded or new TXS hardware modules and system software modules will be used in the U.S. EPR without further NRC review provided they conform to the key TXS principles, features, and methods described in EMF-2110(NP)(A) and identified in ANP-10272. The U.S. EPR FSAR Tier 1, Chapter 2 sections for the PS, and SAS contain commitments that those systems' "hardware modules and system software modules conform to the key TELEPERM XS principles, features and quality methods." The criteria and evaluation process specified in TELEPERM XS Software Program Manual (ANP-10272) (Reference 8) Sections 4.1.1 through 4.1.4 is used to satisfy these Tier 1 commitments by determining that modified, upgraded or new hardware modules and system software modules conform to the key TXS principles, features, and methods.

7.1.1.2.2 QDS Platform Design

The QDS was not included in the scope of EMF-2110NP(A), but is designed to interface with the standard TXS hardware and system software. The QDS hardware and system software are different from the standard TXS platform because the QDS performs video display functionality as opposed to system automation functionality.

07.01-26

The QDS is qualified for use in safety-related applications through a commercial grade dedication process that conforms to the guidance of EPRI TR-106439, "Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications" (Reference 40).

07.01-26

~~The U.S. EPR-specific I&C system architectures that will be implemented using the TXS and QDS platforms are described in Section 7.1 for NRC review against the current regulations and guidance. The U.S EPR-specific system architectures supersede the example system architectures that were included in EMF-2110(NP)(A) to provide context for the review of the generic TXS platform.~~

7.1.1.2.3 Application of the TXS and QDS Platforms

TELEPERM XS Software Topical Report (ANP-10272) (Reference 5) describes the lifecycle processes for application software development used in safety-related applications of the TXS and QDS platforms for the U.S. EPR, as well as software V&V processes. These phases are listed below along with the primary activities included in each phase:

- Basic design:
  - System requirements.
  - System design.
  - Software requirements.
  - Initiate software requirements traceability.
  - Summary reports for V&V activities (i.e., acquisition support, planning, concept, and requirements).
- Detailed design:
  - Software design.
  - Automatic code generation.
  - Application software integration validation test planning (using an NRC-approved simulation test tool).
  - Application software integration validation test execution (using an NRC-approved simulation test tool).
  - Application software integration validation test reporting (using an NRC-approved simulation test tool).
  - Software safety analyses.
  - Continue software requirements traceability.
  - Hardware design.
  - Summary reports for V&V activities (i.e., design and implementation.

- Manufacturing:
  - Hardware manufacturing.
  - Approval of supplier manufactured, tested hardware, and required supplier hardware documentation.
  - Cabinet design.
  - Cabinet internal wiring design.
- System integration and testing:
  - Integration of hardware and software.
  - Software integration, system and acceptance validation test planning.
  - Software integration, system and acceptance validation test execution.
  - Software integration, system and acceptance validation test reporting.
  - Continue software requirements traceability.
  - Summary reports for V&V activities.
- Installation and commissioning:
  - Installation and commissioning test planning.
  - Installation and commissioning test execution.
  - Installation and commissioning test reporting.
  - Summary reports for V&V activities.
- Final Documentation:
  - Generation of final documentation before system is placed in service.

The primary documentation generated as outputs of each of these phases is described in ANP-10272 (Reference 5), Section 4.5. While the development of the QDS application software is performed in accordance with the lifecycle and configuration controls defined in ANP-10272 for the standard TXS platform, there is one difference: the development tools to create the application software (i.e., SPACE) described in ANP-10272 are not used to create QDS application software. The QDS-specific tools are qualified as part of the commercial grade dedication process described in Section 7.1.1.2.2. Once qualified, these tools will be controlled under configuration management as required by IEEE 7-4.3.2-2003, Section 5.3.2.

07.01-26

The U.S. EPR I&C systems supported by the TXS and QDS platforms are described in Sections 7.1.1.3.1, 7.1.1.4.1, 7.1.1.4.2, and 7.1.1.4.5 for review against NRC regulations and guidance. The U.S. EPR-specific system architectures supersede the example system architectures that were included in EMF-21 10(NP)(A) to provide context for the review of the generic TXS platform.

7.1.1.2.4 Reliability of Communications with the TXS and QDS Platforms in the U.S EPR

The safety-related I&C systems use proprietary, time-triggered operating systems that do not rely on hardware and interrupt only on cyclic processing of the software. Because there are no process-driven interrupts, every operation is cyclic and predictive, which verifies that the output of messages on networks link prevents collision.

The hardware components only read the incoming memory buffer or generate a packet to send only when the operating system generates the order. The cyclic operations of the processing units verify that the operator does not simultaneously perform a reading and writing operation.

The communication process sends information written in memory and writes in memory received information. Packet numbering verifies that information is only processed once and that the information is processed without relying on synchronizing both tasks.

Each safety-related Ethernet connection using the TXS protocol for safety-related applications is point-to-point in the U.S. EPR design. Packets are only sent to dedicated receivers by the expected senders. The protocol is at the hardware level and uses the physical addresses of the network components (MAC addresses) to check the consistency between the sender and receiver. Those addresses are set in the applications and will only be changed if the hardware changes.

Using point-to-point connection, without interference on the links, verifies that the response time between sending a message and its reception is predictable and will only change if the link is physically altered. In this case, a regular response time with the Ethernet network exists.

7.1.1.3 ~~Level 2 - Unit Supervision and Control~~DCS HMI Systems

7.1.1.3.1 Safety Information and Control System

The safety information and control system (SICS) is provided as a safety-related HMI. The process information and control system (PICS) is normally used by the operator to monitor and control ~~process~~plant systems, and the SICS is used in the unlikely event

07.01-26

that the PICS is not available. The SICS provides control capabilities in both the main control room (MCR) and remote shutdown station (RSS).

This section describes the SICS with regards to I&C design. Details such as screen displays, levels of automation, and panel layout are designed using the HFE principles described in Chapter 18.

Classification

The SICS is classified as safety-related.

Functions

Table 7.1-3 shows Tthe functions of the SICS are specified for the MCR or the RSS.

Interfaces

Table 7.1-4—DCS Interface Matrix shows the interfaces of the SICS.

The SICS performs these safety-related functions:

- Manual actuation of reactor trip (MCR and RSS).
- Manual actuation and control of engineered safety features (ESF) systems for accident mitigation (MCR).
- Manual control of systems to achieve and maintain safe shutdown (MCR).
- Display of Type A through Type C post-accident monitoring (PAM) variables (MCR).

The SICS performs these non-safety-related functions:

- Monitoring and control of essential non-safety-related systems to achieve and maintain hot standby on a loss of PICS (MCR).
- Monitoring and control of systems to mitigate severe accidents (MCR).
- Backup safety parameter display system (SPDS) functions (MCR).
- Display high priority alarms (MCR).

Architecture

Figure 7.1-2 shows the basic architecture of the SICS.

Figure 7.1-3—Safety Information and Control System Architecture (QDS Portion) shows the QDS architecture.

07.01-26

The SICS provides control capabilities in the main control room (MCR) and limited control capabilities in the remote shutdown station (RSS). At each control location, the inventory of controls and indications is laid out in accordance with relevant electrical separation criteria and the HFE principles described in Chapter 18.

The controls and indications required to be on the SICS are implemented with dedicated, hardwired I&C. In addition, a subset of plant parameters are duplicated on the QDS for situational awareness. Chapter 18 describes the subset of parameters chosen are selected in accordance with the HFE principles.

Each QDS receives input from the four divisions of the protection system (PS). The four QDS shown are a nominal number. The final number and placement of the QDS is determined in accordance with the HFE principles described in Chapter 18.

~~The SICS consists of a safety-related portion and a non-safety-related portion to perform its functions.~~

~~*Safety-Related Portion of SICS*~~

~~Figure 7.1-3—Safety Information and Control System Architecture (Safety-Related PortionQDS Portion) provides a functional representation of the safety-related portion of the SICS.~~

~~The safety-related portion of the SICS is organized into four independent divisions. The four divisions of safety-related panel interfaces are located in separate Safeguards Buildings. The four divisions of the safety-related QDS and other safety-related HMI equipment are located in the MCR and RSS, and are physically separated by safety-related structures, separation distance, barriers, or any combination thereof.~~

~~The safety-related portion of the SICS consists of these functional units:~~

- ~~Panel interfaces (PI)~~
- ~~Qualified display systems (QDS).~~

~~PIs perform data processing functions and are provided to interface between the various Level 1 systems and the HMI devices in the MCR or RSS. Control PIs process manual commands initiated from the HMI devices and information related to actuator status for display. Monitoring PIs only transfer information to the HMI devices for display to the operator. Hardwired connections to non-safety-related I&C systems may be used as required by the SICS human factors design and are isolated as described in Section 7.1.1.6.4.~~

~~Control QDSs provide the capability to initiate manual commands and display actuator-related information. Monitoring QDSs only provide information to the~~

07.01-26

operator. The number and physical arrangement of QDSs provided in the MCR and RSS are determined based on functional and human factors requirements.

Hardwired I&C is used to provide information to the operator and provide the ability to actuate and control plant equipment. Hardwired I&C is connected to the PIs, various Level 1 I&C systems, and the reactor trip devices.

Section 7.2 and Section 7.3 describe the methods used for manual actuation of reactor trip and engineered safety features. For other manual controls, the human factors principles described in Chapter 18 shall be used to select the type of HMI used.

Non-Safety-Related Portion of SICS

Figure 7.1-4—Safety Information and Control System Architecture (Non-Safety-Related PortionDeleted) provides a functional representation of the non-safety-related portion of the SICS.

These functional units are implemented in the non-safety-related portion of the SICS:

- Gateways (GW).
- Qualified display systems.
- Service units.

GWs are provided to interface to the plant data network.

QDSs provided in divisions 2 and 3 to monitor and control other non-safety-related I&C systems via GWs on a loss of PICS.

QDSs are provided in divisions 1 and 4 to monitor and control equipment dedicated to mitigate severe accidents. These QDS utilize point-to-point data connections to transmit and receive information to the severe accident I&C (SA I&C).

Hardwired I&C is also provided to monitor and control non-safety-related I&C systems. The human factors principles described in Chapter 18 are used to select the type of HMI used.

SUs are provided for configuration and maintenance of the SICS. The PIs are serviced by the SUs of the safety automation system (SAS) via the monitoring and service interface (MSI) of the SAS. The QDSs have dedicated non-safety-related SUs that are only connected to the QDS only when the QDS is out of service. They are normally isolated through a key lock switch. The number and location of SUs is determined based on the number and layout of QDSs.

Equipment

07.01-26

The SICS is implemented with hardwired I&C equipment andthe TXS digital I&C platform, the QDS platform, and hardwired I&C equipment. The SICS includes both safety-related and non-safety-related equipment as shown in Figure 7.1-2.

The hardwired I&C consists of conventional HMI devices such as buttons, switches, and digital indicators that are hardwired from the various I&C systems. The PIs utilize the TXS platform and generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. The QDS consists of a computer, video display with touch screen capabilities, and input devices such as a keyboard and trackball. The QDS is capable of trending of information to provide situational awareness by the operator. The hardwired I&C consists of conventional HMI devices such as buttons, switches, and analog and digital indicators that are hardwired from the various I&C systems. Fiber optic and copper cable are used for the various data and hardwired connections.

Qualification Requirements

The safety-related equipment used in the safety-related portion of the SICS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

Quality for the QDS platform is described in Section 7.1.1.2.2.

The application software used in the safety-related portion of the SICS is developed using the lifecycle processes described in Section 7.1.1.2.3.

Diversity Requirements

There are no specific diversity requirements for the SICS because the equipment is specified to be hardwired I&C. The QDS is not used in the demonstration of satisfying defense-in-depth and diversity requirements. The use of SICS is credited in the demonstration of defense-in-depth and diversity analysis is described in Section 7.8. Diversity requirements for the SICS are identified in Reference 8. The manual reactor trip actuation is implemented from the SICS using a hardwired path that is not affected by a software common cause failure (CCF) of the SICS or PS.

Data Communications

Data communications implemented in the safety-related portion of the SICS include:

07.01-26

- PS-SICS (Control) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Control) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- PS-SICS (MonitoringQDS) – uni-directional (PS to SICS), point-to-point data connections implemented with the TXS ProfibusEthernet protocol.
- SAS-SICS (Monitoring) – uni-directional (SAS to SICS), point-to-point data connections implemented with the TXS Profibus protocol.
- PI-QDS (Control) – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- PI-QDS (Monitoring) – uni-directional (PI to QDS), point-to-point data connections implemented with the TXS Ethernet protocol.
- PI-PI (Monitoring) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. This network is provided to allow the display of redundant divisional information on a single QDS for optimization of the human factors design. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4.

Data communications implemented in the non-safety-related portion of the SICS are:

- SU-QDS – bi-directional, networked data connections implemented with the TXS Ethernet protocol. The SU is an auxiliary feature, and this network is a non-safety-related network provided for servicing of the QDSs. These data connections use dedicated ports on the QDS separate from the PI-QDS connections. The SU-QDS link is normally broken by a switch that isolates the two computers. The switch is key lock, and the key is controlled administratively. Software modifications cannot be performed with the QDS in operation. Fiber optic cable is provided for electrical isolation.
- SA I&C-SICS – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- GW-QDS – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data Network – bi-directional, networked communications.

Power Supply

The safety-related portion of the SICS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the emergency diesel generators (EDGs) in the case of a loss of offsite power (LOOP). In the event of a station blackout (SBO), the EUPS has the capability of receiving power from the station blackout diesel generators (SBODGs).

07.01-26

The non-safety-related portion of the SICS is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.3.2 Process Information and Control System

The PICS is a modern, digital HMI. It allows the monitoring and control of process systems for the execution of required plant operations, including those required for abnormal and emergency situations. The PICS is provided in both the MCR and the RSS. ViewMonitoring-only capabilities are provided in other areas of the plant as needed, including the technical support center (TSC) for support of emergency response operations.

This section describes the PICS with regards to I&C design. Details such as screen displays, levels of automation, and panel layout are designed using the HFE principles described in Chapter 18.

Classification

The PICS is classified as non-safety-related, augmented quality.

Functions

Table 7.1-3 shows the functions of the PICS.

Interfaces

Table 7.1-4 shows the interfaces of the PICS.

The PICS performs these functions:

- Monitoring and control of process systems during normal operation, including startup, power, and shutdown operation.
- Monitor the status of the automatic reactor trip and ESF systems during abnormal events, including anticipated operational occurrences (AOO), postulated accidents, and special events.
- Manual reset of automatic reactor trip and ESF actuation functions.
- Non-credited means to monitor and control systems required to achieve and maintain safe shutdown.
- Manual component level control of safety-related process systems via the process automation system (PAS) and priority and actuator control system (PACS).

07.01-26

- Manual actuation of critical safety functions via the DAS or PAS.
- Primary SPDS functions.
- Display of Type A-E PAM variables.
- Monitoring and control of systems required to mitigate severe accidents.
- Display bypassed and inoperable status of safety systems.
- Alarm management.
- Data archival.
- Interface to external I&C computers.
- Interface to external computers via a unidirectional firewall.

Architecture

Figure 7.1-2 shows the basic architecture of the PICS.Figure 7.1-5—Process Information and Control System ArchitectureDeleted provides a functional representation of the PICS.

The PICS consists of primarily of gateways, serversprocessing units (PU), external units (XU), operator workstations, plant overview panels (POP), and a firewalls.

Redundant gateways are provided for communication with the PS, safety automation system (SAS), reactor control, surveillance and limitation (RCSL), and TG I&C. The PICS receives unidirectional signals from the PS and SAS to receive status information on those systems. The PICS communicates bi-directionally with the RCSL and TG I&C for control of reactivity control systems and the TG, respectively.

PUsServers are provided for data exchange between the plant data networkautomation bus and the terminal data networkHMI bus. The PUsservers perform functions such as data message validation, short term data storage, and alarm management. Redundant PUsservers are provided so that the PICS remains operational in case of a failure of a single PUserver. Multiple sets of redundant servers may be used to subdivide functionality (e.g., control and indication, alarm, historian, etc).

PICS workstations with control and monitoring capabilities are located in the MCR and RSS. Normally, the operator displays in the RSS are in supervisory mode (view only) to prevent plant control until authorized in accordance with plant procedures. Operator displays are provided in the TSC with monitoring only capabilities to assist in plant emergency response.other locations in the plant (e.g., TSC) as necessary. PICS workstations may be used for local control of specific plant systems with appropriate administrative controls.

The number of terminals per workstation, and number and location of the operator workstations is determined as a result of the human factors design process described in Chapter 18.

Plant overview panels are provided in the MCR, and other locations such as the TSC as desired. These are wide screen displays that are capable of providing continuously visible information to the operator.

07.01-26

XUs provide an interface to other computers from the PICS. Specialized monitoring systems may utilize dedicated computers that require an interface to the PICS for operator monitoring and management. ARedundant firewalls isare provided for unidirectional transfer of information from the XUsPICS to plant business networks.Level 3 I&C systems. Remote access to the PICS is not possible.prohibited. Refer to Section 7.1.1.6.6 for more information on cybersecurity.

The PICS may include other functional units as necessary to carry out its functions. Examples are:

- Long term data storage units.
- Networked printers.
- Service equipment.

Equipment

The PICS is implemented with an industrial digital I&C and HMI platform.

The PUsservers consist of industrial computers. Operator workstations typically consist of computers, displays, and input devices (i.e., computer mice and keyboards). The operator may use several monitors that share input devices. These monitors display different plant functions, and the display content is interchangeable. The POP is a set of large panels that display an overview of plant and system status. Equipment such as network switches and electrical and fiber optic cable are provided to support data communications. The PICS equipment is capable of trending of information to provide situational awareness by the operator. In addition, the PICS has recording capability so that historical data can be recalled by the operator.

The plant annunciator is integrated into the PICS operating and monitoring system. Special screens display and organize alarms and warnings based on their status and relative level of importance. An alarm hierarchy with a color coding system is used to immediately alert the operator of the importance of the alarm based on the relevance to plant safety.

The PICS is used to control both safety-related (via the process automation system (PAS) and the priority and actuator control system (PACS)) and non-safety-related process systems. The PICS implements these measures to preclude spurious actuation of plant equipment:

- Operation of plant equipment is performed using a two-step process. A single mouse click on a component is followed by a verification step requiring a second single mouse click, so a single inadvertent action by the operator does not result in a command signal.
- Touch screen displays are not used.

07.01-26

Qualification Requirements

~~In the unlikely event of a software common cause failure of the PS, the PICS equipment must function properly under conditions during and following design basis events.~~ The PICS is intended to be used during normal, accident, and severe accident conditions as long as it is available. The PICS equipment is located in Safeguard Buildings that provide a mild environment during and following anticipated operational occurrences (AOOs) or postulated accidents (PAs)~~design basis events~~. Equipment selected for use in the PICS will be rated by the manufacturer (or otherwise reasonably expected) to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used.

Quality Requirements

In its role as the primary operator interface~~, and as a system relied on to mitigate the effects of CCF of the PS~~, the PICS is required to be of sufficient quality to perform its functions in a reliable manner. The PICS is designed using a robust engineering process with appropriate reviews, verifications, tests, and approvals. Sufficient quality is achieved in the design of the PICS through the following measures:

- The PICS is designed, fabricated, erected, and tested under the quality assurance program described in Topical Report ANP-1066A, Addendum A (Reference 42). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 43).
- The design of the PICS is accomplished through a phased approach, including the following (or equivalent) phases:
  - System requirements phase.
  - System design phase.
  - Software/hardware requirements phase.
  - Software/hardware design phase.
  - Software/hardware implementation phase.

- Software/hardware validation phase.
- System integration phase.
- System validation phase.

- A criticality analysis is performed for the PICS software in accordance with accepted industrial practice.
- Verification and validation (V&V) of the PICS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- PICS requirements are documented in a traceable form that is under configuration management.
- The PICS design is validated through acceptance test in the system validation (or equivalent) phase.

07.01-26

Diversity Requirements

There are no equipment diversity requirements for the PICS.

The PICS is credited by the defense-in-depth and diversity analysis described in Section 7.8. Diversity requirements for the PICS are identified in Reference 8:

- The PICS displays are diverse from the SICS displays (QDS).

Data Communications

The PUsservers transmit data to and receive data fromcommunicate with the automationLevel 1 I&C systems via automation bus and gateways for the PS, SAS, RCSL, and TG I&C.the plant data network. The PUsservers, operator workstations, POP, and XUsfirewalls exchange data via the HMI busterminal data network. These networks implement periodic communications and message validation for robust data communications. Remote access of the PICS is not possible.

The redundant servers and redundant segments of the automation busses are physically located in a separate fire areas so that a fire in the MCR does not result in a loss of the PICS at the RSS. The HMI bus hardware is located so that damage from a fire event in the MCR will be limited to network components required for the operation of MCR workstations and have no impact on the overall functionality of the HMI bus. Portions of the HMI bus required for operation from the RSS are located in a separate fire area from the MCR, so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not impact the ability to safely shutdown the plant from the PICS workstations in the RSS.

Sound engineering and design practices will be applied to the development of the PICS automation bus, HMI bus, and the DCS systems connected to the bus. The PICS

07.01-26

automation and HMI busses will be designed to withstand data traffic, and the interfacing DCS systems will be designed with thresholds for network traffic that are consistent with maximum data rates of the busses. Specific design details regarding preclusion of data storm events on a non-safety-related network depends on the specific technology chosen for these non-safety-related networks, and they are not included in the U.S. EPR FSAR.

The PICS will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Power Supply

The PICS is powered from the ~~12-hour uninterruptible power supply (~~12~~hr~~ UPS~~)~~. The 12~~hr~~ UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

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

7.1.1.4 ~~Level 1 - System Automation~~DCS Automation Systems

7.1.1.4.1 Protection System

The PS is an integrated digital reactor protection system (RPS) and ESF actuation system. The PS detects plant conditions that indicate the occurrence of AOOs and ~~postulated accident~~PAs, and it actuates the safety-related process systems required to mitigate the event.

Classification

The PS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the PS.

Interfaces

Table 7.1-4 shows the interfaces of the PS.

~~The PS performs these functions:~~

- ~~Actuation of reactor trip.~~
- ~~Actuation of ESF systems.~~
- ~~Processing Type A-C PAM variables for display on the SICS.~~
- ~~Interlocks.~~

Architecture

07.01-26

Figure 7.1-6—Protection System Architecture provides a functional representation of the PS.

The PS is organized into four redundant, independent divisions located in separate Safeguards Buildings. Each division contains two functionally independent subsystems (A and B). These subsystems are used to implement functional diversity for reactor trip functions.

The PS consists of these functional units:

- ~~Remote Acquisition Units (RAU).~~
- ~~Rod Control Cluster Assembly Units (RCCAU).~~
- Acquisition and Processing Units (APU).
- Actuation Logic Units (ALU).
- Monitoring Service Interfaces (MSIs).
- Gateways (GWs).
- Service Units (SUs.)

Details on these functional units, along with details of the PS architecture, are described in Digital Protection System Technical Report (ANP-10309P) (Reference 6).

Equipment

The PS is implemented with the TXS digital I&C platform.

The ~~RAUs, RCCAUs,~~ APUs, ALUs, and MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable are used for the various data and hardwired connections.

The data communication modules (e.g., communication modules, optical link modules) that are part of the PS are located within the PS cabinets. These cabinets are located in mild environment areas within the four Safeguard Buildings. The cables used to interconnect functional units within the PS are considered part of the PS. Cabling independence and separation are described in Section 8.3.1.1.9.

Qualification Requirements

The equipment used in the PS is qualified for environmental, seismic, electromagnetic interference, and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

The application software used in the PS is developed using the lifecycle processes described in Section 7.1.1.2.3.

Diversity Requirements

There are no equipment diversity requirements for the PS.

Data Communications

The data communications for the PS are described in ANP-10309P (Reference 6).

Power Supply

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

07.01-26

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

7.1.1.4.2 Safety Automation System

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

The SAS only implements safety-related, credited control functions for safety systems. Non-safety-related or non-credited control functions for safety systems are performed by the PAS and PICS.

Classification

The SAS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the SAS.

07.01-26

Interfaces

Table 7.1-4 shows the interfaces of the SAS.

The SAS performs these functions:

- Automatic controls.
- Manual controls.
- Processing Type A-C PAM variables for display on the SICS.
- Interlocks.

Architecture

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

The SAS is organized into four independent divisions located in the following buildings: separate Safeguards Buildings. SAS equipment may also be located in other safety-related structures as necessary.

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

The SAS consists of these functional units:

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

The CUs execute the logic for the assigned automatic and manual grouped control functions. Redundant CUs are provided within each division. Multiple sets of redundant CUs may be used, depending on sizing requirements. Redundant CUs in multiple divisions may have interdivisional communications between them to perform their functions. They CUs acquire hardwired inputs from the signal conditioning and distribution system (SCDS), sensors, the PS, or the SICS via hardwired connections. Manual commands initiated from the SICS (QDS) or PICS are received via the MSI. Outputs from the CUs are sent to the PACS for signal prioritization and drive actuation. Outputs may also be sent to the PAS to coordinate logic for related

07.01-26

actuators within PAS. Data are sent from the CUs to the MSIs for display on SICS, or via the MSIs and redundant GWs for display on the PICS. or PICS.

The MSIs provide a communication path between the SAS and other I&C systems via the GWs for both display of information and transfer of manual commands. The MSIs also provides a path to the service unit (SU) for testing and maintenance of the CUs.

Redundant GWs are provided to interface to the plant data network.

The SU provides the ability to monitor, service, and test the SAS.

Equipment

The SAS is implemented with the TXS digital I&C platform.

The CUs and MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable are used for the various data and hardwired connections.

Qualification Requirements

The equipment used in the SAS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

Quality for the TXS platform is described in Section 7.1.1.2.1.

The application software used in the SAS is developed using the lifecycle processes described in Section 7.1.1.2.3.

Diversity Requirements

There are no equipment diversity requirements for the SAS.

Data Communications

Data communications implemented in the SAS are:

- CU-CU (A or B) – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol. This network is provided to implement signal selection algorithms using redundant sensors for improved reliability in the control of safety-related processes. Separate connections are used for redundant CUs.redundancies A and B. The design features that provide for independence between redundant divisions are described in Section 7.1.1.6.4.

07.01-26

- CU-Monitoring Service Interface (MSI) – bi-directional, point to point data connections implemented with the TXS Profibus protocol.
- SAS-SICS (Control) – refer to Section 7.1.1.3.1.
- SAS-SICS (Monitoring) – refer to Section 7.1.1.3.1.
- MSI-GW – buni-directional, point-to-point data connections implemented with the TXS Ethernet protocol. This network is provided so the SAS can provide status information to the PICSto allow monitoring and control of the SAS from the PICS. The design features that provide for independence between safety-related and non-safety-related systems are described in Section 7.1.1.6.4.
- MSI-SU – non-safety-related, inter-divisional, bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol. This network is provided for the servicing of the SAS. The design features that provide for independence between safety-related and non-safety-related systems are described in Section 7.1.1.6.4.
- GW-PICS - bi-directional, point-to-point data communications. Signals are only engineered to be sent from the SAS to the PICS. Signals coming from the PICS to the SAS GW are to request messages to be sent.GW-Plant Data Network – non-safety-related, divisional, bi-directional, networked communications.

Power Supply

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

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

7.1.1.4.3 Priority and Actuator Control System

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

Classification

The PACS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the PACS.

Interfaces

Table 7.1-4 shows the interfaces of the PACS.

~~The PACS supports the functions of other I&C systems by performing these functions:~~

- ~~Prioritize actuation requests from the various Level 1 and Level 2 I&C systems.~~
- ~~Essential equipment protection.~~
- ~~Drive actuation.~~
- ~~Drive monitoring.~~

Architecture

07.01-26

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

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

- Safeguard Buildings.
- Emergency Power Generating Buildings.
- Essential Service Water Pump Structures.~~The PACS is organized into four independent divisions located in separate Safeguards Buildings. PACS equipment may also be located in other safety-related structures as necessary.~~

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

The PACS is composed of ~~safety-related~~ priority modules~~,~~ and ~~non-safety-related~~ communication modules. One priority module and one communication module are provided for each ~~safety-related~~ actuator.

The PACS receives actuation orders sent by the various ~~I&C~~DCS systems for prioritization. Signals are sent either via hardwired connections or a dedicated data connection to the PAS. Interfaces with actuation devices and actuated equipment (e.g., switchgear, torque and limit switches) are via hardwired connections. Priority between actuation requests from the various ~~I&C~~DCS systems is established by wiring the inputs using the priority principles described in Section 7.1.1.6.5.

Equipment

The PACS is implemented primarily with subracks, priority modules, communication modules, and qualified isolation devices as needed. Fiber optic cable is used for the data connection between the PAS and the PACS.

07.01-26

The PACS equipment may be modified and upgraded as needed, but shall exhibit these characteristics.

- The priority module consists of logic that can not be modified while the module is installed. To modify the priority module logic, the module must be removed prior to any modifications being performedand replaced with another module containing the modified logic.
- The inputs and outputs of the priority module are via hardwired connections.
- The logic of the priority module is subject to 100 percent combinatory proof-of-design testing to eliminate consideration fromand not subject to software common cause failure.
- The communication module is qualified as an associated circuit.
- The data communications from the PAS is only via the communication module.

Qualification Requirements

The equipment used in the PACS is qualified for environmental, seismic, electromagnetic interference and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

The PACS is designed under the TXS quality program described in Section 7.1.1.2.1.

Diversity Requirements

The priority modules are diverse from the digital TXS function processors. In addition, the priority modules must be 100 percent tested to eliminate consideration of software common-cause failure (CCF) as described above. The testing methodology is described in ANP-10310P (Reference 44).

Data Communications

Non-safety-related, bi-directional, data connections are implemented between the communication modules and the PAS.

Power Supply

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

07.01-26

The non-safety-related PACS equipment in the Safeguard Buildings is powered from the 12UPS. The 12UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The non-safety-related PACS equipment in the Emergency Power Generating Buildings and the Essential Service Water Pump structure is powered from a UPS and a diesel backed source.

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

7.1.1.4.4 Deleted.Severe Accident Instrumentation and Control

Classification

The SA I&C is classified as non-safety-related.

Functions

The SA I&C performs monitoring and control functions required for severe accident mitigation.

Architecture

Figure 7.1-9—Severe Accident I&C System Architecture provides a functional representation of the SA I&C.

The SA I&C is organized into four divisions located in separate Safeguards Buildings.

The SA I&C consists of these functional units:

- Control Units (CU).
- Drive Control Modules (DCM).
- MSIs.
- GWs.
- SUs.

The CUs perform data acquisition and control functions. Hardwired inputs are acquired directly from field sensors or from isolated outputs of the safety I&C systems. Hardwired outputs are sent to the DCMs or PACS for component actuation. DCMs are provided to interface to the non-safety-related actuated equipment used for severe accident mitigation.

07.01-26

The MSIs provide a communication path between the SA I&C and other I&C systems via the GWs for both display of information and transfer of manual commands. The MSIs also provides a path to the SU for testing and maintenance of the CUs.

Redundant GWs are provided to interface to the plant data network.

The SU provides the ability to monitor, service, and test the SA I&C.

Equipment

The SA I&C is implemented with the TXS digital I&C platform.

The CUs and MSIs generally consist of subracks, I/O modules, function processors, communication modules, and optical link modules. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

There are no qualification requirements for the SA I&C equipment.

Quality Requirements

There are no quality requirements for the SA I&C equipment.

Diversity Requirements

There are no diversity requirements for the SA I&C equipment.

Data Communications

Data communications implemented in the SA I&C are:

- CU-MSI—bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- MSI-GW—bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- MSI-SU—bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data Network—bi-directional, networked communications.

Power Supply

The SA I&C is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.5 Reactor Control, Surveillance, and Limitation System

Classification

The reactor control, surveillance, and limitation system (RCSL) is classified as non-safety-related.

07.01-26

Functions

Table 7.1-3 shows the functions of the RCSL.

Interfaces

Table 7.1-4 shows the interfaces of the RCSL.

The RCSL performs these functions:

- Automatic reactor limitation functions.
- Automatic and manual reactor operational (control) functions.
- Core monitoring.

Architecture

Figure 7.1-10—Reactor Control, Surveillance, and Limitation System Architecture provides a functional representation of the RCSL.

The RCSL is organized into four divisions located in separate Safeguards Buildings.

The RCSL consists of these functional units:

- Acquisition Units (AU).
- Control Units (CU).
- Drive Units (DU).
- MSIs.
- GWs.
- SUs.

The AUs perform data acquisition functions. Hardwired inputs are acquired directly from the SCDSfield sensors or from isolated outputs of the safety I&C systems.

07.01-26

Redundant CUs acquire information from the AUs. The CUs implement signal selection algorithms for use in the control and limitation functions described in Section 7.7.1. Outputs from the CUs are sent to the DUs for actuation of control rods, or to PAS for commands of other actuators.

Redundant DUs are provided in both divisions 1 and 4. This configuration is chosen so that the control rods remain operable given a failure of a single CU. Hardwired outputs from the DUs are sent to the Control Rod Drive Control System (CRDCS) or to other I&C systems for actuation.

The MSIs provide a communication path between the RCSL and the PICS other I&C systems via theredundant GWs for both display of information and transfer of manual commands. The MSIs also provide a path to the SU for testing and maintenance of the various functional units of the RCSL.

Redundant GWs are provided to interface to the plant data network.

The SU provides the ability to monitor, service, and test the RCSL.

Equipment

The RCSL is implemented with the TXS digital I&C platform.

The AUs, CUs, DUs and MSIs generally consist of subracks, I/O modules, function processors, and communication modules, and optical link modules. SUs and GWs are non-safety-related and consist of industrial grade computers. Fiber optic and copper cable is used for the various data and hardwired connections.

Qualification Requirements

The RCSL equipment is located in Safeguard Buildings that provide a mild environment during and following AOOs or PAs. Equipment used in the RCSL will be rated by the manufacturer (or otherwise reasonably expected) to operate under the mild environmental conditions expected to exist at its location during the events that the equipment is expected to be used.

There are no qualification requirements for the RCSL equipment.

Quality Requirements

For the RCSL equipment, the quality requirements will be consistent with the Quality Assurance Plan for non-safety-related equipment as described in Addendum A of Topical Report ANP-10266.

There are no quality requirements for the RCSL equipment.

Diversity Requirements

There are no diversity requirements for the RCSL equipment.

07.01-26

Data Communications

Data communications implemented in the RCSL are:

- AU-CU – bi-directional, point-to-pointnetworked data connections implemented with the TXS Profibus protocol.
- CU-DU – bi-directional, point-to-pointnetworked data connections implemented with the TXS Profibus protocol.
- AU-MSI - bi-directional, point-to-pointnetworked data connections implemented with the TXS Profibus protocol.
- CU-MSI - bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- DU-MSI - bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.
- MSI-GW – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- MSI-SU – bi-directional, point-to-point data connections implemented with the TXS Ethernet protocol.
- GW-Plant Data NetworkPICS – bi-directional, networkedpoint-to-point data communications.

The RCSL will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Power Supply

The RCSL is powered from the 12-hour uninterruptible power supply (12hr UPS). The 12hr UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.6 Process Automation System

The PAS is the main automation and control system for the plant. The PAS provides controls for both safety-related and non-safety-related equipment.

07.01-26

~~The PAS implements only non-safety-related or non-credited control functions for safety-related systems. The SAS is provided to perform safety-related, credited control functions for safety-related process systems.~~

Classification

The PAS is classified as non-safety-related.

Functions

Table 7.1-3 shows the functions of the PAS.

Interfaces

Table 7.1-4 shows the interfaces of the PAS.

~~The PAS performs the following functions:~~

- ~~Automatic primary plant limitation functions.~~
- ~~Automatic operational functions, including;~~
  - ~~Equipment protection.~~
  - ~~Closed loop controls.~~
- ~~Manual control functions.~~
- ~~Processing of information for display, including;~~
  - ~~Type A-E PAM variables.~~
  - ~~Process system instrumentation.~~
  - ~~Alarms.~~

Architecture

Figure 7.1-11—Process Automation System Architecture (Nuclear Island) provides a functional representation of the PAS in the Nuclear Island (NI). Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant) provides a functional representation of the PAS in the Turbine Island and Balance of Plant.

The PAS is comprised of four divisions located in the NI, in the following buildings:

- Safeguard Buildings.
- Emergency Power Generating Buildings.

07.01-26

- Essential Service Water Pump Structures.
- Nuclear Auxiliary Building (Division 4 only).
- Radioactive Waste Building (Division 4 only).

In addition, the PAS includes two trains that are located in the Turbine Island and Balance of Plant in the following buildings:

- Switchgear Building.
- Circulating Water Cooling Tower Structure.

~~The PAS is segregated into subsystems to account for differences in geographic location within the plant, and design and quality requirements. The PAS contains the following subsystems:~~

- ~~Nuclear island subsystem (NIS).~~
- ~~Turbine island subsystem (TIS).~~
- ~~Balance of plant subsystem (BPS).~~

~~For these descriptions, a statement regarding the PAS includes all three subsystems. Statements applicable to a particular subsystem refer specifically to that subsystem.~~

~~*Nuclear Island Subsystem*~~

~~Figure 7.1-11—Process Automation System Architecture (Nuclear Island Subsystem) provides a functional representation of the NIS.~~

~~The NIS is organized into four divisions located in separate Safeguards Buildings. NIS equipment may also be located in other structures in the Nuclear Island as necessary.~~

The ~~NIS~~PAS implements redundant CUs to perform its functions. The CUs acquire hardwired signals ~~directly~~ from the SCDS, diverse actuation system (DAS), PS, SAS, field sensors, or black boxes~~from other I&C systems~~. Outputs are sent to non-safety-related actuators directly or to the PACS ~~for the actuation of safety-related actuators~~. Interfaces are also provided to the TG I&C for TG operation. The CUs interface with the PICS ~~via the plant data network~~ for manual commands and display of information. CUs in the NI may utilize networked data communications between divisions to accomplish functions that require information from different divisions.

~~*Turbine Island Subsystem*~~

~~Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant Subsystem) provides a functional representation of the TIS.~~

07.01-26

The TIS is located in the Switchgear Building.

The TIS implements redundant CUs to perform its functions. The CUs acquire hardwired signals directly from field sensors or from other I&C systems. Outputs are sent to non-safety-related actuators. The CUs interface with the PICS via the plant data network for manual commands and display of information.

Balance of Plant Subsystem

Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant Subsystem) provides a functional representation of the BPS.

The BPS is located in the Switchgear Building and other locations in the Balance of Plant as necessary.

The BPS implements redundant CUs to perform its functions. The CUs acquire hardwired signals directly from field sensors or from other I&C systems. Outputs are sent to non-safety-related actuators. The CUs interface with the PICS via the plant data network for manual commands and display of information.

Equipment

The PAS is implemented with an industrial digital I&C platform.

The PAS generally consists of subracks, I/O modules, function processors, communication modules, and optical link modules. Fiber optic and copper cable is used for the various data and hardwired connections. Specialized components, such as drive modules and interfaces to third party control systems, may be used.

Qualification Requirements

There are no qualification requirements for the NIS, TIS, or BPSPAS equipment.

Quality Requirements

There are no quality requirements for the NIS, TIS, or BPSPAS.

Diversity Requirements

There are no diversity requirements for the PAS.

Data Communications

The functional units in the PAS interface to the PICS via networked connectionsthe plant data network.

07.01-26

The NISPAS in the NI may implements point-to-point networked data connections between the CUs in each division to share signals as needed (e.g., to implement signal selection algorithms).

The PAS will have adequate bandwidth to reliably operate the process systems in the reactor plant needed for plant operation and to keep the plant reliably online.

Other types of data connections may be implemented within the same division of the NIS and the PAS.

The TIS and BPS are not divisionalized. Other types of data connections may be implemented within the TIS and BPS.

Power Supply

The PAS is powered by the following power supplies:

- Safeguard Buildings - 12UPS.
- Turbine Building - non-Class 1E uninterruptible power supply (NUPS).
- Other buildings - UPS and diesel backed source.

various subsystems of the PAS have different power supplies.

The NIS is powered from the 12hr UPS. The 12hr UPS provides backup power with 12-hour batteries and the SBODGs in the event of a LOOP.

The TIS and the BPS are powered from the non-Class 1E uninterruptible power supply (NUPS). The NUPS provides backup power with 2-hour batteries and the SBODGs in the event of a LOOP.

The electrical power systems are described in detail in Chapter 8.

7.1.1.4.7 Diverse Actuation System (DAS)

The DAS is the non-safety-related I&C system that provides diverse actuation of protective functions in the unlikely event of an ATWS or a software common cause failure of the PS.

Classification

The DAS is classified as non-safety related, augmented quality.

Functions

Table 7.1-3 shows the functions of the DAS.

07.01-26

Interfaces

Table 7.1-4 shows the interfaces of the DAS.

~~The DAS performs automatic risk-reduction functions, including:~~

- ~~Mitigation of ATWS and PS software common cause failure.~~
- ~~Manual, system-level actuation of critical safety functions.~~
- ~~Mitigation of SBO.~~
- ~~Mitigation of other risk significant events.~~

Architecture

Figure 7.1-13—Diverse Actuation System Architecture provides a functional representation of the DAS.

The DAS is organized into four redundant divisions located in separate Safeguards~~s~~ Buildings. Each division of the DAS contains a diverse actuation unit (DAU). Hardwired signals are acquired from the ~~PS~~SCDS~~, as described in Section 7.1.1.6.4,~~ and compared to a setpoint. ~~Fiber optic data~~Hardwired connections are provided to share trip requests, and two-out-of-four voting is done in each DAU. Outputs are sent to the reactor trip breakers, CRDCS, TG I&C, and PACS via hardwired connections. Signals are also sent to the PAS to display information on PICS and to coordinate logic, as necessary.

The DAUs interface with the ~~P~~SICS via ~~the plant data network~~hardwired connections to receive manual system level commands and to display information.

Equipment

The DAS is implemented with non-microprocessor based technology.~~an industrial digital I&C platform.~~

The DAS generally consists of various modules, such as threshold comparators, voting, and alarm modules.~~subracks, I/O modules, function processors, communication modules, and link modules. Fiber optic and c~~Copper cable is used for the ~~various data and~~ hardwired connections. Specialized components may be used.

Qualification Requirements

~~In the unlikely event of a software common cause failure of the PS, t~~The DAS equipment must function properly under conditions during and following AOOs or PAs concurrent with a CCF of the PS~~design basis events~~. The DAS equipment is located in Safeguard Buildings that provide a mild environment during and following

07.01-26

AOOs or PAsdesign basis events. Equipment selected for use in the DAS shall be rated by the manufacturer (or otherwise reasonably expected) to operate under the mild environmental conditions expected to exist at its location during the events for which the equipment is expected to respond.

Quality Requirements

As a system relied on to mitigate the effects of AOOs and PAs concurrent with a CCF of the PS, the DAS is required to be of sufficient quality to perform its functions in a reliable manner. The DAS is therefore designed using a robust engineering process with appropriate reviews, verification, tests, and approvals. Sufficient quality is achieved in the design of the DAS through the following measures:

- The DAS is designed, fabricated, erected, and tested under the quality assurance program described in Topical Report ANP-1066A, Addendum A (Reference 42). This quality assurance program is consistent with the guidance of Generic Letter 85-06 (Reference 43).
- The design of the DAS is accomplished through a phased approach including the following (or equivalent) phases:
  - System requirements phase.
  - System design phase.
  - Software/hardware requirements phase.
  - Software/hardware design phase.
  - Software/hardware implementation phase.
  - Software/hardware validation phase.
  - System integration phase.
  - System validation phase.
- A criticality analysis is performed for the DAS software in accordance with accepted industrial practice.
- Verification and validation (V&V) of the DAS software is performed according to a V&V plan that is consistent with accepted industrial practice.
- DAS requirements are documented in a traceable form that is under configuration management.
- The DAS design is validated through acceptance test in the system validation (or equivalent) phase.

07.01-26

Diversity Requirements

The DAS ~~is~~ credited by the defense-in-depth and diversity analysis is described in Section 7.8. Diversity requirements for DAS are described in Reference 8~~:~~.

Data Communications

There are no data communications associated with the DAS.

~~The DAS interfaces with the PICS via the plant data network and implements point-to-point data connections between the DAUs for voting purposes.~~

~~Other types of data communications may be implemented within the same division in the DAS.~~

Power Supply

The DAS is powered from the 12-UPS. The 12-UPS provides backup power with 12-hour batteries and the SBODGs in the event of a LOOP.

7.1.1.4.8 Signal Conditioning and Distribution System (SCDS)

The SCDS is a safety-related system that performs signal conditioning and distribution of signals from sensors or black boxes.

Classification

The SCDS is classified as safety-related.

Functions

Table 7.1-3 shows the functions of the SCDS.

Interfaces

Table 7.1-4 shows the interfaces of the SCDS.

Architecture

Figure 7.1-23—Signal Conditioning and Distribution System Architecture provides a functional representation of the SCDS.

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

- Safeguard Buildings.
- Emergency Power Generating Buildings.

07.01-26

- Essential Service Water Pump Structures.

In each division, there are safety-related and non-safety-related SCDS equipment to interface with safety-related and non-safety-related sensors, respectively. The safety-related SCDS and non-safety-related SCDS equipment is located in separate cabinets.

The SCDS is composed of non-computerized signal conditioning modules and signal distribution modules that are part of the TXS platform. Multiple signal conditioning modules or signal distribution modules may be used for a particular signal, depending on the required conditioning and the number of DCS systems the output signal is required in.

The SCDS receives hardwired signal inputs from sensors or black boxes. The SCDS sends hardwired signal outputs to the SICS, DAS, PS, SAS, RCSL, and PAS, as needed. Outputs from safety-related SCDS equipment to non-safety-related DCS systems are electrically isolated by the signal distribution modules.

Equipment

The SCDS is implemented with TXS signal conditioning and distribution equipment.

The SCDS is implemented primarily with subracks, signal conditioning modules, and signal distribution modules.

Qualification Requirements

The equipment used in the SCDS is qualified for environmental, seismic, electromagnetic interference, and radio frequency interference (EMI/RFI) conditions in accordance with the environmental qualification program described in Section 3.11.

Quality Requirements

The SCDS is designed under the TXS quality program described in Section 7.1.1.2.1.

Diversity Requirements

The signal conditioning and distribution modules are diverse from the digital TXS function processors. In addition, the signal conditioning and distribution modules are simple devices that are not considered susceptible to software CCF.

Data Communications

There are no data communications in the SCDS.

07.01-26

Power Supply

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

The non-safety-related SCDS equipment in the Safeguard Buildings is powered from the 12UPS. The 12UPS provides backup power with 12-hour batteries and the SBODGs during a LOOP.

The non-safety-related SCDS equipment in the Emergency Power Generating Buildings and the Essential Service Water Pump Structure is powered from an UPS and diesel backed source.

7.1.1.5 ~~Level 0 - Process Interface~~Other I&C Systems

~~The process interface level includes components such as sensors, actuators, and switchgear.~~

~~The majority of the process interface equipment is included within the mechanical and electrical process systems that the I&C systems monitor and control. These systems are described in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10 and Chapter 11. Additionally, the plant fire alarm system (PFAS) and the Communication System are described in Chapter 9, Sections 9.5.1 and 9.5.2, respectively.~~

~~The systems listed in the following sections are distinct I&C systems within the process interface level.~~

7.1.1.5.1 Control Rod Drive Control System

Classification

The CRDCS is classified as non-safety-related. ~~The trip contactors are safety-related.~~

Description

The CRDCS controls the actuation of the 89 rod cluster control assemblies (RCCA) in the reactor vessel. The CRDCS accomplishes this task by providing current to the individual coils of the control rod drive mechanism (CRDM) to move the corresponding RCCA.

The CRDCS receives DC power from the NUPS to move and hold the CRDMs. The reactor trip breakers are upstream of the CRDCS. Refer to Section 8.3 for more information on the NUPS and the reactor trip breakers.

Within the CRDCS, the safety-related trip contactor modules interrupt power to the CRDMs when a trip signal is received from the PS. The trip contactors get a signal from each division of the PS and are arranged to implement two-out-of-four logic. The contactor modules are environmentally qualified, including seismic, EMI, and RFI effects.

07.01-26

The DAS provides a reactor trip signal to the CRDCS in case of an AOO or PA concurrent with a CCF of the PS. The reactor trip signal is sent to the control logic to drop the rods in a diverse manner from the trip contactors.

The RCSL transmits commands containing the direction of movement (i.e., withdrawal or insertion), speed of movement, and drop and hold information to the CRDCS. Withdrawal and insertion commands are used for reactor control functions. Drop orders are issues for a partial or full reactor trip in support of the reactor limitation functions. Refer to Section 7.7.1 for a description of the reactor control and limitation functions.

The non-safety-related components of the CRDCS are designed such that a seismic event does not result in damage that disables the safety function of the trip contactors.

Refer to Section 4.6.2 for more information on the reactivity control systems.

7.1.1.5.2 Incore Instrumentation System

Classification

The incore instrumentation system (ICIS) is classified as safety-related.

Description

Figure 4.4-8—Arrangement of Incore Instrumentation (Top View) shows the arrangement of the various components within the core.

Figure 7.1-24—Self Powered Neutron Detector Functional Arrangement shows the signal path of the SPNDs through the incore equipment into the SCDS for distribution in the other DCS systems.

The ICIS measures certain in-vessel parameters. The ICIS consists of safety-related and non-safety-related equipment.

The ICIS consists of:

- Self-powered neutron detectors (SPND) (safety-related except for test equipment).
- Aeroball measurement system (AMS) (non-safety-related).
- Fixed core outlet thermocouple (COT) measurement system (safety-related).

- Reactor pressure vessel dome temperature (RPVDT) measurement system (non-safety-related).

There are 72 SPNDs that continuously measure the neutron flux at given positions in the core to provide information about the three-dimensional flux distribution. The AMS is used to calibrate the SPNDs at regular intervals. The SPNDs and AMS are described in detail in the Incore Transient Methodology Topical Report (ANP-10287P) (Reference 7).

The COT continuously measures coolant temperature at the outlet of the fuel assembly. The fixed thermocouples are placed in selected fuel assemblies that are located azimuthally and radially within the core. The core outlet temperature is used to determine the saturation margin (ΔT_{sat}) at the core exit and provide information about the radial temperature distribution in the core and average temperature in the reactor coolant system (RCS). There are a total of 36 COTs. The COTs are arranged with three thermocouples (two narrow range thermocouples and one wide range thermocouple) within each of the twelve SPND finger assemblies.

The RPVDT measurement system continuously measures the temperature within the reactor dome. The sensing elements are thermocouples, which are passive devices that do not use electrical power. RPVDT instrumentation provides temperature signals corresponding to the top-level, mid-level, and bottom-level measurement regions of the dome. The measurements of fluid temperature in the RPV dome provide information to the operator during normal and emergency operations if they are available (although not required for post-accident monitoring).

The main functions of the dome thermocouples are to:

- Indicate a potential steam bubble.
- Indicate average dome temperature.
- Indicate temperature above the RCCA plate to determine temperature difference across the plate.
- Indicate air temperature during RCS venting during startup.

7.1.1.5.3 Excore Instrumentation System

Classification

The excore instrumentation system (EIS) is classified as safety-related.

Description

The EIS monitors neutron flux during power and shutdown modes of operation. Because it is not possible to measure the entire operating range of reactor power with a single instrument, three ranges of detection are used.

- Power range – uses an uncompensated, boron lined ionization chamber detector.
- Intermediate range – uses a gamma compensated, boron lined ionization chamber detector.
- Source range – uses a boron lined proportional counter detector.

Figure 7.1-14—Measuring Ranges of Excore Instrumentation illustrates the coverage and overlaps of the excore detectors. These ranges provide coverage from shutdown conditions to about 200 percent reactor power. Overlaps in the measuring ranges are provided to allow operation of each range during transitions in power levels.

Figure 7.1-15—Excore Instrument Detector Locations illustrates the arrangement of the excore detectors.

There are eight power range detectors (PRD) that cover the upper three decades up to 200 percent reactor power. Two detectors are located in one of four radial locations around the core (45°, 135°, 225°, 315°). The two detectors at each location measure the center of the upper and lower portions of the core for monitoring and control of axial flux distributions.

Four intermediate range detectors (IRD) monitor a little more than seven decades up to at least 60 percent full power, with an overlapping of the source range by about 2.5 decades. They are located in the same radial locations as the PRDs.

Three source range detectors are provided at three radial locations around the core (0°, 90°, 270°). The source range detectors monitor the lower six decades.

7.1.1.5.4 Boron Concentration Measurement System

Classification

The boron concentration measurement system (BCMS) is classified as safety-related.

Description

07.01-26

Figure 7.1-16—Boron Concentration Measurement System Arrangement illustrates the arrangement of the BCMS.

The BCMS measures the boron concentration in the CVCS. The measured boron concentration is conditioned and compensated for temperature effects. The resulting

07.01-26

signal is sent to the SCDS for distribution to various systems within the DCS. The signal is ~~further processed and~~ used by the PS to mitigate the risk of homogeneous and heterogeneous dilution of the RCS. Each boron concentration signal generated by the four redundant measuring devices is processed in a separate division.

To measure boron concentration, an Americium-Beryllium neutron source is used. The neutron source is located adjacent to CVCS piping. Neutrons are counted on the other side of the pipe. The number of neutrons counted is indicative of the boron concentration of the CVCS. A temperature sensor is used to measure the temperature of the fluid and provide a correction factor to the measured boron concentration.

7.1.1.5.5 Radiation Monitoring System

Classification

The radiation monitoring system (RMS) is classified as safety-related.

Description

The RMS performs these functions:

- Post-accident radioactivity monitoring.
- Process radioactivity monitoring.
- Effluent radioactivity monitoring.
- Airborne radioactivity monitoring.
- Area radioactivity monitoring.

The U.S. EPR digital radiation monitoring system (RMS) instrumentation and control includes self-testing features and diagnostics that allow early detection of failures. The tests and inspections of the RMS include checks, calibrations, and functional tests of the individual instrumentation channels which can be performed during power operation or refueling. Calibrations are performed in accordance with industry standards and manufacturer recommendations.

In addition, the RMS subsystems and components incorporate features for periodic and unscheduled maintenance, repair, and inspection. The purpose of these system inspection and maintenance capabilities is to minimize the occurrence of system faults and to increase RMS availability. Inspection intervals depend on the local situation and the working condition of the RMS. If a subsystem or component of the RMS is unavailable or removed for maintenance, inspection or repair, the ability of the redundant divisions to perform their safety-related functions is not impaired.

Access to the internally set parameters (e.g., calibration factors, alarm thresholds, and analog output ranges) is prohibited while the instrument is in operation. However, a dedicated portable test computer allows access to the internal parameters when the RMS is removed from service, and the test procedures described above are done with the help of this test computer. While the instrument is removed from service for testing, maintenance, or repair, it is put in a test mode that makes any output signal or alarm invalid.

The RMS consists of various detectors and processing equipment throughout the plant. Refer to Section 7.3.1 for radiation monitors used in ESF actuation functions. For radiation monitors used for PAM, refer to Section 7.5.1. For other monitoring functions, refer to Chapter 11 and Chapter 12.

7.1.1.5.6 Hydrogen Monitoring System

Classification

The hydrogen monitoring system (HMS) is classified as safety-related.

Description

The HMS is described in Section 6.2.5.

7.1.1.5.7 Reactor Pressure Vessel Level Measurement System

Classification

The reactor pressure vessel level (RPVL) measurement system is classified as supplemented grade (NS-AQ).

Description

Figure 4.4-8—Arrangement of Incore Instrumentation (Top View) shows the arrangement of the various components within the core.

Figure 4.4-10—Arrangement of Incore Instrumentation (Side View) illustrates the vertical arrangement of the RPVL measurement system.

The RPVL measurement system provides an indication to the operator of the water level in the reactor vessel. The RPVL measurement instrumentation primarily consists of four probes containing three thermocouple sensors each for level measurement. Three thresholds are detected by the RPVL measurement instrumentation.

- Higher threshold located at the top of hot leg of the RCS.
- Lower threshold located at the bottom of hot leg of the RCS.

- Intermediate threshold located between the top and the bottom of hot leg of the RCS.

Sensing elements consist of heated and unheated thermocouples. The difference between the signals of the heated and unheated thermocouples is used to indicate coolant level in the RPV. If the difference of the thermovoltages between heated and unheated thermocouples exceeds a defined threshold, this would indicate that the water level is below the heated thermocouples.

7.1.1.5.8 Seismic Monitoring System

Classification

The seismic monitoring system is classified as non-safety-related.

Description

The seismic monitoring system is described in Section 3.7.4.

7.1.1.5.9 Loose Parts Monitoring System

Classification

The loose parts monitoring system (LPMS) is classified as non-safety-related.

Description

The LPMS detects, locates, and analyzes detached or loosened parts and foreign bodies in the RCS and the secondary side of the steam generators during normal plant operation. By providing an early detection of loose parts, the probability of primary or secondary system component damage can be lessened and exposure to station personnel can be minimized.

Metallic loose parts excited by fluid streaming impact the inner wall of the pressurized boundary of the primary or secondary system. These impacts (also called bursts) generate structure borne noise, which can be detected by accelerometers attached to the outer surface of the monitored components. Signal conditioning equipment is used to provide the LPMS with reliable data. The signals are recorded and analyzed and common alarms are provided to the operators in the MCR upon violating predefined thresholds. Background noise generated by the plant is eliminated to the greatest extent possible to avoid faulty alarms or inaccurate measurements.

7.1.1.5.10 Vibration Monitoring System

Classification

The vibration monitoring system (VMS) is classified as non-safety-related.

Description

The VMS monitors changes in the vibration behavior of the RPV and its internals, the primary system components, the main coolant pumps, and portions of the main steam line structures in the secondary system by monitoring the frequencies and amplitudes of service-induced component and fluid vibrations.

Changes in the vibration behavior of a structure or component is one of the most sensitive indicators of a change in the condition of the component, such as reduction of screw bolt pretensions, reduction in the stiffness of core barrel hold-down springs, direct contact between primary components and the Containment Building, damage to main coolant pump bearings, and cracks in the main coolant pump shaft.

The system automatically performs measuring, analysis, and logging functions required for monitoring vibration, either at selectable intervals or upon operator command. Threshold violations caused by changes in frequency and amplitude are annunciated. In addition to component and fluid vibrations, process parameters such as temperature, pressure or flow rate, which have an influence on vibration behavior, are also acquired and then used to distinguish between service-induced and abnormal changes in vibration. This minimizes the probability of false diagnoses.

7.1.1.5.11 Fatigue Monitoring System

Classification

The fatigue monitoring system is classified as non-safety-related.

Description

The fatigue monitoring system is provided to record actual fatigue loading conditions on plant equipment. It measures various plant parameters such as temperature and pressure to calculate actual stress loads on major plant components. This allows the comparison of actual loads against design loading conditions, which provides plant operating personnel the information needed to adjust operations, maintenance, and inspection activities accordingly.

Thermocouples are used to measure actual component temperatures. System pressure is considered uniform and is received from existing sensors. The information is received, processed, stored and analyzed. Data is retrievable by operators and other plant personnel.

7.1.1.5.12 Leak Detection System

Classification

The leak detection system (LDS) is classified as non-safety-related.

Description

The LDS, in conjunction with other associated systems, promptly detects, quantifies, and localizes leakage from the RCPB and selected portions of the main steam system.

The LDS includes these components:

- Condensate mass flow measurement devices inside containment.
- Humidity and temperature sensors inside containment.
- Local humidity detection system for the main steam piping.

The leak-before-break approach for the U.S. EPR is described in Section 3.6.3. The RCPB leakage detection approach is described in Section 5.2.5.

07.01-26

The local humidity detection system measures local increases in relative humidity along appropriate portions of the ~~MS lines~~main steam lines (MSL) inside of the containment to detect and localize leakages from the lines ~~with a high degree of accuracy~~. The local humidity detection system is capable of detecting MSL leakage as low as 0.1 gallons per minute.

The condensate mass flow measurement devices inside containment measure condensate flow from the Reactor Building fan cooler collectors. Changes in the Containment Building relative humidity levels result in changes in the condensate flow rate. The condensate mass flow measurement devices inside containment are capable of measuring fan cooler condensate collector flow rates as low as 0.5 gallons per minute. Alarms and indications associated with the LDS are available to the operators in the MCR.

7.1.1.5.13 Turbine Generator I&C

The turbine generator (TG) I&C system regulates the operation of the turbine generator for power generation. It provides speed and load control, as well as control of TG auxiliaries. Refer to Section 10.2 for further information on the TG I&C.

07.01-26

7.1.1.5.14 Rod Position Measurement System (RPMS)

Classification

The RPMS is classified as safety-related.

Description

Figure 7.1-25—Rod Position Measurement System Arrangement shows the signal path of the rod position measurements through the RPMS equipment into the DCS for distribution.

07.01-26

The RCCA position measurement system (RPMS) measures the position of a RCCA located in the reactor vessel and provides the measurement to the DCS for control and indication to the operator.

CRDM Position Measurement Coils

The rod position measurement coils are part of the CRDM. The description of the coils is provided here for information.

The rod position sensor is comprised of one primary and three secondary coils. Two of the secondary coils, called auxiliary secondary coils, indicate the rod at its lowest or highest end position. The third secondary coil, or main secondary coil, indicates the entire range of RCCA travel. The analog position measurement of the RCCA is derived from the magnetic coupling through the control rod between the primary coil and the secondary coils. The auxiliary secondary coil signal determines the extreme positions of the drive rod.

The primary coil also provides an input to the RPMS equipment to compensate any variations in indicated RCCA position resulting from temperature effects.

Signal Conditioning and Processing Equipment

The signal conditioning and processing equipment is part of the RPMS.

The RPMS receives four inputs from the CRDM, which are the rod top signal, analog rod position signal, rod bottom signal, and temperature measurement signal for compensation.

The RPMS conditions these signals, and also performs temperature compensation of the analog rod position measurement. The signal processing is performed by analog conditioning modules and a TXS processing unit, the rod position measurement unit (RPMU).

The RPMS provides three signal outputs to the DCS for each RCCA, which include top, bottom, and temperature compensated analog position.

The RPMS is arranged in four divisions located in each of the four Safeguard Buildings. Divisions 1, 2, and 3 process measurement for 22 RCCAs, and Division 4 processes measurements for 23 RCCAs, for a total of 89 RCCA position measurements.

Each division of the RPMS has a MSI for testing and maintenance of the RPMS. Each MSI connects to a dedicated SU for the RPMS, which resides in the I&C service center. The RPMS MSI does not have any other connections than to its dedicated SU. The SU connections to the MSI are implemented in the same manner as the PS and SAS, which are described in Section 7.1.1.6.4.

7.1.1.6 I&C ArchitectureDCS Design Principles

7.1.1.6.1 Defense-in-Depth

07.01-26

The U.S. EPR implements the following lines of defense to establish the defense-in-depth principle:

- Preventive line of defense.
- Main line of defense.
- Risk reduction line of defense.

These lines of defense The overall defense-in-depth and diversity concept areis described in the Diversity and Defense-in-Depth Assessment Technical Report (ANP-10304) (Reference 8).

To implement the defense-in-depth principle, four primary functional categories are defined for proper operation of the plant. These categories are mapped to the various sections of this document.

- Safety I&C functions—used to prevent or mitigate DBEs:
  - Section 7.2—Reactor trip functions.
  - Section 7.3—ESF actuation and control functions.
  - Section 7.4—Safe shutdown functions.
  - Section 7.5—Safety-related information display functions.
  - Section 7.6—Interlock functions.
  - Chapter 8 and Chapter 9—Safety-related functions for auxiliary support features.
- Risk Reduction I&C functions—used to mitigate BDBEs:
  - Section 7.8—Diverse I&C functions.
  - Section 8.4—SBO mitigation functions.
  - Chapter 19—Severe accident and other risk mitigation functions.
- Limitation I&C functions:
  - Section 7.7—Control functions.
- Operational I&C functions:

07.01-26

– Section 7.7—Control functions.

Figure 7.1-17—Implementation of Defense-In-Depth illustrates the implementation of the defense-in-depth concept for the U.S. EPR.

7.1.1.6.2 Diversity

ANP-10304 (Reference 8) describes the diversity present in the DCS designI&C architecture based on the diversity attributes identified in NUREG/CR-6303.

7.1.1.6.3 Redundancy

Redundancy is implemented throughout the I&C architectureDCS design to prevent a single failure from causing a loss of function. The level of redundancy assigned depends on the classification and functional requirements of the system. Table 7.1-1—Levels of Redundancy in I&C Architecture illustrates the redundancies assigned to the various I&C systems.

7.1.1.6.4 Independence

For safety I&C systems, independence is established so that a single failure does not result in the loss of the safety function.

The following measures are implemented for the safety I&C systems:

- Independence between redundant divisions.
- Independence from the effects of DBEs.
- Independence between the safety-related I&C systems and the non-safety-related I&C systems.

Independence of Redundant Safety Divisions

Figure 7.1-19—Implementation of Independence Between Redundant Divisions illustrates the implementation of inter-divisional independence.

The SICS, PS, SAS, SCDS and PACS each consists of four independent divisions. Independence between redundant divisions is maintained using the following:

- Physical separation.
- Electrical isolation.
- Communications independence.

Independent divisions are located in each of the four physically separated Safeguardss Buildings.

07.01-26

Electrical isolation is required for hardwired and data connections, and is provided through the use of qualified isolation devices and fiber optic cable.

The ~~SICS,~~ PS~~,~~ and SAS implement interdivisional communications to support the system functional requirements. Communications independence is provided by the following features of the TXS platform:

- Communications modules are provided separate from the function processors performing the safety function.
- Communications are implemented with separate send and receive data channels.
- Asynchronous, cyclic operation of the function processors and communications modules.

In addition, only predefined messages are accepted by the receiving function processor, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

Refer to Section 2.9 of Reference 3 for more information on the principles of communications independence.

Independence from the Effects of Design Basis Events

The TXS equipment used in the safety-related I&C systems is qualified to withstand the effects of AOOs or PAs~~DBEs~~.

Independence between the Safety I&C Systems and Non-Safety I&C Systems

Figure 7.1-20—Implementation of Independence Between Safety and Non-Safety I&C illustrates the implementation of independence between safety-related and non-safety-related I&C systems.

Independence between safety-related and non-safety-related I&C systems is provided using these principles:

- Physical separation.
- Electrical isolation.
- Communications independence.

The safety-related I&C systems are physically separated from non-safety-related I&C systems.

Electrical isolation is provided for both hardwired and data communications between safety-related and non-safety-related I&C. For hardwired signals, qualified isolation

07.01-26

devices are used with the safety-related I&C systems for signals to and from the non-safety-related I&C. Fiber optic cable is used for data connections between safety-related and non-safety-related I&C.

Class 1E communication independence is provided between the PS and SAS and the PICS, and between the PS and SAS and their SUs by the safety-related MSI. The following features of the MSIs provide for communication independence:

- Communication modules separate from the function processors are used for the purpose of handling communications to the GWs.
- Communications between the function processors and communications modules are implemented with separate send and receive data channels.
- The function processors and communications modules operate cyclically and asynchronous to each other.

In addition, only predefined messages are accepted by the MSI, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

Section 2.9 of Reference 3 provides more information on the principles of communications independence for the TXS platform.

The non-safety-related networks between the MSI and SU and between the MSI and GWs contain design features that limit the scope of non-safety-related equipment failures that the MSI must protect against.

Connection between the MSI and GWs

This section describes the features in the non-safety networks between the MSI and PICS that eliminate the need for the MSI to protect against non-safety network communication failures between the MSI and the PICS.

The connection between the MSI and the GW is limited to one-way data communication from the MSI to the GW. This is accomplished via a segment that is physically restricted to unidirectional communication (transmit only port connected to receive only port). This interface is described in more detail in Reference 6.

Connection between the MSI and the SUs

This section describes the design and operation of the SU and describes the features in the non-safety-related networks between the MSI and SU that limit the scope of faults in the non-safety-related SU that must be protected against by the PS and SAS MSIs.

The SU is a non-safety-related, standard computer that is temporarily connected to a TXS system when needed to perform surveillances or troubleshoot.

07.01-26

The SU connection is located in the I&C service center. The communication path between the SU and the divisional MSIs for PS and SAS are isolated by hardwired disconnects while not in use. This is achieved with key operated isolation switches located in the control room. This allows the control room operators to monitor the position of the isolation switches, providing them with control over the connection of the SU. A local connection point for SU connection is located in the lockable MSI cabinet in each PS and SAS division. Control room annunciation will communicate the access to the local connection using the'door open alarm. This local connection is isolated by a key-operated isolation switch. The isolation switches in a system are keyed so that a single key operates the eight switches (four MCR and four local), and they are physically retained in the switch when positioned to allow the SU connection to the system. This prevents the connection of a SU to more than a single division of the PS or SAS.

The SU isolation switches are connected to prevent the SU from being connected to more than a single division of a system at a time. In the unlikely event of a fault caused by the non-safety-related SU, the fault will be confined to a single division, which is bounded by the current plant design basis. The design of the safety systems will prevent the SU from operating any plant equipment.

Each PS and SAS processor has a CPU state switch that controls each processor's operation state. These keyswitches are located in the associated processor's TXS cabinet. The keyswitches prevent alteration of modifiable parameters and changes to software from the SU, except when the processor is placed in the proper operational state for the change. TXS processors can be in one of four operating states using the CPU state switch:

1. Cyclic processing state (operable for Technical Specifications).
   - Processor operates normally, outputs are active.
   - SU cannot modify processor software or parameters.
2. Parameterization state (inoperable for Technical Specifications).
   - Processor operates normally, outputs are active.
   - SU can only modify predefined, changeable parameters (e.g., calibration constant).
3. Functional test state (inoperable for Technical Specifications).
   - Processor outputs disabled, can be selectively enabled via SU for testing purposes.
   - SU can modify predefined, changeable parameters.

07.01-26

4. Diagnosis state (inoperable for Technical Specifications).

 – Processor outputs disabled, cannot be enabled.

 – New version of application software can be loaded.

The keys associated with the CPU state switches and the isolation switches are part of the key control program. This provides a layer of protection via administrative controls and allows the operators to have specific control of what items are able to be made inoperable and what software/setpoints are available for alteration.

During normal operation (SU isolation switches open), fault alarms are collected in the application software of the PS or SAS computers and are sent to the PICS for alarm annunciation and logging. The detailed information about these faults will be downloaded to the SU from the message buffer on the next SU connection. In the event where multiple fault alarms occur in the system, some messages may be lost because the message buffer has limited space. The messages are stored in the order received, with any messages received after filling the buffer being lost, which allows the initiating fault messages to be retained.

The SU will only be connected to a division to:

1. Perform Technical Specification Surveillance Requirements and Actions.

2. Diagnose system faults following indication of a fault.

3. Load new software versions needed to implement approved plant design changes.

The SU is not intended to be continuously connected or used, except as part of approved procedures. These procedures prescribe when to connect the SU and when to disconnect the SU along with the initial conditions and the required retest.

Before closing the isolation switch and establishing communication between the SU and the safety system, it is necessary to perform and pass cyber security checks to verify the condition of the SU in accordance with the Cyber Security Program.

The CPU state switch keys and the isolation switch key are part of the key control program. The key will be issued to the maintenance personnel by the operators. This provides a layer of protection via administrative controls and allows the operators to have specific control of the state of the equipment.

~~Communications independence is provided between the safety-related I&C systems and the non-safety-related I&C systems via the MSIs. Connections to the SUs are also via the MSI.~~

~~These features of the MSIs provide for communications independence:~~

07.01-26

- Communication modules separate from the function processors for the purpose of handling communications to the GWs.
- Communications between the function processors and communications modules are implemented with separate send and receive data channels.
- The function processors and communications modules operate cyclically and asynchronous to each other.

In addition, only predefined messages are accepted by the MSI, and data integrity checks are performed on the received messages. Faulted messages are flagged and ignored in subsequent logic.

Refer to Section 2.9 of Reference 3 for more information on the principles of communications independence for the TXS platform.

Data connections exist between the PAS and PACS. However, this connection is only between the PAS and non-safety-related PACS communication module. Connections between the communication module and safety-related priority module are hardwired. The communication module is qualified as an associated circuit.

The safety-related I&C systems are implemented in four independent divisions. The safety-related I&C systems retain their ability to perform their function given a single failure of a common element to both the safety-related and non-safety-related systems concurrent with another single failure. The control systems implement signal selection algorithms and redundancy to minimize the possibility of a single failure that results in an AOO design basis event that also reduces the redundancy of the safety-related systems. The safety-related systems implement error detection algorithms to detect and accommodate failures.

7.1.1.6.5 Priority

The U.S. EPR I&C design allows for multiple I&C systems to send requests to a given actuator. To make certain that each individual actuator executes the proper action for the given plant condition, priority management rules for the PACS are provided. The following systems inputs to the PACS are listed in order of priority:

- PS.
- DAS.
- SAS.
- SICS.
- PAS.

07.01-26

The DAS is given a higher priority than the SAS because it is a functional substitute to the PS and is needed at this level of priority to verify proper operation of SAS functions on a CCF of the PS.

During normal operation, the operational I&C disable switch on the SICS is set so that the PAS can send commands to the PACS. In this configuration, automatic commands from the PAS override manual commands from the SICS because of the nature of the manual control logic in the PACS. If the operational I&C disable switch is set to DISABLE by the operator, the PAS input will be disabled, verifying the priority of the SICS manual commands.

~~The four primary functional categories provide the basis for priority management of the U.S. EPR I&C architecture.~~

~~The order of priority for I&C functions is listed from highest to lowest:~~

- ~~Safety-related I&C functions~~
  - ~~PS actuation functions~~
  - ~~SAS control functions~~
- ~~Non-safety-related reduction functions~~
  - ~~SA I&C functions~~
  - ~~DAS functions~~
- ~~Non-safety-related limitation functions (PAS, RCSL)~~
- ~~Non-safety-related operational I&C functions (PICS, PAS, RCSL)~~
  - ~~Equipment protection functions~~
  - ~~Automatic control~~
  - ~~Manual control~~

~~The PACS manages priority for safety-related plant components. Figure 7.1-8 shows the interfaces between PACS and the level 1 I&C systems. For non-safety-related plant components, priority is managed in the application software of the level 1 I&C systems.~~

7.1.1.6.6 ~~Cyber Security~~Deleted.

~~The U.S. EPR I&C design provides features for cyber security. These include:~~

07.01-26

- ~~Communications independence measures implemented between the non-safety-related I&C and safety-related I&C.~~
- ~~SUs for the safety-related I&C systems are not connected to non-safety-related I&C networks.~~
- ~~No direct connections from external networks to the safety-related I&C systems.~~
- ~~Connections between non-safety-related I&C networks and external plant networks are via a unidirectional firewall. Remote access to the I&C systems is prohibited. No other interface points are provided.~~

~~The I&C systems comprise a level of defense for cybersecurity. Figure 7.1-21—Levels of Defense for Cybersecurity illustrates these concepts.~~

~~External levels of defense and other features that provide for cyber security are addressed as part of the overall security plan, which is described in Section 13.6.~~

7.1.2 Identification of Safety Criteria

Table 7.1-2—I&C System Requirements Matrix, shows the I&C system requirements matrix which details the regulatory requirements for the I&C systems of the U.S. EPR.

The U.S. EPR is designed in accordance with IEEE Std 603-1998 (Reference 1). ANP-10309P (Reference 6) describes how IEEE Std 603-1998 (Reference 1) meets or exceeds the requirements established in IEEE Std 603-1991 (Reference 2).

These I&C systems are within the scope of the protection system as defined in IEEE Std 603-1998 (Reference 1):

- Protection system.
- Incore instrumentation system.
- Excore instrumentation system.
- Boron concentration measurement system.
- Radiation monitoring system.
- Process instrumentation (refer to Section 7.2 and Section 7.3 for details).
- Signal conditioning and distribution system.

The scope of the safety systems, as defined in IEEE Std 603-1998 (Reference 1) are those I&C systems that are classified as safety-related and the safety-related trip contactors.

7.1.2.1 Compliance to 10 CFR 50 and 52

7.1.2.1.1 10 CFR 50.55a(a)(1) – Quality Standards and Records for Systems Important to Safety

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements of 10 CFR 50.55a(a)(1). This is provided by compliance with Clause 5.3 (quality) of IEEE Std 603-1998 (Reference 1).

7.1.2.1.2 10 CFR 50.55a(h)(2) – Protection Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.55a(h)(2). This is provided by compliance with IEEE Std 603-1998 (Reference 1), which meets or exceeds the requirements established by IEEE Std 603-1991 (Reference 2).

7.1.2.1.3 10 CFR 50.55a(h)(3) – Safety Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.55a(h)(3). This is provided by compliance with conformance to IEEE Std 603-1998 (Reference 1), which meets or exceeds the requirements established by IEEE Std 603-1991 (Reference 2).

7.1.2.1.4 10 CFR 50.34(f)(2)(v) – Bypass and Inoperable Status Indication

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(v). This is provided by compliance to Clause 5.8.2 (system status indication) and Clause 5.8.3 (indication of bypasses) of IEEE Std 603-1998 (Reference 1). Refer to Section 7.5.2.1.1 for more information regarding bypassed and inoperable status.

7.1.2.1.5 10 CFR 50.34(f)(2)(xi) – Direct Indication of Relief and Safety Valve Position

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xi). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.6 10 CFR 50.34(f)(2)(xii) – Auxiliary Feedwater System Automatic Initiation and Flow Indication

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xii). Section 7.3.1.2.2 describes the automatic and manual initiation of the emergency feedwater (EFW) system. Section 7.5.2.1.1 describes the EFW flow indication.

7.1.2.1.7 10 CFR 50.34(f)(2)(xiv) – Containment Isolation Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xiv). Section 7.3.1.2.9 describes the containment isolation function, including reset of the function. Section 6.2.4 describes the containment isolation system.

7.1.2.1.8 10 CFR 50.34(f)(2)(xvii) – Accident Monitoring Instrumentation

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xvii). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.9 10 CFR 50.34(f)(2)(xviii) - Instrumentation for the Detection of Inadequate Core Cooling

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xviii). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.10 10 CFR 50.34(f)(2)(xix) – Instruments for Monitoring Plant Conditions Following Core Damage

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xix). Refer to Section 7.5.2.1.1 for more information.

7.1.2.1.11 10 CFR 50.34(f)(2)(xx) – Power for Pressurizer Level Indication and Controls for Pressurizer Relief and Block Valves

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements 10 CFR 50.34(f)(2)(xx). The pressurizer level sensors are acquired by the PS for the functions described in Section 7.2.1.2.12 and Section 7.3.1.2.10. The pilot valves for the pressurizer safety relief valves (PSRV) are controlled by the PS and PACS as described in Section 7.3.1.2.13. The PS and PACS are powered by the EUPS as described in Section 7.1.1.4.1 and Section 7.1.1.4.3. The PSRVs are described in Section 5.2. The EUPS is described in Section 8.3. Refer to Section 7.5.2 for more information.

7.1.2.1.12 10 CFR 50.62 – Requirements for Reduction of Risk from Anticipated Transients without Scram

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements of 10 CFR 50.62. Refer to Section 7.8.2.1.3 for more information.

7.1.2.2 Compliance to 10 CFR 50, Appendix A GDC

Compliance statements in this section are specific to the I&C systems. Refer to Section 3.1.1 for compliance to the GDC for the U.S. EPR.

7.1.2.2.1 GDC 1 – Quality Standards and Records

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements of GDC 1. This is provided by compliance with Clause 5.3 (quality) of IEEE Std 603-1998 (Reference 1).

7.1.2.2.2 GDC 2 – Design Bases for Protection against Natural Phenomena

07.01-26

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements for GDC 2. The applicable I&C systems are located within the four Safeguard~~s~~ Buildings and other safety-related structures as necessary. The design of these structures is described in Chapter 3. Compliance with Clause 5.4 (equipment qualification) of IEEE Std 603-1998 (Reference 1) demonstrates that the applicable I&C systems remain operable during and following seismic events.

7.1.2.2.3 GDC 4 – Environmental and Dynamic Effects of Design Bases

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements for GDC 4. This is provided by compliance with Clause 5.4 (equipment qualification) of IEEE Std 603-1998 (Reference 1).

7.1.2.2.4 GDC 10 – Reactor Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 10. Section 7.7 describes control and limitation functions that regulate the operation of the reactor and limit the effects of AOOs. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15. Setpoints for these protective actions shall be determined using the methodology described in U.S. EPR Instrument Setpoint Methodology (ANP-10275P) (Reference 11). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.2.2.5 GDC 13 – Instrumentation and Control

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 13. Refer to the I&C systems description in Section 7.1.1 for more information.

7.1.2.2.6 GDC 15 – Reactor Coolant System Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 15. Section 7.7 describes control and limitation functions that regulate the operation of the RCS and limit the effects of AOOs. Section 7.2 and Section 7.3 describe the I&C related protective actions credited in the RCS overpressure analysis described in Section 5.2.2. Setpoints for these protective actions shall be determined using the methodology described in ANP-10275P (Reference 11). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.2.2.7 GDC 16 – Containment Design

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 16. Section 7.3.1.2.9 describes the containment isolation function. Section 6.2.4 describes the containment isolation system. Section 7.3.1.2.1 describes the safety injection actuation function. This actuates the safety injection system, which provides for long-term heat removal from the containment and is described in Section 6.3.

7.1.2.2.8 GDC 19 – Control Room

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 19. Section 7.1.1.3.1 and Section 7.1.1.3.2 describe the capabilities of the SICS and PICS with regards to the capability for safe operation of the plant from the MCR during normal and accident conditions. Section 7.3.1.2.16 describes the MCR air conditioning isolation and filtering function to limit radiation levels in the MCR. Section 7.1.1.3.1 and Section 7.1.1.3.2 describe the capabilities of the SICS and PICS to achieve both hot and cold shutdown conditions from the RSS.

7.1.2.2.9 GDC 20 – Protection System Functions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 20. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15. Setpoints for these protective actions shall be determined using the methodology described in ANP-10275P (Reference 11). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.2.2.10 GDC 21 – Protection System Reliability and Testability

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 21. This is provided by compliance with IEEE Std 603-1998 (Reference 1). Specifically, compliance with Clause 5.1 (single-failure criterion), Clauses 5.7 and 6.5 (capability for testing and calibration), and Clauses 6.7 and 7.5 (maintenance bypass) demonstrates the capability for testing the applicable I&C systems during operation.

7.1.2.2.11 GDC 22 – Protection System Independence

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 22. This is provided by compliance with Clause 5.6 (independence) of IEEE Std 603-1998 (Reference 1).

7.1.2.2.12 GDC 23 – Protection System Failure Modes

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 23. The failure modes and effects analysis (FMEA) for the applicable I&C systems are described in Section 7.2.2.2 and Section 7.3.2.2.

7.1.2.2.13 GDC 24 – Separation of Protection and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 24. This is provided by compliance with IEEE Std 603-1998 (Reference 1). Specifically, compliance with Clause 5.1 (single-failure criterion), Clause 5.6 (physical, electrical, and communications independence), Clauses 6.3 and 6.6 (control protection interaction), Clause 5.12 (auxiliary features), and Clause 8 (power sources) limit the interconnections to assure that safety is not significantly impaired. Section 7.7 describes design features of the controls systems that minimize and limit challenges to the PS due to controls system failures. Worst-case credible failures of the plant control systems are postulated in the analysis of off-design operational transients and accidents described in Chapter 15.

7.1.2.2.14 GDC 25 – Protection System Requirements for Reactivity Control Malfunctions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 25. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15 for malfunctions of the reactivity control systems.

7.1.2.2.15 GDC 28 – Reactivity Limits

07.01-26

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 28. Section 7.7 describes the control systems for the U.S. EPR. Section 7.2 and Section 7.3 describe the protective actions implemented in the PS to mitigate the effects of AOOs and ~~postulated accidents~~PAs. Section 5.2.2 describes the overpressure analyses of the RCS, and Chapter 15 describes the safety analyses given malfunctions of control systems.

7.1.2.2.16 GDC 29 – Protection against Anticipated Operational Occurrences

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 29. Section 7.2 and Section 7.3 describe the protective actions credited in the accident analysis described in Chapter 15. Setpoints for these protective actions shall be determined using the methodology described in ANP-10275P (Reference 11). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.2.2.17 GDC 33 – Reactor Coolant Makeup

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 33. Reactor coolant makeup is provided by the chemical volume and control system (CVCS) and the safety injection system (SIS). Refer to Section 9.3.4 and Section 6.3 for more information about the CVCS and SIS, respectively. Section 7.7 describes the pressurizer level control function that provides for reactor coolant makeup using the CVCS. Section 7.3 describes the actuation of the SIS, which provides for a safety-related source of borated water for makeup for small breaks in the RCPB. The I&C systems that perform the various functions, including information on power supplies, are described in Section 7.1.1.

7.1.2.2.18 GDC 34 – Residual Heat Removal

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 34. The SIS performs the residual heat removal function, and is described in Section 6.3. Section 7.4 describes the use of SIS to achieve and maintain safe shutdown following an accident. Section 7.6 describes the interlocks associated with the SIS. Section 7.7 describes the use of SIS to remove decay heat during normal shutdown periods. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.19 GDC 35 – Emergency Core Cooling

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 35. The SIS performs the emergency core cooling function, and is described in Section 6.3. Section 7.3 describes the actuation of the SIS to provide abundant core cooling. Section 7.6 describes the interlocks associated with the SIS. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.20 GDC 38 – Containment Heat Removal

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 38. The SIS performs containment heat removal function, and is described in Section 6.3. Section 7.3 describes the actuation of the SIS. Section 7.6 describes the interlocks associated with the SIS. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.2.21 GDC 41 – Containment Atmosphere Cleanup

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 41. The combustible gas control system (CGCS) performs the containment atmosphere cleanup function, and is described in Section 6.2.5.

7.1.2.2.22 GDC 44 – Cooling Water

The applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 44. The essential service water system (ESWS) and component cooling water system (CCWS) are provided to transfer heat from the plant to the ultimate heat sink. These systems are described in Section 9.2.1 and Section 9.2.2, respectively. Section 7.3 describes the actuation of the SIS, which starts the CCWS and ESWS. Section 7.4 describes the use of the CCWS and ESWS to achieve and maintain safe shutdown. Section 7.6 describes the interlocks associated with the CCWS. The I&C systems that perform the various functions, including information on redundancy, independence, and power supplies, are described in Section 7.1.1.

7.1.2.3 Conformance to Staff Requirements Memoranda

7.1.2.3.1 SRM to SECY 93-087 II.Q – Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of the SRM to SECY 93-087 II.Q (Reference 10). The diversity and defense-in-depth (D3) assessment for the U.S. EPR is described in ANP-10304 (Reference 8). Section 7.1.1.4.7 describes the DAS, including architecture, quality and diversity requirements, and power supplies. Section 7.8 identifies the functions performed by the DAS.

The adequacy of the automatic functions of the DAS shall be verified as part of the plant procedures program described in Section 13.5. The adequacy of the controls and displays shall be verified in accordance with the human factors V&V program described in Section 18.10.

7.1.2.3.2 SRM to SECY 93-087 II.T – Control Room Annunciator (Alarm) Reliability

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of the SRM to SECY 93-087 II.T (Reference 10). Conformance is provided by these design features:

- Redundant PUs are provided for the transmittal of alarms to the operator workstations in the MCR.
- Multiple workstations are provided in the MCR. Each workstation has the same capabilities with regards to monitoring and control of plant systems.

7.1.2.4 Conformance to Regulatory Guides

7.1.2.4.1 RG 1.22 – Periodic Testing of Protection System Actuation Functions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.22. The measures for continuous self testing and periodic testing of the protection system actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

7.1.2.4.2 RG 1.47 – Bypassed and Inoperable Status Indication for Nuclear Power Plant Safety Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.47. The PICS automatically indicates the bypassed and inoperable status of the safety systems in the MCR. The bypassed and inoperable status of electrical auxiliary support features are described in Section 8.3.

7.1.2.4.3 RG 1.53 – Application of the Single-Failure Criterion to Safety Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.53, which endorses IEEE Std 379-2000 (Reference 11). The redundancy and independence of the applicable I&C systems is described in Section 7.1.1.6.3 and Section 7.1.1.6.4. The FMEA for the PS functions are described in Section 7.2.2.2 and Section 7.3.2.2.

7.1.2.4.4 RG 1.62 – Manual Initiation of Protective Actions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.62. The means for manual initiation of protective functions are described in Section 7.2 and Section 7.3.

7.1.2.4.5 RG 1.75 – Criteria for Independence of Electrical Safety Systems

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.75, which endorses IEEE Std 384-1992 (Reference 12) with modifications. The design features that provide for independence are described in Section 7.1.1.6.4.

7.1.2.4.6 RG 1.97 – Criteria for Accident Monitoring Instrumentation for Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.97, which endorses IEEE Std 497-2002 (Reference 13) with modifications. Accident monitoring instrumentation is described in Section 7.5.1.2.

7.1.2.4.7 RG 1.105 – Setpoints for Safety-Related Instrumentation

The setpoints for the applicable I&C systems listed in Table 7.1-2 shall be developed using the guidance of RG 1.105, with the exception of those differences described in Instrument Setpoint Topical Report (ANP-10275P) (Reference 14). The setpoint methodology described in ANP-10275P (Reference 14) implements the guidance of Setpoints for Nuclear Safety Related Instrumentation (ANSI/ISA-67.04.01-2006) (Reference 15) which accounts for recent industry advances in setpoint methodologies. ANP-10275P (Reference 14) provides justification for its use as an acceptable method for calculating setpoints. The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints. ~~Additional guidance for setpoints associated with both safety-related and non-safety-related systems is described in ISA-TR67.04.09-2005, "Graded Approaches to Setpoint Determination" (Reference 41).~~

7.1.2.4.8 RG 1.118 – Periodic Testing of Electric Power and Protection Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.118, which endorses IEEE Std 338-1987 (Reference 16) with modifications. The measures for continuous self testing and periodic testing of the protection system actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

7.1.2.4.9 RG 1.151 – Instrument Sensing Lines

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.151, which endorses ISA-S67.02-1980 (Reference 17) with modifications. The design features of the controls systems that minimize and limit challenges to the PS failures of a single sensing line common to both protection and control functions are described in Section 7.7. The redundancy and independence of the PS that maintain functionality in the event of a single sensor failure are described in Section 7.1, Section 7.2, and Section 7.3.

7.1.2.4.10 RG 1.152 – Criteria for Use of Computers in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall conform to the guidance of RG 1.152, which endorses IEEE 7-4.3.2-2003 (Reference 18). Conformance to IEEE 7-4.3.2-2003 (Reference 18) is described in Section 7.1.2.6 with the compliance of IEEE 603-1998 (Reference 1).

RG 1.152 also provides additional guidance for cyber security. Conformance to the cyber security elements of RG 1.152 (Regulatory Positions 2.1 through 2.5) are addressed in Section 13.6 as part of the security plan. The standard TXS platform (hardware and operating system) was designed several years prior to the issuance of Revision 2 to RG 1.152. Aspects of the TXS platform design that address the nuclear safety aspects of communication independence, safety to non-safety system isolation, and interference-free communication are equally applicable to cyber security. Some elements of the development activities are not explicitly addressed as cyber security activities in EMF-2110(NP)(A) (Reference 3) and the associated NRC safety evaluation report. The development process, including cyber security controls, for TXS application software for U.S. projects is described in ANP-10272 (Reference 5). The cyber security controls for TXS application software development fully meets the intent of Regulatory Positions C.2.1 through C.2.5.

7.1.2.4.11 RG 1.168 – Verification, Validation, Reviews and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall conform to the guidance of RG 1.168, except for the differences described in ANP-10272 (Reference 5) with regard to the use of alternate V&V methods. The methods used for software V&V are described and justified in ANP-10272 (Reference 5).

7.1.2.4.12 RG 1.169 – Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall conform to the guidance of RG 1.169, with the exception that a configuration control board is not used. The methods used for software configuration management plans are described and justified in ANP-10272 (Reference 5).

7.1.2.4.13 RG 1.170 – Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.170. Refer to ANP-10272 (Reference 5) for a description of the software test documentation.

7.1.2.4.14 RG 1.171 – Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.171. Refer to ANP-10272 (Reference 5) for a description of software unit testing.

7.1.2.4.15 RG 1.172 – Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.172. Refer to ANP-10272 (Reference 5) for a description of software requirement specifications.

7.1.2.4.16 RG 1.173 – Developing Software Life Cycle Processes for Digital Computer Software used in Safety Systems of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be developed in accordance with the guidance of RG 1.173. Refer to ANP-10272 (Reference 5) for a description of software requirement specifications.

7.1.2.4.17 RG 1.180 – Guidelines for Evaluating Electromagnetic and Radio-Frequency Interference in Safety-Related Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.180. The equipment qualification program, which includes EMI/RFI qualification, is described in Section 3.11.

7.1.2.4.18 RG 1.189 – Fire Protection for Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of RG 1.189. The design of the SICS, PICS, and the RSS are described in Section 7.1.1.3.1, Section 7.1.1.3.2, and Section 7.4.1.3.2. These systems provided the capability to achieve hot and cold shutdown from the RSS in case of a fire. Fiber optic cable is extensively used for communications to the Level 1 I&C systems to reduce the risk of fires and hot shorts. The fire analysis for the U.S. EPR is described in Chapter 9.

7.1.2.4.19 RG 1.204 – Guidelines for Lightning Protection of Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.204, which endorses IEEE Std 1050-1996 (Reference 19) and IEEE Std C62.23-1995 (Reference 20). Refer to Section 8.3 for more information on lighting and surge protection for the U.S. EPR.

7.1.2.4.20 RG 1.209 – Guidelines for Environmental Qualification of Safety-Related Computer-Based Instrumentation and Control Systems in Nuclear Power Plants

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of RG 1.209, which endorses IEEE 323-2003 (Reference 21) with modifications. The equipment qualification program is described in Section 3.11.

7.1.2.5 Conformance to Branch Technical Positions

7.1.2.5.1 BTP 7-1 – Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-1 (Reference 22), with the exception that the applicable RHR valves are not automatically shut upon re-pressurization of the RCS. The RHR suction valve interlocks and a justification for this approach are described in Section 7.6.1.2.1.

7.1.2.5.2 BTP 7-2 – Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-2 (Reference 23). The interlocks associated with the safety injection accumulators are described in Section 7.6.1.2.1.

7.1.2.5.3 BTP 7-3 – Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service

The applicable I&C systems listed in Table 7.1-2 are designed to the meet the intent of the guidance of BTP 7-3 (Reference 24). Upon a loss of a RCP, a three-loop signal is automatically generated and is used to modify the calculation of various reactor trips described in Section 7.2 to account for the changes in flow rate. This performs the same effect as modifying the setpoint.

7.1.2.5.4 BTP 7-4 – Guidance on Design Criteria for Auxiliary Feedwater Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-4 (Reference 25). Section 7.3 describes the actuation of the EFW system and the FMEA of the PS. Section 10.4.9.3 describes the capability of the EFW system to withstand a postulated line break, an active single failure, and a LOOP.

7.1.2.5.5 BTP 7-5 – Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-5 (Reference 26). Section 7.7 describes the control and limitation functions that regulate reactor operation. Section 15.4 describes the assumptions and analysis for reactivity and power distribution anomalies.

7.1.2.5.6 BTP 7-8 – Guidance for Application of Regulatory Guide 1.22

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-8 (Reference 27). Section 7.2.2.3.5 and Section 7.3.2.3.6 describes the continuous self-testing measures and design for periodic testing. The PS and PACS provide the capability to periodically test actuated equipment at the intervals required by the technical specifications for the process systems in described Chapter 16.

7.1.2.5.7 BTP 7-9 – Guidance on Requirements for Reactor Protection System Anticipatory Trips

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-9 (Reference 28). The reactor trips implemented in the PS meet the requirements of IEEE 603-1998 (Reference 1). The RCSL performs non-safety-related, non-credited partial trips and an anticipatory full reactor trip on a complete loss of feed. Refer to Section 7.7 for further information.

7.1.2.5.8 BTP 7-10 – Guidance on Application of Regulatory Guide 1.97

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-10 (Reference 29). Accident monitoring instrumentation is described in Section 7.5.1.2.

7.1.2.5.9 BTP 7-11 – Guidance on Application and Qualification of Isolation Devices

The applicable I&C systems listed in Table 7.1-2 shall be designed to meet the guidance of BTP 7-11 (Reference 30). The equipment and means provided for isolation are described in Section 7.1.1.

7.1.2.5.10 BTP 7-12 – Guidance on Establishing and Maintaining Instrument Setpoints

The setpoints for the applicable I&C systems listed in Table 7.1-2 shall be developed using the guidance of BTP 7-12 (Reference 31). The setpoint methodology is described in ANP-10275P (Reference 14). The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

7.1.2.5.11 BTP 7-13 – Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors

The applicable I&C systems listed in Table 7.1-2 implement the guidance of BTP 7-13 (Reference 32). The method for cross-calibration of PS resistance temperature detectors (RTD) is provided in Siemens Topical Report EMF-2341P (Reference 39).

7.1.2.5.12 BTP 7-14 – Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 shall be developed using the software development and V&V processes described in ANP-10272 (Reference 5).

Conformance with BTP HICB 7-14 (Revision 4 of NUREG 0800, "Standard Review Plan") is described in ANP-10272 (Reference 5). The topical report identifies specific differences and provides appropriate justification. BTP HICB-14 was used, since it was the version of the guidance in effect at the time the topical report was submitted for approval. AREVA NP provided additional information on alignment with BTP HICB-14 during the review of the topical report. Both BTP HICB-14 (Revision 4, June 1997) and BTP 7-14 (Reference 33) are based on the same regulations, RGs, and endorsed IEEE Standards. As such, acceptance of the topical report, based on these common regulatory requirements, is sufficient to address conformance with BTP 7-14. The software quality assurance plan, software safety plan, software verification and validation plan, and software configuration management plan required by ANP-10272 (Reference 5) are designed to make sure there is proper implementation of the TXS application software development activities and the proper production of the required design output documents.

7.1.2.5.13 BTP 7-17 – Guidance on Self-Test and Surveillance Test Provisions

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-17 (Reference 34). The measures for continuous self testing and periodic testing of the protection system actuation functions are described in Section 7.2.2.3.5 and Section 7.3.2.3.6.

7.1.2.5.14 BTP 7-18 – Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP 7-18 (Reference 35). The system hardware, software, and engineering tools used in the PS, SAS, and SICS are qualified in accordance with the processes described in Reference 3. Application software is developed using the processes described in ANP-10272 (Reference 5).

7.1.2.5.15 BTP 7-19 – Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP-19 (Reference 36), with the exception of providing system level actuation of critical safety functions. The diversity and defense-in-depth (D3) assessment for the U.S. EPR is described in ANP-10304 (Reference 8). Section 7.1.1.4.7 describes the DAS, including architecture, quality and diversity requirements, and power supplies. Section 7.8 identifies functions performed by the DAS.

7.1.2.5.16 BTP 7-21 – Guidance on Digital Computer Real-Time Performance

The applicable I&C systems listed in Table 7.1-2 are designed to meet the guidance of BTP-21 (Reference 37). The design features that provide for real-time, deterministic behavior of the SICS, PS, and SAS are described in EMF-2110(NP)(A) (Reference 3). Acceptable response times for protective actions are described in Section 15.0.

7.1.2.6 Compliance to IEEE Std 603-1998

This section describes compliance to IEEE Std 603-1998 (Reference 1). IEEE Std 603-1998 meets or exceeds the requirements of IEEE Std 603-1991 (Reference 2). By demonstrating compliance to IEEE Std 603-1998, compliance to 10 CFR 50.55a(h) is satisfied.

07.01-26

Pursuant to 10 CFR 50.55a(a)(3)(i), two alternatives to IEEE Std 603-1991 were proposed for the U.S. EPR design (Reference 45). First, regarding safety-related I&C and electrical systems, IEEE Std 603-1998 is used by the U. S. EPR design in lieu of IEEE Std 603-1991. Second, regarding the self-powered neutron detector (SPND)-based reactor trip functions, the use of a conservative setpoint selection method to satisfy single failure requirements is used by the U. S. EPR design as an alternative to

07.01-26

independence between redundant divisions required by IEEE Std 603-1991, Clause 5.6.1.

Where applicable, compliance to Clauses of IEEE Std 603-1998 (Reference 1) is supplemented with conformance statements to IEEE Std 7-4.3.2-2003 (Reference 18) to address the digital safety systems (SICS, PS, and SAS).

The Clauses of IEEE Std 603-1998 (Reference 1) are listed in this section. However, the primary focus of the description in this section is on the systems aspect of compliance. For information that is related primarily to functional requirements, references to other sections of this document are provided.

The scope of the sense and command features includes these systems:

- Safety information and control system.
- Protection system.
- Safety automation system.
- Priority and actuator control system.
- Incore instrumentation system.
- Excore instrumentation system.
- Boron concentration measurement system.
- Radiation monitoring system.
- Process instrumentation (refer to Section 7.2 and 7.3 for details).
- Signal conditioning and distribution system.

The execute features consist of:

- The trip breakers (part of the NUPS).
- The trip contactors (part of the CRDCS).
- Class 1E actuation devices (i.e., switchgear) (part of the Class 1E electrical distribution systems).
- Actuated equipment (part of the process systems).

7.1.2.6.1 Design Basis: Design Basis Events and Corresponding Protective Actions (Clauses 4.a and 4.b)

Compliance to Clauses 4.a and 4.b is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.2 Design Basis: Permissive Conditions (Clause 4.c)

Compliance to Clause 4.c is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.3 Design Basis: Monitored Variables (Clause 4.d)

~~Compliance to Clause 4.d is described in Section 7.2.2 and Section 7.3.2~~The variables used to initiate protective actions monitored by the protection system are described in Section 7.2.2 and Section 7.3.2.

The sensor response times and protection system cycle times required to accommodate the rates of change of monitored variables listed in Tables 15.0-7 and 15.0-8. For the design basis events requiring protective action, the accident analysis models the rates of change of variables monitored by the protection system from the occurrence of the accident to where the plant has reached a controlled state following protection system actions. Relative to the design basis for the protection system, the rates of change of these variables are included to determine that the sensor response time and input sampling rate of the protection system are adequate to detect and mitigate the event. The response times assumed in the accident analysis include sensor response times and worst case input sampling rate (i.e., input to the protection system changes just after the beginning of a clock cycle and is not seen until the beginning of the next clock cycle).

7.1.2.6.4 Design Basis: Manual Actions (Clause 4.e)

Manual actions credited in the accident analysis are described in Section 15.0. The protective actions and variables used to initiate those actions are described in Section 7.2.2 and Section 7.3.2. Manual actions are executed by the operators from the MCR. The MCR air conditioning regulates the environmental conditions in the MCR to provide an adequate environment for operator actions during normal, abnormal, and accident conditions. The MCR air conditioning system is described in Section 9.4.1. The radiological analysis of the MCR during accident conditions is provided in Section 15.0.3.

7.1.2.6.5 Design Basis: Spatially Dependent Variables (Clause 4.f)

Compliance to Clause 4.f is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.6 Design Basis: Range of Operating Conditions (Clause 4.g)

The safety systems are qualified in accordance with the program described in Section 3.11. This qualification includes:

- Environmental effects (e.g., temperature and humidity).
- Seismic effects.

- EMI/RFI effects.

The safety systems are powered by Class 1E power supplies, including the EUPS and Class 1E power supply system (EPSS). The safety systems are designed to remain functional within the range of voltage and frequency provided. The EPSS and EUPS are described in Section 8.3.

7.1.2.6.7 Design Basis: Protection Against Natural Phenomena and Unusual Events (Clause 4.h)

The safety systems are designed to perform their required functions in the presence of natural phenomena and unusual events, which include seismic events, tornadoes, and internal flooding. Refer to Chapter 3 for further information on these events. This is accomplished through the principles of independence described in Section 7.1.1 and equipment qualification described in Section 3.11.

7.1.2.6.8 Design Basis: Reliability Methods (Clause 4.i)

Two methods are used to evaluate the reliability of the safety systems. A FMEA is performed for the PS, and provides a qualitative means of evaluating the reliability of the system.

The probabilistic risk assessment (PRA) is used as a quantitative means for performing reliability analysis. The PRA is described in Chapter 19.

7.1.2.6.9 Design Basis: Critical Points in Time or Plant Conditions (Clause 4.j)

Compliance to Clause 4.j is described in Section 7.2.2 and Section 7.3.2.

7.1.2.6.10 Design Basis: Equipment Protection Provisions (Clause 4.k)

The I&C systems provide the capability to implement equipment protection of the safety process systems. Equipment protection can be implemented as an operational I&C function or a safety I&C function. The categorization is derived from process system requirements. Safety I&C functions have priority over operational I&C functions as described in Section 7.1.1.6. Refer to Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10, and Chapter 11 for descriptions of the process systems.

The U.S. EPR contains equipment protective functions that may prevent a piece of safety equipment from performing its function. If a piece of safety equipment is prevented from performing its function by an equipment protective function, then a single failure has occurred. This scenario is functionally equivalent to that piece of equipment failing to perform its safety function due to any number of failure mechanisms. 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. Therefore, no single equipment protective function can prevent performance of a safety function.

7.1.2.6.11 Design Basis: Special Design Basis (Clause 4.l)

07.01-26

A software CCF of the PS concurrent with an AOO or PA design basis event is considered in the design. The D3 principles described in Section 7.1.1.6 provide sufficient means to mitigate this software CCF. Section 7.8 describes the D3 assessment.

7.1.2.6.12 Single Failure Criterion (Clause 5.1)

The safety systems meet the requirements of Clause 5.1 of IEEE Std 603-1998 (Reference 1).

The safety systems are arranged in four independent divisions, located in four physically separated Safeguards Buildings. The PS acquires redundant sensors and generally implements 2/4 voting logic to accommodate single failures. This approach also prevents a single failure from resulting in a spurious actuation of process safety-related systems.

Independence is provided so that the redundancy of the safety systems is not defeated due to a single failure. The independence measures provided are described in Section 7.1.1.6.4.

A FMEA for the protective functions executed by the PS is described in Section 7.2.2 and Section 7.3.2. Demonstration of the single failure criterion for the execute features is provided with the description of the process systems in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10, and Chapter 11.

7.1.2.6.13 Completion of Protective Action (Clauses 5.2 and 7.3)

The safety systems meet the requirements of Clause 5.2 of IEEE Std 603-1998 (Reference 1). When initiated by a safety system, protective actions proceed to completion. Return to normal operation requires deliberate operator intervention.

Once opened by the PS, the reactor trip breakers remain open until the reactor trip signal has cleared and they are able to be manually closed. The reactor trip signal is only cleared when the initiating plant variable returns to within an acceptable range.

Refer to Section 7.3.2.3 for a description of completion of protection action for ESF actuation functions.

The execute features within the U.S. EPR are designed so that once initiated, the protective actions continue until completion, in accordance with IEEE 603-1998, Clause 7.3.

7.1.2.6.14 Quality (Clause 5.3)

The safety systems meet the requirements of Clause 5.3 of IEEE Std 603-1998 (Reference 1). The safety systems are within the scope of the U.S. EPR quality assurance program (QAP) described in Section 17.5. The TXS hardware quality is described in EMF-2110(NP)(A) (Reference 3).

The digital safety systems meet the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18). This guidance addresses software quality processes for the use of digital technology in safety systems.

TXS system software is developed in accordance with the processes described in EMF-2110 (NP)(A) (Reference 3).

The application software of the digital safety systems conform to the guidance of IEEE Std 7-4.3.2-2003 (Reference 18), with these exceptions:

- Alternate V&V methods are used. These methods are described and justified in ANP-10272 (Reference 5).
- A configuration control board is not used. The justification for this approach is provided in ANP-10272 (Reference 5).

The application software is developed in accordance with the software development and V&V processes that are summarized in Section 7.1.1.2 and described in detail in ANP-10272 (Reference 5). These processes provide an acceptable method of software development to meet the quality requirements of IEEE Std 603-1998 (Reference 1).

7.1.2.6.15 Equipment Qualification (Clause 5.4)

The safety systems shall meet the requirements of Clause 5.4 of IEEE Std 603-1998 (Reference 1). The equipment used shall be qualified using appropriate methods under the program described in Section 3.11.

The digital safety systems meet the additional guidance of IEEE Std 7-4.3.2 (Reference 18). Integrated system testing (including factory acceptance testing and site acceptance testing) is performed as part of the TXS development process described in Section 7.1.1.2 to verify that the performance requirements of the safety functions have been met.

7.1.2.6.16 System Integrity (Clause 5.5)

The safety systems meet the requirements of Clause 5.5 of IEEE Std 603-1998 (Reference 1), and the guidance of Clause 5.5 of IEEE Std 7-4.3.2-2003 (Reference 18).

The systems are designed to perform their functions as described in the design basis. Equipment qualification is performed so that the safety systems perform their function under the range of conditions required for operation. The ~~SICS,~~ PS, SAS, SCDS, and PACS are implemented in four divisions located in physically separated Safeguards~~s~~ Buildings with electrical and communications independence measures.

07.01-26

The PS implements a fail-safe design. The reactor trip breakers are de-energized to trip, so that a reactor trip occurs on a loss of power. ESF actuations are energized to actuate, so a loss of power results in a fail as-is condition.

For digital safety systems, these provide for system integrity:

- Design for computer integrity.
- Design for test and calibration.
- Fault detection and diagnostics.

The processing principles of the TXS platform described in Section 7.1.1.2 provide for real-time, deterministic operation of the safety systems. The processing is independent of changes in process variable and other external effects.

The TXS platform is designed for in-service testing and calibration, as well as inherent fault detection and diagnostics. These include features such as message error checks and a watchdog timer circuit. Refer to IEEE Std 603-1998 (Reference 1) for further information.

7.1.2.6.17 Independence (Clause 5.6)

The safety systems ~~meet~~satisfies the independence requirements of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2 (Reference 18) as described in the alternative request in Reference 45.

The features that provide for independence are described in Section 7.1.1.6.4.

7.1.2.6.18 Capability for Testing and Calibration (Clause 5.7)

The safety systems meet the requirements of Clause 5.7 of IEEE Std 603-1998 (Reference 1). Refer to Section 7.2.2 and Section 7.3.2 for information regarding the capability for testing and calibration.

7.1.2.6.19 Information Displays (Clause 5.8)

The safety systems meet the requirements of Clause 5.8 of IEEE Std 603-1998 (Reference 1). Displays and control are provided by the SICS for those manual actions described in Section 15.0. The displays meet the requirements of IEEE Std 497-2002 (Reference 13). Refer to Section 7.5 for further information.

The safety systems provide to the PICS their bypassed and inoperable status. This allows the operator to identify the specific bypassed functions and determine the state of actuation logic.

The arrangement of displays and controls shall be determined using the HFE principles described in Chapter 18.

7.1.2.6.20 Control of Access (Clause 5.9)

07.01-26

The safety systems meet the requirements of Clause 5.9 of IEEE Std 603-1998 (Reference 1).

Access to the cabinets of the SICS, PS, SAS, SCDS, and PACS are provided via doors that are normally closed and locked. Door positions are monitored, allowing operators the ability to investigate unexpected opening of cabinet doors. Cabinets are also located in physically separate equipment rooms within the four Safeguards Buildings and can only be accessed by authorized personnel.

Access to software of the digital safety systems is limited to the SU. The SU and the safety systems have multiple features to control access and prevent unauthorized changes to software including:

- Authorized personnel may only access the SU.
- Access to the SU is password protected.
- Access is provided to the safety computers via the MSI.
- The Class 1E MSI, which serves as a communication isolation point between a division of PS or SAS and the SU, prevents unauthorized communication from entering the division and affecting the safety processors.

The computer terminals for the SUs are located in the I&C service center (I&C SC). Additional control of access measures are provided in Reference 3.

The SICS equipment is located in the MCR and RSS. Both rooms are controlled security areas. Refer to Section 7.1.1 for a description of access controls for the QDS.

7.1.2.6.21 Repair (Clause 5.10)

The safety systems meet the requirements of Clause 5.10 of IEEE Std 603-1998 (Reference 1).

Safety systems built upon the TXS platform contain self-diagnostic test features to detect both hardware and software faults and assist in diagnostic and repair activities. Details on the self-test diagnostic capabilities are provided in EMF-2110(NP)(A) (Reference 3).

7.1.2.6.22 Identification (Clause 5.11)

The safety systems meet the identification requirements of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18).

Redundant divisions of each safety system are distinctively marked. Equipment within a cabinet that belongs to the same train as the cabinet marking does not contain additional identification. However, equipment within a cabinet that is not the same train as the cabinet marking is marked to show its different train assignment. Equipment within the safety system cabinets that is too small to carry an identification plate are housed in larger equipment clearly marked as part of a single redundant division of that safety system. Versions of hardware are marked accordingly. Configuration management is used for maintaining identification of safety-related software.

7.1.2.6.23 Auxiliary Features (Clause 5.12)

The safety systems meet the requirements of Clause 5.12 of IEEE Std 603-1998 (Reference 1).

The safety systems include the scope of auxiliary supporting features, which are described in Chapter 8 and Chapter 9. These systems include EUPS, EPSS, and safety-related HVAC systems throughout the plant.

Other auxiliary features that are not required to be operable for the safety systems to perform their functions (e.g., SU) are designed to meet criteria that does not degrade the safety functionality of the safety systems below an acceptable level.

7.1.2.6.24 Multi-Unit Stations (Clause 5.13)

The safety systems meet the requirements of Clause 5.13 of IEEE Std 603-1998 (Reference 1).

The U.S. EPR is designed as a single-unit plant. If multiple units are constructed at the same site, safety systems are not shared between units.

7.1.2.6.25 Human Factors Considerations (Clause 5.14)

The safety systems meet the requirements of Clause 5.14 of IEEE Std 603-1998 (Reference 1).

Human factors are considered throughout the design of the safety systems in accordance with the HFE principles described in Chapter 18.

7.1.2.6.26 Reliability (Clause 5.15)

The safety systems meet the reliability requirements of IEEE Std 603-1998 (Reference 1) and the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 18).

The safety systems are designed to accomplish their safety functions in a reliable manner to support overall plant availability. High reliability is provided through various features, including:

- Highly redundant architecture.
- Reliable equipment.
- Independent subsystems within each division of the PS to implement functional diversity.
- Continuous online fault detection and accommodation abilities.
- High quality software design process.
- Strong operating experience of the TXS platform.

The safety systems (including software) are analyzed as part of the probabilistic risk assessment, which is described in Chapter 19.

7.1.2.6.27 Common Cause Failure Criteria (Clause 5.16)

The safety systems meet the requirements of Clause 5.16 of IEEE Std 603-1998 (Reference 1).

The U.S. EPR architecture is designed so that plant parameters are maintained within acceptable limits established for each DBE in the presence of a single, credible common cause failure. The defense-in-depth and diversity principles that minimize the probability of a CCF and mitigate the consequences of a CCF are described in ANP-10304 (Reference 8).

7.1.2.6.28 Automatic Control (Clauses 6.1 and 7.1)

The safety systems meet the requirements of Clauses 6.1 and 7.1 of IEEE Std 603-1998 (Reference 1).

The various Level 0 systems provide signals representing the state of the process systems to the Level 1 safety systems.

The PS is designed to automatically initiate reactor trip and actuate the ESF systems necessary to mitigate the effects of DBEs. The PS automatically initiates appropriate safety functions whenever a measured variable exceeds a predefined setpoint.

The SAS is designed to perform ESF control functions and automated safety-related closed loop control functions once the safety-related process systems have been initiated by the PS.

The PACS is designed to automatically prioritize signals issued to safety-related actuators and monitor drive and actuator status for the execute features. The priority principles are described in Section 7.1.1.6.5.

The execute features within the U.S. EPR receive and act upon automatic control signals from the safety systems. Reactor trip output signals from the PS result in an opening of the reactor trip devices. Output signals for ESF actuation from the PS are sent to the PACS. The ESF control signals from the SAS are also sent to the PACS. The PACS prioritizes the signals from the PS and SAS and produces an output signal to the execute features.

7.1.2.6.29 Manual Control (Clauses 6.2 and 7.2)

The safety systems meet the requirements of Clauses 6.2 and 7.2 of IEEE Std 603-1998 (Reference 1).

Manual actuation of protective actions is possible from the SICS. The means provided minimize the amount of discrete operator manipulations, and depend on a minimum of equipment. Refer to Section 7.2 and Section 7.3 for the methods provided to initiate these functions.

Controls and indications are provided for those manual actions credited in the accident analyses described in Section 15.0. The controls are described in Section 7.2, Section 7.3, and Section 7.4. Type A variables are selected using the process described in Section 7.5.

The SICS provides the means to achieve and maintain safe shutdown following a DBE. This capability is provided through appropriate controls and indications. Refer to Section 7.4 and Section 7.5 for further information safe shutdown.

The execute features within the U.S. EPR are capable of receiving and acting upon manual control signals from the sense and command features. Manual control of equipment within the execute features is provided by the SICS and the PICS. Manual control of the execute features has a lower priority than the automatic actuation and control signals from the PS and SAS, consistent with the priority rules provided in Section 7.1.1.6.5.

7.1.2.6.30 Interaction between the Sense and Command Features and Other Systems (Clause 6.3)

The safety systems meet the requirements of Clause 6.3 of IEEE Std 603-1998 (Reference 1).

Sensors are shared between the safety and non-safety I&C systems for the execution of different functions (e.g., control, protection, diverse actuation, etc.). The sharing of sensors minimizes the amount of penetrations required in the various components in the RCS. This reduces the probability of small breaks in the RCPB and also reduces the amount of required piping.

These measures are provided that minimize the impact of a single, credible failure:

- The control systems (PAS, RCSL) are implemented using redundant controllers.
- The control systems (PAS, RCSL) implement signal selection algorithms that accommodate a single sensor failure. Refer to Section 7.7 for more information.
- The PS and SAS are implemented in four, independent divisions.
- The PS generally implements 2/4 voting. A single failed sensor does not result in a spurious action of safety-related equipment. Refer to Section 7.2 and Section 7.3 for more information.

07.01-26

- ~~The SAS implements signal selection algorithms for critical control loops that accommodate a single sensor failure. Refer to Section 7.3 for more information.~~
- The DAS generally implements 2/4 voting. A single failed sensor does not result in a spurious action of the safety-related equipment.
- Independence between the safety-related and non-safety-related systems. The independence measures provided are described in Section 7.1.1.6.4.

7.1.2.6.31 Derivation of System Inputs (Clause 6.4)

The safety systems meet the requirements of Clause 6.4 of IEEE Std 603-1998 (Reference 1).

The signals used in the sense and command features are direct measures of the desired variable in the design basis. The variables used for the inputs to the PS are described in Section 7.2 and Section 7.3.

The U.S. EPR implements an evolutionary means of reactor protection by acquiring a three-dimensional measurement of reactor flux through the use of safety-related SPNDs. The SPNDs provide the inputs to the high linear power density (HLPD) reactor trip and low departure from nucleate boiling ratio (DNBR) reactor trip described in Section 7.2. The use of actual incore parameters in protection functions reduces the uncertainty associated with previous methods.

7.1.2.6.32 Capability for Testing and Calibration (Clause 6.5)

The safety systems meet the requirements of Clause 6.5 of IEEE Std 603-1998 (Reference 1).

Sensors are tested at intervals described in Chapter 16. The methods of testing include:

- Perturbing the monitored variable.
- Providing a substitute input to the sensor (e.g., calibrated source for a pressure sensor).
- Cross checking channels that have known relationships.

Operational availability during an accident may be verified using one of the above methods, or by specifying the time period it retains its calibration.

7.1.2.6.33 Operating Bypass (Clauses 6.6 and 7.4)

The safety systems meet the requirements of Clause 6.6 and 7.4 of IEEE Std 603-1998 (Reference 1).

Operating bypasses are implemented using permissive signals from the PS. If the plant conditions associated with allowing operational bypasses are not met, the PS automatically prevents the activation of the operating bypass.

When an operating bypass is in effect, indication of this condition is provided to the MCR. If plant conditions change during activation of an operating bypass, and the operating bypass is no longer permissible, in general the PS automatically removes the appropriate active operating bypass.

Low temperature overpressure protection (LTOP) of the RCS is normally bypassed using P17 when at power. During shutdown operations, LTOP protection is enabled when P17 is manually validated by the operator once the conditions for P17 are satisfied. This is a controlled evolution governed by plant operating procedures. This is consistent with the guidance provided in BTP 5-2 (Reference 38), industry precedent, and meets the intent of Clause 6.6 of IEEE Std 603-1998 (Reference 1). Refer to Section 5.2 for more information about LTOP.

Refer to Section 7.2 and Section 7.3 for further information on permissives and the operating bypasses of the protective functions.

7.1.2.6.34 Maintenance Bypass (Clauses 6.7 and 7.5)

The safety systems meet the requirements of Clause 6.7 of IEEE Std 603-1998 (Reference 1).

The safety systems are designed to permit channel bypass for maintenance, testing, or repair. Individual function computers of the SICS, PS, and SAS can be placed into testing and diagnostic modes via the SU. The function computer being tested automatically changes its outputs to the associated I/O modules to test status, and communication from the unit under test is disregarded by the remainder of the system. This bypass is accomplished during power operation without causing initiation of a protective function. During maintenance bypass, the single failure criterion is still met, or acceptable reliability is demonstrated.

Sufficient redundancy and administrative controls that manage reduction of redundancy exist within each system to maintain acceptable reliability when a portion of the execute features is placed in bypass, in accordance with IEEE 603-1998, Clause 7.5.

7.1.2.6.35 Sense and Command Features: Setpoints (Clause 6.8)

The safety systems meet the requirements of Clause 6.8 of IEEE Std 603-1998 (Reference 1).

Allowance for uncertainties between the process analytical limit and the setpoint used in the protective functions of the PS is determined using a documented methodology. The U.S. EPR setpoint methodology is described in ANP-10275P (Reference 14). The methodology establishes that setpoints used within the PS are determined so that plant safety limits are not exceeded. The single-sided measurement uncertainty reduction factor shall not be used in determining U.S. EPR setpoints.

Where multiple setpoints are used for adequate protection under different plant conditions, the more restrictive setpoint is used when required. The logic that detects the need to change setpoints is part of the PS. Refer to Section 7.2 and Section 7.3 for functions that use multiple setpoints.

7.1.2.6.36 Electrical Power Sources (Clause 8.1)

The safety systems meet the requirements of Clause 8.1 of IEEE Std 603-1998 (Reference 1).

The safety systems are powered by the EUPS and EPSS. These systems provide reliable, Class 1E power that is backed by the EDGs. The EUPS provides uninterruptible power in case of a LOOP. Refer to Section 8.3 for information regarding the EUPS and EPSS.

7.1.2.6.37 Non-Electrical Power Sources (Clause 8.2)

The safety systems do not rely on non-electrical power sources for operation. The requirements for actuated equipment that utilize non-electrical power sources (e.g., compressed gas or media actuated valves) are described within the process system descriptions.

7.1.2.6.38 Maintenance Bypass (Clause 8.3)

The safety systems can perform their safety functions while power sources are in maintenance bypass. Details on the electrical power systems that fulfill this requirement are described in Chapter 8.

7.1.3 References

1. IEEE Std 603-1998, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,"1998.

2. IEEE Std 603-1991, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations,"1991.

3. EMF-2110(NP)(A), Revision 1, "TELEPERM XS: A Digital Reactor Protection System," Siemens Power Corporation, July 2000.

4. ANP-10273P, Revision 0, "AV42 Priority Actuation and Control Module Topical Report," AREVA NP Inc., November 2006.

5. ANP-10272, Revision 2, "Software Program Manual TELEPERM XS™ Safety Systems Topical Report," AREVA NP Inc., May 2010.

07.01-26

6. ANP-10309P, Revision ~~0~~1, "U.S. EPR Digital Protection System Technical Report," AREVA NP Inc., ~~November 2009~~March 2011.

7. ANP-10287P, Revision 0, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," AREVA NP Inc., November 2007.

8. ANP-10304, Revision ~~1~~2, "U.S. EPR Diversity and Defense-In-Depth Assessment Technical Report," AREVA NP Inc., ~~December 2009~~March 2011.

9. NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems," U.S. Nuclear Regulatory Commission, December 1994.

10. SRM to SECY 93-087 II.Q, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems," United States Nuclear Regulatory Commission, Office of Nuclear Reactor Regulation, 1993.

11. IEEE Std 379-2000, "IEEE Standard Application of the Single-Failure Criterion to Nuclear Power Generating Station Safety Systems," 2000.

12. IEEE Std 384-1992, "IEEE Standard Criteria for Independence of Class 1E Equipment and Circuits," 1992.

13. IEEE Std 497-2002, "IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations," 2002.

14. ANP-10275P, Revision 0, "U.S. EPR Instrument Setpoint Methodology Topical Report," AREVA NP Inc., March 2007.

15. ANSI/ISA-67.04.01-2006, "Setpoints for Nuclear Safety Related Instrumentation," 2006.

16. IEEE Std 338-1987, "IEEE Standard Criteria for the Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems," 1987.

17. ISA-67.02-1980, "Nuclear-Safety-Related Instrument Sensing Line Piping and Tubing Standards for Use in Nuclear Power Plants," 1980.

18. IEEE 7-4.3.2-2003, "IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations," 2003.

19. IEEE 1050-1996, "IEEE Guide for Instrumentation and Control Equipment Grounding in Generating Stations," 1996.

20. IEEE Std C62.23-1995, "IEEE Application Guide for Surge Protection of Electric Generating Plants," 1995.

21. IEEE Std 323-2003, "IEEE Standard for Qualifying Class 1E Equipment for Nuclear Power Generating Stations," 2003.

22. BTP 7-1, "Guidance on Isolation of Low-Pressure Systems from the High Pressure Reactor Coolant System," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

23. BTP 7-2, "Guidance on Requirements of Motor-Operated Valves in the Emergency Core Cooling System Accumulator Lines," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

24. BTP 7-3, "Guidance on Protection System Trip Point Changes for Operation with Reactor Coolant Pumps Out of Service," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

25. BTP 7-4, "Guidance on Design Criteria for Auxiliary Feedwater Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

26. BTP 7-5, "Guidance on Spurious Withdrawals of Single Control Rods in Pressurized Water Reactors," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

27. BTP 7-8, "Guidance for Application of Regulatory Guide 1.22," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

28. BTP 7-9, "Guidance on Requirements for Reactor Protection System Anticipatory Trips," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

29. BTP 7-10, "Guidance on Application of Regulatory Guide 1.97," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

30. BTP 7-11, "Guidance on Application and Qualification of Isolation Devices," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

31. BTP 7-12, "Guidance on Establishing and Maintaining Instrument Setpoints," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

32. BTP 7-13, "Guidance on Cross-Calibration of Protection System Resistance Temperature Detectors," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

33. BTP 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

34. BTP 7-17, "Guidance on Self-Test and Surveillance Test Provisions," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

35. BTP 7-18, "Guidance on the Use of Programmable Logic Controllers in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

36. BTP 7-19, "Guidance for Evaluation of Diversity and Defense-In-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

37. BTP 7-21, "Guidance on Digital Computer Real-Time Performance," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

38. BTP 5-2, "Overpressurization Protection of Pressurized-Water Reactors While Operating at Low Temperatures," U.S. Nuclear Regulatory Commission, Standard Review Plan, Branch Technical Position, Rev. 3, March 2007.

39. EMF-2341(P), Revision 1, "Generic Strategy for Periodic Surveillance Testing of TELEPERM[TM] XS Systems in U.S. Nuclear Generating Stations," Siemens Power Corporation, March 2000.

40. EPRI TR-106439, "Guidance on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications," Electric Power Research Institute, October 1996.

07.01-26

41. Deleted.ISA-TR67.04.09-2005, "Graded Approaches to Setpoint Determination," The Instrumentation, Systems, and Automation Society, October 2005.

42. ANP-10266A, Revision 12, "AREVA NP Inc. Quality Assurance Plan (QAP) for Design Certification of the U.S. EPR Topical Report," AREVA NP Inc., April 2007December 2008.

43. Generic Letter 85-06, "Quality Assurance Guidance for ATWS Equipment that is Not Safety-Related," U.S. Nuclear Regulatory Commission, April 16, 1985.

44. ANP-10310P, Revision 1, "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report," AREVA NP Inc., March 2011.

45. Letter, Sandra Sloan (AREVA NP Inc.) to Document Control Desk (NRC), "Request for Alternatives to IEEE Std 603-1991 to Satisfy 10 CFR 50.55a(h) Requirements - U.S. EPR Design Certification," March 29, 2011.

07.01-26

Table 7.1-1—Levels of Redundancy in I&C Architecture

I&C System	Level of Redundancy
SICS	4
PICS	2
PS	4
SAS	4
PACS	4
~~SA I&C~~RCSL	~~4~~2 (Note 1)
~~RCSL~~PAS	2 (Note 2)
~~PAS~~DAS ~~(NIS, TIS, BPS)~~	~~2~~4
~~DAS~~SCDS	4

Notes:

~~1. SA I&C is implemented with four divisions of I&C. Plant severe accident mitigation features are implemented with varying levels of redundancy.~~

1. RCSL is a redundant control system, but acquires sensor inputs in all four divisions.

2. PAS uses redundant controllers in each division and train. Some functions in the NI utilize multiple divisions (e.g., pressurizer level control).

Next File

Table 7.1-2—I&C System Requirements Matrix (Sheet 1 of 9)

Applicable Regulations and Guidance	10 CFR 50											
	50.55a(a)(1)	50.55a(h)(2)	50.55a(h)(3)	50.34(f)(2)(v)	50.34(f)(2)(xi)	50.34(f)(2)(xii)	50.34(f)(2) (xiv)	50.34(f)(2) (xvii)	50.34(f)(2) (xviii)	50.34(f)(2) (xix)	50.34(f)(2) (xx)	50.62
07.01-26 Industry Standard		IEEE Std 603-1991 (1)(2)	IEEE Std 603-1991 (1)(2)									
Safety Information and Control System (S)	x	x	x	~~x~~	x	x		x	x	x	x	
Process Information and Control System (NS-AQ)				x	x	x		x	x	x		
Protection System (S)	x	x	x	x		x	x	~~x~~	x	~~x~~	x	
Safety Automation System (S)	x		x	x	~~x~~	~~x~~		~~x~~	~~x~~	~~x~~		
Priority and Actuator Control System (S)	x	x	x	x	x	x	x			~~x~~	x	x
~~Severe Accident I&C (NS)~~										~~x~~		
Reactor Control, Surveillance & Limitation System (NS)												
Process Automation System (NS)				x	x	x		x	x	x		~~x~~
Turbine Generator I&C (NS)												
Control Rod Drive Control System (NS)	x	x	x	x								
Incore Instrumentation System (S)	x	x	x	x					x	x		
Excore Instrumentation System (S)	x	x	x	x						x		
Boron Concentration Measurement System (S)	x	x	x	x						x		
Radiation Monitoring System (S)	x	x	x	x			x	x		x		
Hydrogen Monitoring System (S)	x		x	x				x		x		
Reactor Pressure Vessel Level Measurement System (NS-AQ)	x		x	x					x	x		
Seismic Monitoring System (NS)												
Loose Parts Monitoring System (NS)												
Vibration Monitoring System (NS)												
Fatigue Monitoring System (NS)												
Leak Detection System (NS)												
Signal Conditioning and Distribution System (S)	x	x	x	x		x	x	x	x	x	x	x
Diverse Actuation System (NS-AQ)												x

07.01-26

Table 7.1-2—I&C System Requirements Matrix
(Sheet 2 of 9)

Rod Position Measurement System (S)	x	x	x									

Notes on Tables 7.1–2; Sheet 2 of ~~7~~9:

1. With correction sheet dated January 30, 1995.
2. The U.S. EPR uses IEEE Std 603-1998, which meets or exceeds the requirements of IEEE Std 603-1991.

Table 7.1-2—I&C System Requirements Matrix (Sheet 3 of 9)

Applicable Regulations and Guidance 07.01-26	General Design Criteria											
	GDC 1	GDC 2	GDC 4	GDC 10	GDC 13	GDC 15	GDC 16	GDC 19	GDC 20	GDC 21	GDC 22	GDC 23
Industry Standard												
Safety Information and Control System (S)	x	x	x		x			x				
Process Information and Control System (NS-AQ)					x			x				
Protection System (S)	x	x	x	x	x	x	x	x	x	x	x	x
Safety Automation System (S)	x	x	x	x	x	~~x~~		~~x~~				
Priority and Actuator Control System (S)	x	x	x	x	x	x	x	x	x	x	x	x
~~Severe Accident I&C (NS)~~					~~x~~			~~x~~				
Reactor Control, Surveillance & Limitation System (NS)				x	x	x		~~x~~				
Process Automation System (NS)				x	x	x		x				
Turbine Generator I&C (NS)					x			x				
Control Rod Drive Control System (NS)	x	x	x	x	x			x				
Incore Instrumentation System (S)	x	x	x	x	x			x	x	x	x	x
Excore Instrumentation System (S)	x	x	x	x	x			x	x	x	x	x
Boron Concentration Measurement System (S)	x	x	x	x	x			x	x	x	x	x
Radiation Monitoring System (S)	x	x	x		x			x	x	x	x	x
Hydrogen Monitoring System (S)	x	x	x		x			x				
Reactor Pressure Vessel Level Measurement System (NS-AQ)	x	x	x		x			x				
Seismic Monitoring System (NS)		x			x			x				
Loose Parts Monitoring System (NS)					x			x				
Vibration Monitoring System (NS)					x			x				
Fatigue Monitoring System (NS)					x			x				
Leak Detection System (NS)		x			x			x				
Signal Conditioning and Distribution System (S)	x	x	x	x	x	x	x	x	x	x	x	x
Diverse Actuation System (NS-AQ)					x							
Rod Position Measurement System (S)	x	x	x	x	x			x	x	x	x	x
Notes:												

DRAFT

Table 7.1-2—I&C System Requirements Matrix
(Sheet 4 of 9)

07.01-26

Applicable Regulations and Guidance	General Design Criteria										SRM to SECY 93-087	
	GDC 24	GDC 25	GDC 28	GDC 29	GDC 33	GDC 34	GDC 35	GDC 38	GDC 41	GDC 44	II.Q	II.T
Industry Standard												
Safety Information and Control System (S)											x	x
Process Information and Control System (NS-AQ)											~~x~~	x
Protection System (S)	x	x	x	x	x	x	x	x	x	x	~~x~~	
Safety Automation System (S)					x	x	x	x		x	~~x~~	
Priority and Actuator Control System (S)	x	x			x	x	x	x	x	x	x	
~~Severe Accident I&C (NS)~~									~~x~~			
Reactor Control, Surveillance & Limitation System (NS)			x	x								
Process Automation System (NS)			x		~~x~~						~~x~~	
Turbine Generator I&C (NS)												
Control Rod Drive Control System (NS)			x	x								
Incore Instrumentation System (S)	x	x		x								
Excore Instrumentation System (S)	x	x		x								
Boron Concentration Measurement System (S)	x	x		x								
Radiation Monitoring System (S)	x	x		x								
Hydrogen Monitoring System (S)												
Reactor Pressure Vessel Level Measurement System (NS-AQ)												
Seismic Monitoring System (NS)												
Loose Parts Monitoring System (NS)												
Vibration Monitoring System (NS)												
Fatigue Monitoring System (NS)												
Leak Detection System (NS)												
Signal Conditioning and Distribution System (S)	x	x	x	x	x	x	x	x	x		x	
Diverse Actuation System (NS-AQ)											x	
Rod Position Measurement System (S)	x	x		x								

Notes:

**Table 7.1-2—I&C System Requirements Matrix
(Sheet 5 of 9)**

Applicable Regulations and Guidance	Regulatory Guides									
	1.22	1.47	1.53	1.62	1.75	1.97	1.105	1.118	1.151	1.152
Industry Standard 07.01-26			IEEE Std 379-2000		IEEE Std 384-1992	IEEE Std 497-2002	ISA-67.04-1994(1)	IEEE Std 338-1987	ISA-S67.02-1980	IEEE Std 7-4.3.2-2003
Safety Information and Control System (S)	x	~~x~~	x	x	x	x		x		x
Process Information and Control System (NS-AQ)		x				x				
Protection System (S)	x	x	x	x	x	x	x	x	x	x
Safety Automation System (S)		x	x		x	~~x~~				x
Priority and Actuator Control System (S)	x	x	x	x	x	x		x		
~~Severe Accident I&C (NS)~~										
Reactor Control, Surveillance & Limitation System (NS)									x	
Process Automation System (NS)		x				x			x	
Turbine Generator I&C (NS)										
Control Rod Drive Control System (NS)	x	x	x	x	x					
Incore Instrumentation System (S)	x	x	x		x	x				
Excore Instrumentation System (S)	x	x	x		x	x				
Boron Concentration Measurement System (S)	x	x	x		x	x				
Radiation Monitoring System (S)	x	x	x		x	x				
Hydrogen Monitoring System (S)		x	x		x	x			x	
Reactor Pressure Vessel Level Measurement System (NS-AQ)		x	x		x	x				
Seismic Monitoring System (NS)										
Loose Parts Monitoring System (NS)										
Vibration Monitoring System (NS)										
Fatigue Monitoring System (NS)										
Leak Detection System (NS)										
Signal Conditioning and Distribution System (S)	x	x	x		x	x		x	x	
Diverse Actuation System (NS-AQ)										

07.01-26

Table 7.1-2—I&C System Requirements Matrix (Sheet 6 of 9)

Rod Position Measurement System (S)	x	x	x		x	x				x

Notes: on Table 7.1–2; Sheet 5 of ~~7~~9

1. U.S. EPR follows ISA-67.04.01-2006.

Table 7.1-2—I&C System Requirements Matrix
(Sheet 7 of 9)

07.01-26

Applicable Regulations and Guidance	Regulatory Guides									
	1.168	1.169	1.170	1.171	1.172	1.173	1.180	1.189	1.204	1.209
Industry Standard	IEEE Std 1012-1998 IEEE Std 1028-1997	IEEE Std 828-1990 IEEE Std 1042-1987	IEEE Std 829- 1983	IEEE Std 1008-1987	IEEE Std 830- 1993	IEEE Std 1074-1995	Various Standards		IEEE Std 1050-1996	IEEE Std 323-2003
Safety Information and Control System (S)	x	x	x	x	x	x	x	x	x	x
Process Information and Control System (NS-AQ)								x		
Protection System (S)	x	x	x	x	x	x	x	x	x	x
Safety Automation System (S)	x	x	x	x	x	x	x	~~x~~	x	x
Priority and Actuator Control System (S)							x	x	x	
~~Severe Accident I&C (NS)~~										
Reactor Control, Surveillance & Limitation System (NS)										
Process Automation System (NS)								x		
Turbine Generator I&C (NS)										
Control Rod Drive Control System (NS)							x		x	
Incore Instrumentation System (S)							x		x	
Excore Instrumentation System (S)							x	x	x	
Boron Concentration Measurement System (S)							x		x	
Radiation Monitoring System (S)							x		x	
Hydrogen Monitoring System (S)							x		x	
Reactor Pressure Vessel Level Measurement System (NS-AQ)							x		x	
Seismic Monitoring System (NS)										
Loose Parts Monitoring System (NS)										
Vibration Monitoring System (NS)										
Fatigue Monitoring System (NS)										
Leak Detection System (NS)										
Signal Conditioning and Distribution System (S)							x	x	x	
Diverse Actuation System (NS-AQ)										

07.01-26

Table 7.1-2—I&C System Requirements Matrix
(Sheet 8 of 9)

Rod Position Measurement System (S)	x	x	x	x	x	x	x		x	x

Notes:

Table 7.1-2—I&C System Requirements Matrix
(Sheet 9 of 9)

07.01-26

Applicable Regulations and Guidance	Branch Technical Positions															
	7-1	7-2	7-3	7-4	7-5	7-8	7-9	7-10	7-11	7-12	7-13	7-14	7-17	7-18	7-19	7-21
Industry Standard																
Safety Information and Control System (S)		x				x		x	x			x		x	x	x
Process Information and Control System (NS-AQ)		x						x							~~x~~	
Protection System (S)	x	x	x	x	x	x	x	x	x	x	x	x	x	x	~~x~~	x
Safety Automation System (S)				~~x~~				~~x~~	x			x	x	x	~~x~~	x
Priority and Actuator Control System (S)	x	x		x		x		x	x				x		x	
~~Severe Accident I&C (NS)~~																
Reactor Control, Surveillance & Limitation System (NS)					x											
Process Automation System (NS)								x							~~x~~	
Turbine Generator I&C (NS)																
Control Rod Drive Control System (NS)					x				x							
Incore Instrumentation System (S)						x		x	x							
Excore Instrumentation System (S)						x		x	x							
Boron Concentration Measurement System (S)						x		x	x							
Radiation Monitoring System (S)						x		x	x							
Hydrogen Monitoring System (S)								x	x							
Reactor Pressure Vessel Level Measurement System (NS-AQ)								x	x							
Seismic Monitoring System (NS)																
Loose Parts Monitoring System (NS)																
Vibration Monitoring System (NS)																
Fatigue Monitoring System (NS)																
Leak Detection System (NS)																
Signal Conditioning and Distribution System (S)	x	x		x	x	x	x	x	x		x				x	
Diverse Actuation System (NS-AQ)															x	
Rod Position Measurement System (S)					x			x	x			x	x	x	x	x
Notes:																

DRAFT

Next File

07.01-26

Table 7.1-3—DCS Functional Requirements Allocation Matrix
Sheet 1 of 2

Functional Requirements	DCS Subsystem								
	SICS	PICS	DAS	PS	SAS	RCSL	PAS	SCDS	PACS
Process Control Functions									
Non-reactivity related		X					X	X	X
Reactivity related (with rods)		X				X		X	
Reactivity related (without rods)[1]		X				X	X	X	X
Process Limitation Functions									
Non-reactivity related		X					X	X	X
Reactivity related (with rods)		X				X		X	
Reactivity related (without rods)[1]		X				X	X	X	X
Reactor Trip	X			X				X	
ESF Actuation	X			X				X	X
Safety Controls									
Automatic[2]	X				X			X	X
Manual Grouped Control[3]	X	X			X		X		X
Manual Component Control[4]	X	X					X		X
Safety Interlocks[5, 6]	X			X	X			X	X
Severe Accident Controls[7]	X	X					X		X
Diverse Reactor Trip	X		X					X	
Diverse ESF Actuation	X		X					X	X
Process Indications[8]		X					X	X	X

07.01-26

Table 7.1-3—DCS Functional Requirements Allocation Matrix
Sheet 2 of 2

Functional Requirements	DCS Subsystem								
	SICS	PICS	DAS	PS	SAS	RCSL	PAS	SCDS	PACS
PAM Indications									
PAM Type A[9]	X	X					X	X	X
PAM Type B[9]	X	X					X	X	X
PAM Type C[9]	X	X					X	X	X
PAM Type D		X					X		
PAM Type E		X					X		
Severe Accident Indications[10]	X	X					X	X	X
Alarms[11]	X	X	X	X	X	X	X	X	

Notes:

1. Process control and limitation functions that are reactivity related and command actuators other than control rods (e.g., reactor boron water makeup) are allocated to RCSL and PAS. RCSL performs the bulk of the logic, and then sends the specific actuator command (i.e., open/close) to the PAS. This provides a common actuator interface from the PICS.

2. Safety automatic control functions are allocated to SICS if an operator interface is needed for the function (e.g., auto/manual transfer).

3. Safety-related manual grouped controls are allocated to two different paths, which are:

   – SICS -> SAS -> PACS (credited path).

   – PICS -> PAS -> PACS (duplicated path provide so the operator can perform these functions on PICS).

07.01-26

4. Safety-related manual component controls are allocated to two different paths, which are:
   - SICS -> PACS (credited path).
   - PICS -> PAS -> PACS (duplicated path provide so the operator can perform these functions on PICS).
5. Safety interlock functions are allocated to SICS if an operator interface is needed for the function (e.g., validating a permissive to enable an interlock).
6. The interlock is allocated to PS if it relies on a permissive that resides in the PS (e.g., P14 for RHR interlock). Otherwise, the interlock is allocated to SAS. This minimizes wiring between the PS and SAS.
7. Severe accident controls are allocated to two different paths, which are:
   - SICS -> PACS (credited path).
   - PICS -> PAS -> PACS (duplicated path provide so the operator can perform these functions on PICS).
8. Process indications are routed as follows:
   - PAS -> PICS (path used if the signal is needed only in PAS).
   - SCDS or PACS (for actuator feedback) -> PAS -> PICS -> (path used if the signal is needed in multiple DCS subsystems).
9. PAM Type A-C indications are allocated to two different paths, which are:
   - SCDS or PACS (for actuator feedback) -> SICS (credited path).
   - SCDS or PACS (for actuator feedback) -> PAS -> PICS (duplicated path provide so the operator can monitor these parameters on PICS).

10. Severe accident indications are allocated to two different paths, which are:

    – SCDS or PACS (for actuator feedback) -> SICS (credited path).

    – SCDS or PACS (for actuator feedback) -> PAS -> PICS (duplicated path provide so the operator can monitor these parameters on PICS).

11. The alarms are provided on PICS. These alarms are generated in the PS, SAS, RCSL, DAS (sent to PAS via HW link), or PAS. A limited number of alarms are provided on SICS. These alarms are generated in DAS, PS, or SAS.

07.01-26

Table 7.1-4—DCS Interface Matrix
Sheet 1 of 4

From	To	Type	Basis
SICS (MCR)	DAS	Hardwired	Manual diverse reactor trip, diverse ESF actuation, diverse ESF resets, diverse permissives
	PS	Hardwired	Manual reactor trip, ESF actuation, ESF resets, permissives
	SAS	Hardwired	Signals to interface with automatic functions (e.g., auto/manual switchover) and manual grouped commands for SAS functions
	PACS	Hardwired	Manual component level control commands, Operational I&C Disable
SICS (RSS)	DAS	Hardwired	MCR-RSS Transfer
	PS	Hardwired	Manual reactor trip, limited ESF resets, limited permissives, MCR-RSS Transfer
	SAS	Hardwired	MCR-RSS Transfer
	PACS	Hardwired	MCR-RSS Transfer
	PICS	Hardwired	MCR-RSS Transfer
PICS	RCSL	Data	Signals to interface with automatic functions (e.g., auto/manual switchover), manual grouped commands for RCSL functions, manual controls for individual rods
	TG I&C	Data	Manual commands related to Turbine Generator operation
	PAS	Data	Signals to interface with automatic functions, manual grouped commands, manual component control commands
	Plant Business Networks	Data	Information to transfer to plant business networks for use by plant staff.

07.01-26

**Table 7.1-4—DCS Interface Matrix
Sheet 2 of 4**

From	To	Type	Basis
DAS	SICS	Hardwired	Provide information to SICS regarding DAS operation (e.g., DAS reactor trip initiated)
	PAS	Hardwired	Provide DAS information to PAS for display on PICS, provide signals to PAS to coordinate logic on diverse reactor trip or ESF actuation
	RTB	Hardwired	Diverse reactor trip signal
	CRDCS	Hardwired	Diverse reactor trip signal
	TG I&C	Hardwired	Diverse turbine trip signal
	PACS	Hardwired	Diverse ESF actuation signals
PS	SICS	Hardwired	Provide information to SICS regarding PS operation (e.g., PS reactor trip initiated)
	SICS	Data	Provide information to QDS for graphical display and trends
	PICS	Data	Provide information to PICS regarding PS operation (e.g., PS reactor trip initiated)
	SAS	Hardwired	Initiate ESF controls following ESF actuation
	PAS	Hardwired	Provide signals to PAS to coordinate logic on reactor trip or ESF actuation
	RTB	Hardwired	Reactor trip signal
	CRDCS	Hardwired	Reactor trip signal
	TG I&C	Hardwired	Turbine trip signal
	PACS	Hardwired	ESF actuation signals

07.01-26

Table 7.1-4—DCS Interface Matrix
Sheet 3 of 4

From	To	Type	Basis
SAS	SICS	Hardwired	Provide information to SICS regarding SAS operation (e.g., PS reactor trip initiated)
	PICS	Data	Provide information to PICS regarding SAS operation (e.g., PS reactor trip initiated)
	PAS	Hardwired	Provide for coordination of logic between SAS and PAS (if needed)
	PACS	Hardwired	Safety control signals
RCSL	PICS	Data	Provide information to PICS regarding RCSL operation (e.g., ACT control mode)
	PAS	Hardwired	Provide command signals for actuators used in RCSL functions other than control rods (e.g., RBMWS components for Boron control)
	CRDCS	Hardwired	Actuation commands for control rods
	TG I&C	Hardwired	Turbine actuation signals related to reactivity control and limitation functions
PAS	PICS	Data	Provide process and safety indications to PICS, provide information to PICS regarding PAS operation (e.g., auto/manual status, etc)
	PACS	Data	Actuator commands
	Actuators/ Black Boxes	Hardwired	Actuator commands
	TG I&C	Hardwired	TG I&C actuation commands
SCDS	SICS	Hardwired	Distribute DCS input signals to SICS
	DAS	Hardwired	Distribute DCS input signals to DAS
	PS	Hardwired	Distribute DCS input signals to PS

07.01-26

Table 7.1-4—DCS Interface Matrix
Sheet 4 of 4

From	To	Type	Basis
SCDS (cont)	SAS	Hardwired	Distribute DCS input signals to SAS
	RCSL	Hardwired	Distribute DCS input signals to RCSL
	PAS	Hardwired	Distribute DCS input signals to PAS
PACS	SICS	Hardwired	Actuator checkbacks
	SAS	Hardwired	Actuator checkbacks
	PAS	Data	Actuator checkbacks
Sensors/ Black Boxes	SCDS	Hardwired	Send signals to the DCS for distribution to multiple DCS subsystems
	PAS	Hardwired	Send non-safety related signals to the DCS if only needed in PAS
Actuators/ Black Boxes	PACS	Hardwired	Actuator checkbacks
	PAS	Hardwired	Actuator checkbacks
CRDCS	RCSL	Hardwired	Control rod checkbacks
TG I&C	RCSL	Hardwired	Turbine generator information needed in RCSL functions (e.g., 1st stage pressure)
	PAS	Hardwired	Turbine generator information needed in PAS functions
	PICS	Data	Indications and actuator checkbacks for equipment controlled by TG I&C

Notes:

1. Table 7.1-3 shows the major internal and external DCS interfaces needed for monitoring and control of the plant. Additional interfaces may be necessary, such as those interfaces that are necessary to implement testing, bypassed and

07.01-26

inoperable status, data storage (time stamping) requirements. Additional interfaces not defined in Table 7.1-3 that are needed to fulfill requirements shall be implemented using the following rules:

- The interfaces are hardwired.
- The interfaces between safety and non-safety systems will be implemented using qualified electrical isolation devices in accordance with the applicable regulatory requirements and codes and standards.

2. Each entry in the DCS interface matrix shows interfaces in a unidirectional fashion, even though interfaces may be bidirectional. For example, Figure 7.1-2 shows bidirectional hardwired connections between PS and SICS. Table 7.1-4 shows two entries for this, one for the interface from SICS to PS, and one for the interface from PS to SICS.

Next File

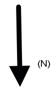
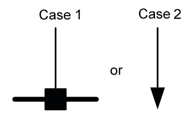
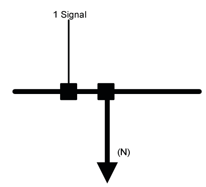
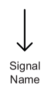
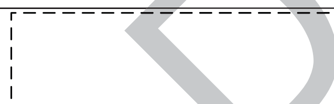
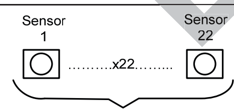
Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 1 of 16

Symbols – Logic Figures	Definition
Deleted	
Deleted	
Deleted	
Deleted	
Deleted	
Deleted	
Deleted	
Deleted	
Deleted	
Deleted	
	Sensor Measurement Signal
Deleted	
Deleted	
Deleted	

07.01-26

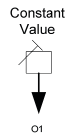
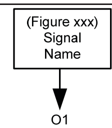
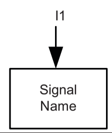
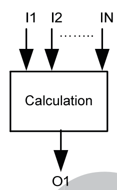
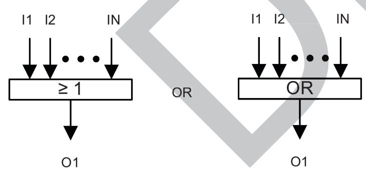
REV 003
EPR3000-I T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 2 of 16

Symbols – Logic Figures	Definition
	Multiple Signals of the Same Type
	Single Signal (2 Cases)
	Signal Transfer Between Divisions
	Signal Sent Elsewhere in Figure
	Signal Received from Elsewhere in Figure
	The logic within the block is duplicated in other divisions of the system.
	Multiple instances of the same type of object. Multiple sensors are given as an example. This convention is also applied to signal arrows and calculation boxes.

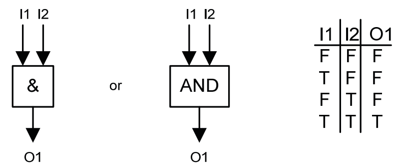
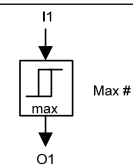
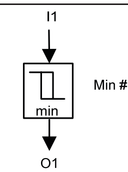
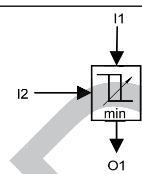
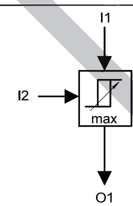
REV 003
EPR3000-2 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 3 of 16

Symbols – Logic Figures	Definition
	Constant Value Generator
	Signal Generated in Another Figure
	Result of Logic or Signal Sent to Another Figure
	"Black Box" Calculation
	OR Function

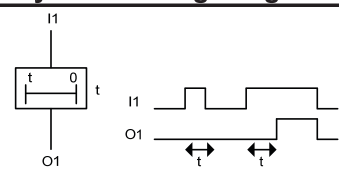
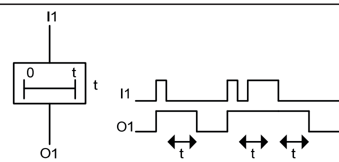
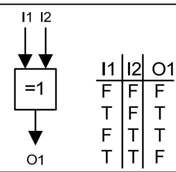
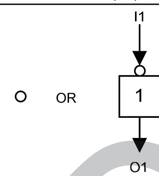
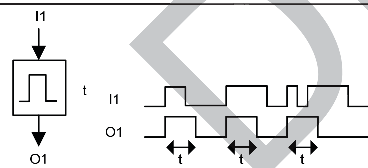
EPR3000-3 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 4 of 16

Symbols – Logic Figures	Definition
	AND Function
	High Threshold
	Low Threshold
	Low Variable Threshold
	High Variable Threshold

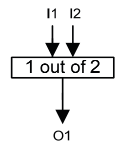
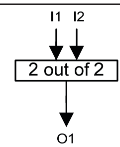
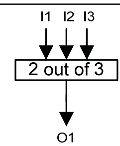
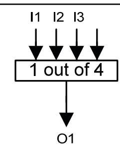
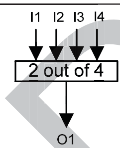
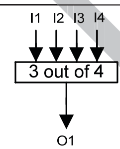
EPR3000-4 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 5 of 16

Symbols – Logic Figures	Definition
	On Time Delay
	Off Time Delay
	XOR Function
	Logic Inversion
	Pulse Function

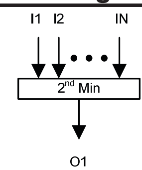
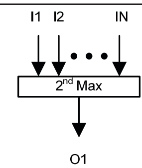
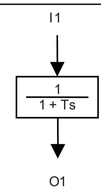
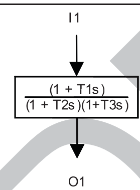
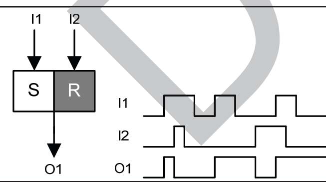
EPR3000-5 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 6 of 16

Symbols – Logic Figures	Definition
	1 out of 2 Function
	2 out of 2 Function
	2 out of 3 Function
	1 out of 4 Function
	2 out of 4 Function
	3 out of 4 Function

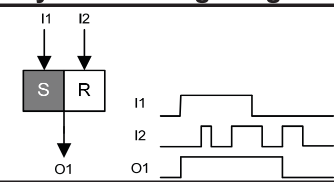
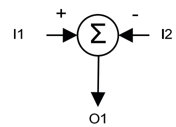
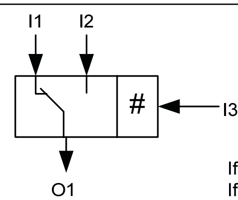
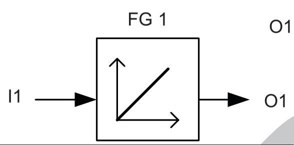
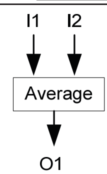
EPR3000-6 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 7 of 16

Symbols – Logic Figures	Definition
	2nd Min Function
	2nd Max Function
	First Order Filter
	Second Order Filter
	Memory with Reset Priority

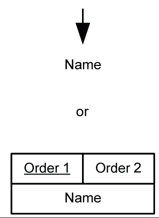
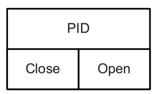
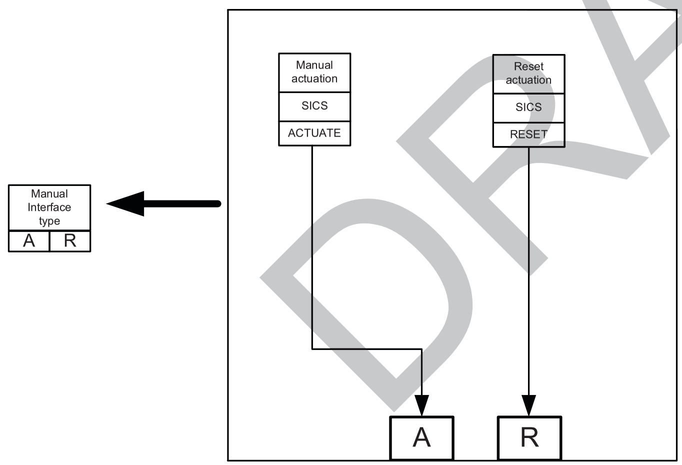
EPR3000-7 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 8 of 16

Symbols – Logic Figures	Definition
	Memory with Set Priority
	Analog Summation
 If I3 = “0”, O1 = I1 If I3 = “1”, O1 = I2	Logic Switch
 O1 is a function of I1 according to reference	Function Generator
 O1 = the average of the input values	Average Function

EPR3000-8 T2

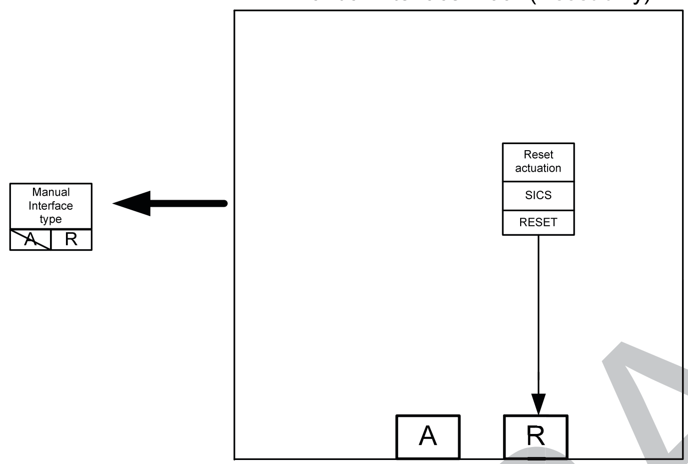
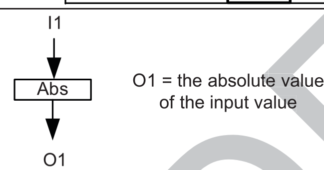
Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 9 of 16

Symbols – Logic Figures	Definition
 Actuator with one control order Actuator with two control orders (Priority order is underlined)	Outputs to Actuator
 PID Controller The controller structure is indicated in the symbol. It is a combination of "P" = proportional action enabled "I" = integral action enabled "D" = derivative action enabled	PID Controller
Manual Interface Block 	Manual Interface Block Actuate and Reset

07.01-26

REV 003
EPR3000-9 T2

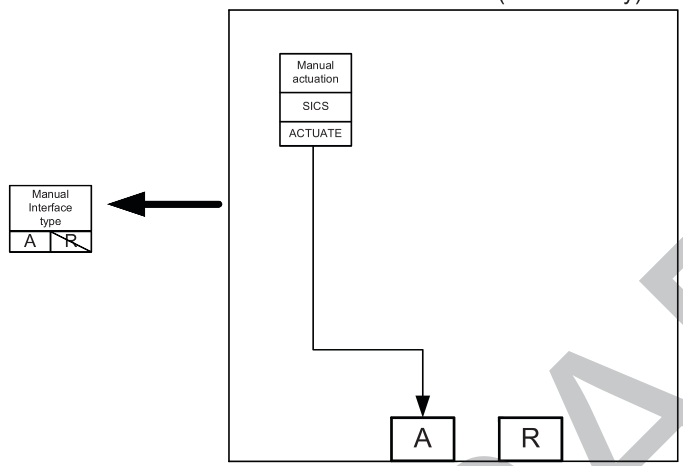
Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 10 of 16

Symbols – Logic Figures	Definition
Manual Interface Block (Reset only) 	Manual Interface Block Reset Only
	Absolute Value Function

07.01-26

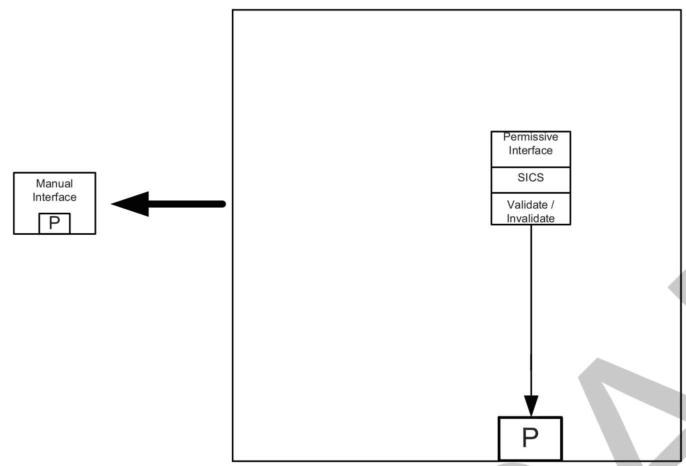
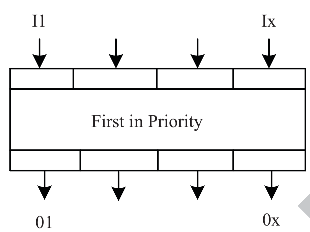
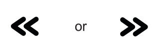
REV 003
EPR3000-10 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 11 of 16

Symbols – Logic Figures	Definition
Manual Interface Block (Actuate Only) 	Manual Interface Block Actuate Only

EPR3000-11 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 12 of 16

Symbols – Logic Figures	Definition
Permissive Interface Block 	Permissive Interface Block
 Binary First in Priority Logic Output 0x is latched = 1 if Input Ix is the first input to = 1 otherwise 0x = 0	Binary First in Priority
 Line Continuation Symbol	Line Continuation

07.01-26

REV 003
EPR3000-12 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 13 of 16

Acronym	Description
ALU	Actuation & Logic Unit
Amps	Ampere
APU	Acquisition & Processing Unit
Aux	Auxiliary
Blwndn	Blowdown
BYP	Bypass
CI	Containment Isolation
CI-V	Containment Isolation Valve
Cleg	Cold Leg
Cls	Close
CPL	Core Power Level
CRDM	Control Rod Drive Mechanism
C-V	Control Valve
CVCS	Chemical and Volume Control System (KBA)
DEGV	Degraded Voltage
Div	Division
DNB	Departure from Nucleate Boiling
DNBR	Departure from Nucleate Boiling Ratio
dP	Differential Pressure
DT	Doubling Time
D-V	Drain Valve
EDG	Emergency Diesel Generator
EFW	Emergency Feedwater
EFWS	Emergency Feedwater System

EPR3000-13 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 14 of 16

Acronym	Description
Ex	Exercise
FCV	Flow Control Valve
FLD	Full Load
FST	Fast
HL	Hot Leg
HLEG	Hot Leg
HLPD	High Linear Power Density
IMB	Imbalance
IRD	Intermediate Range Detector
I-V	Isolation Valve
LCV	Level Control Valve
LLD	Low Load
LOOP	Loss of Offsite Power
LOV	Loss of voltage
LPD	Linear Power Density
Max	Maximum
MaxRD	Maximum Rod Drop
MCR	Main Control Room
MFW	Main Feedwater
Min	Minimum
MS	Main Steam
MSIV	Main Steam Isolation Valve
MSRCV	Main Steam Relief Control Valve
MSRIV	Main Steam Relief Isolation Valve
MSRT	Main Steam Relief Train

EPR3000-14 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 15 of 16

Acronym	Description
NF	Neutron Flux
Norm	Normal
NR	Narrow Range
PICS	Process Information and Control System
PIL V	Pilot Valve
PRD	Power Range Detector
Press	Pressure
Psat	Saturation Pressure
PSRV	Pressurizer Safety Relief Valve
PZR	Pressurizer
QROC	Flux Rate of Change
QUAL	Quality
RAU	Remote Acquisition Unit
RCCA	Rod Cluster Control Assembly
RCPS	Reactor Coolant Pump Speed
RCP	Reactor Coolant Pump
RD	Rod Drop
RT	Reactor Trip
SAS	Safety Automation System
SAT	Saturation
SI	Safety Injection
SICS	Safety Information and Control System
SIS	Safety Injection System
SG	Steam Generator
SGPD	Steam Generator Pressure Drop

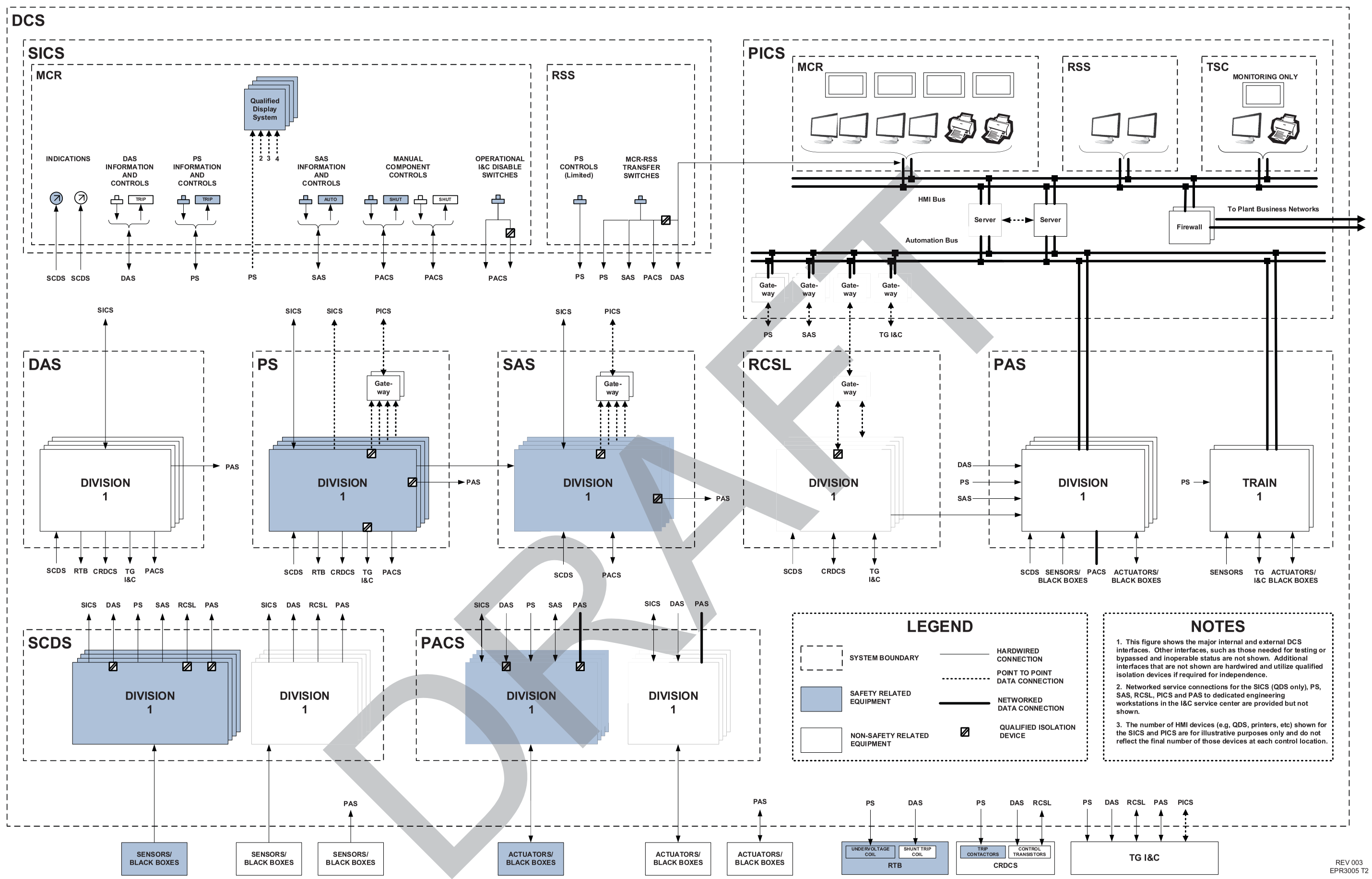
EPR3000-15 T2

Figure 7.1-1—Chapter 7 Symbol Legend
Sheet 16 of 16

Acronym	Description
SOV	Solenoid Operated Valve
SP	Set Point
SPND	Self Powered Neutron Detector
SSS	Startup Shutdown System
T1, T2, T3, T4	Train 1, Train 2, Train 3, Train 4
TDEGV	Time Delay – Degraded Voltage
TEMP	Temperature
TLOV	Time Delay – Loss of Voltage
U.V.Coil	Under Voltage Coil
VLLD	Very Low Load
VCT	Volume Control Tank
WR	Wide Range

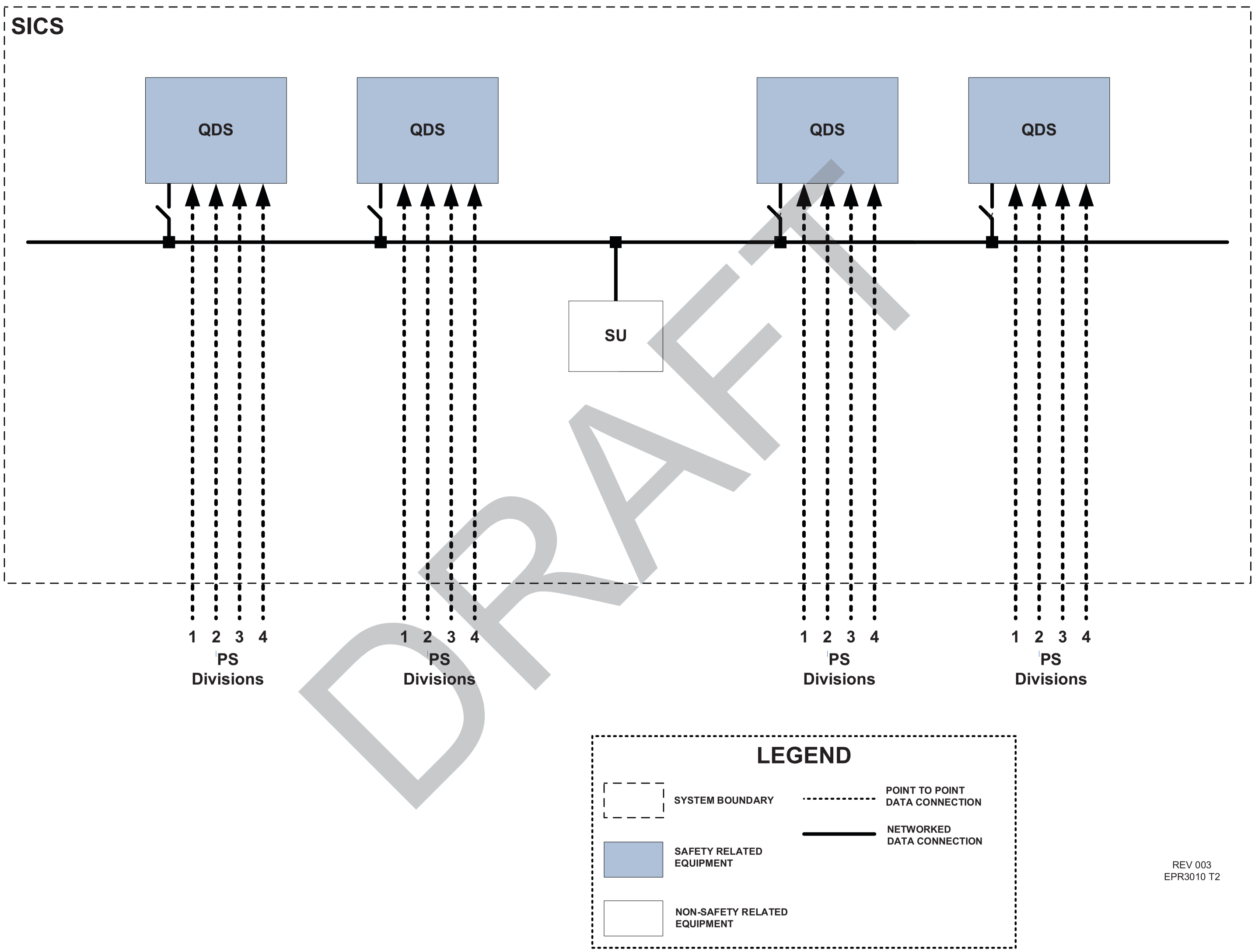
EPR3000-16 T2

Figure 7.1-2—~~U.S. EPR I&C Architecture~~Distributed Control System Functional Architecture



07.01-26

Figure 7.1-3—Safety Information and Control System Architecture (~~Safety-Related Portion~~QDS Portion)



07.01-26

Figure 7.1-4—~~Safety Information and Control System Architecture (Non-Safety-Related Portion~~Deleted~~)~~

07.01-26

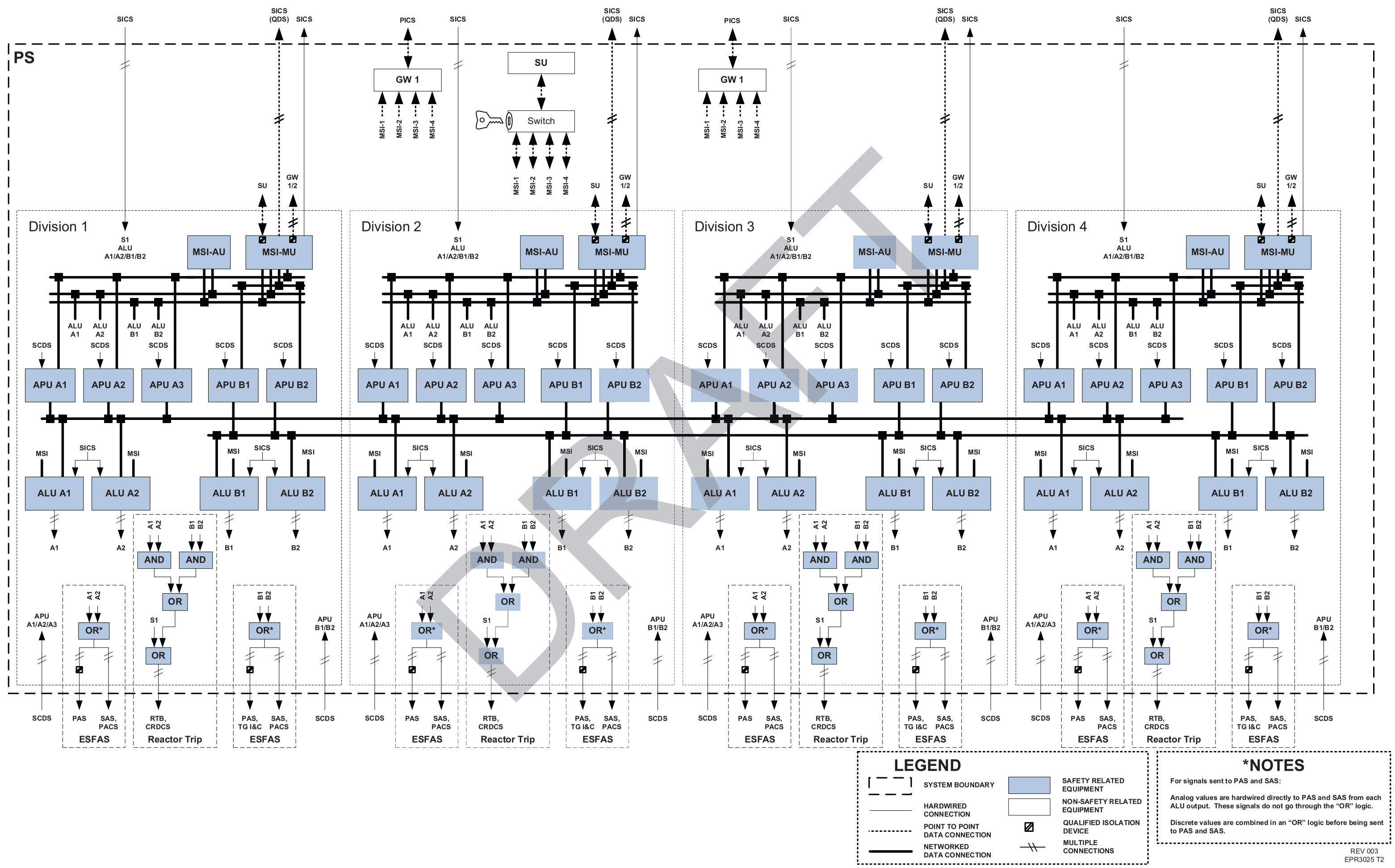
Figure 7.1-5—~~Process Information and Control System Architecture~~Deleted

07.01-26

Next File

07.01-26

Figure 7.1-6—Protection System Architecture



07.01-26

Figure 7.1-7—Safety Automation System Architecture

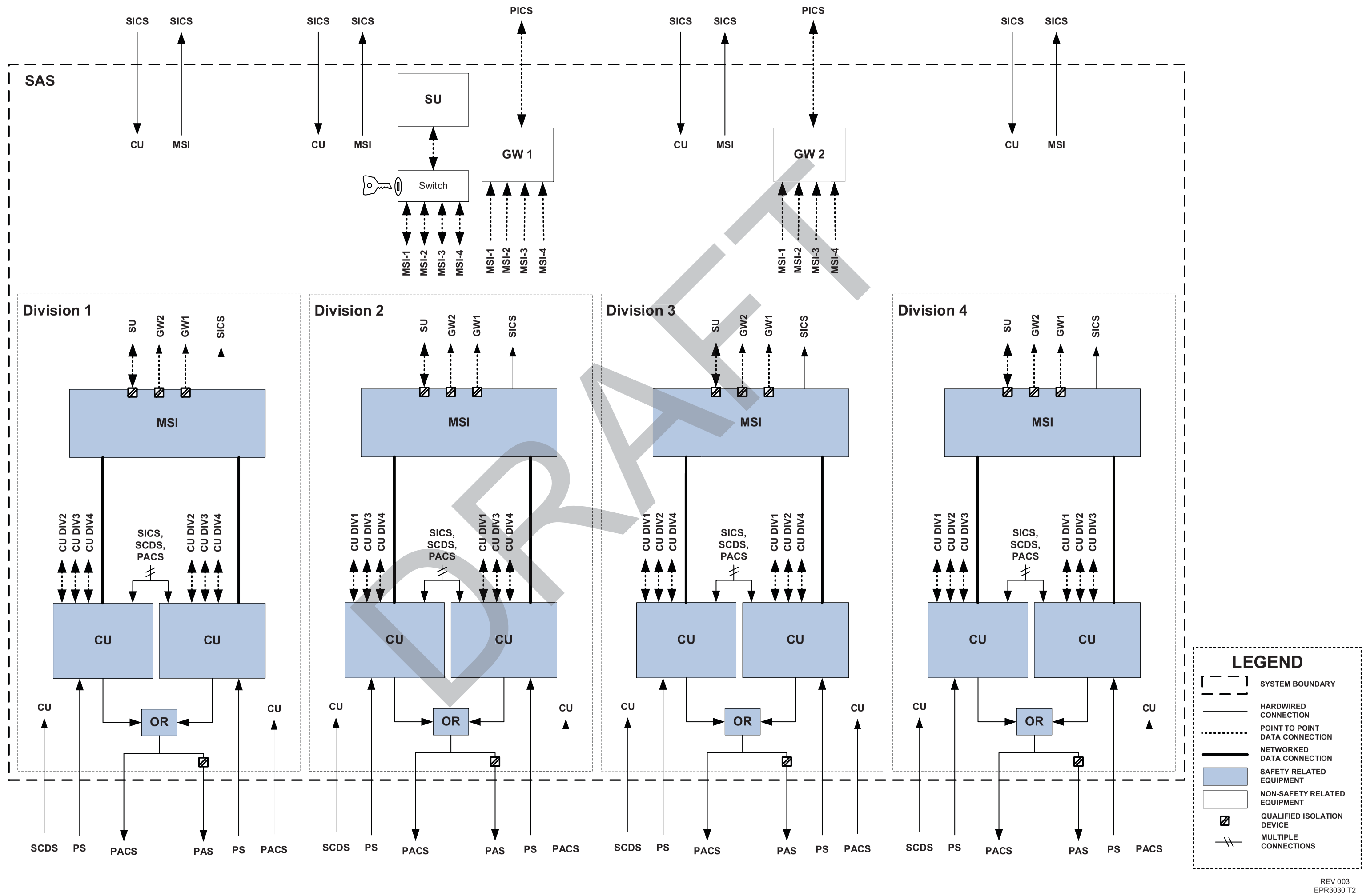
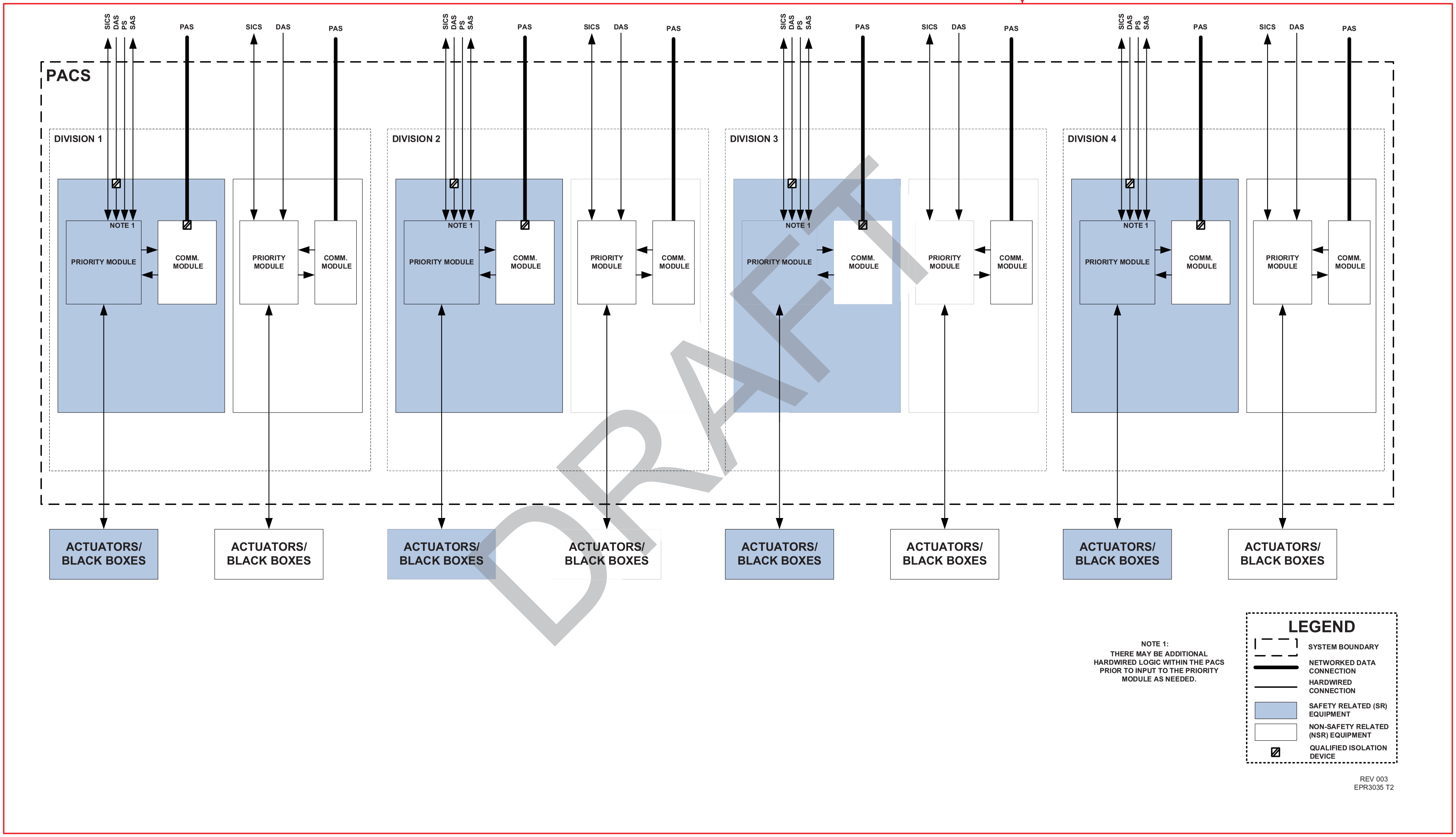


Figure 7.1-8—Priority and Actuator Control System Architecture

07.01-26

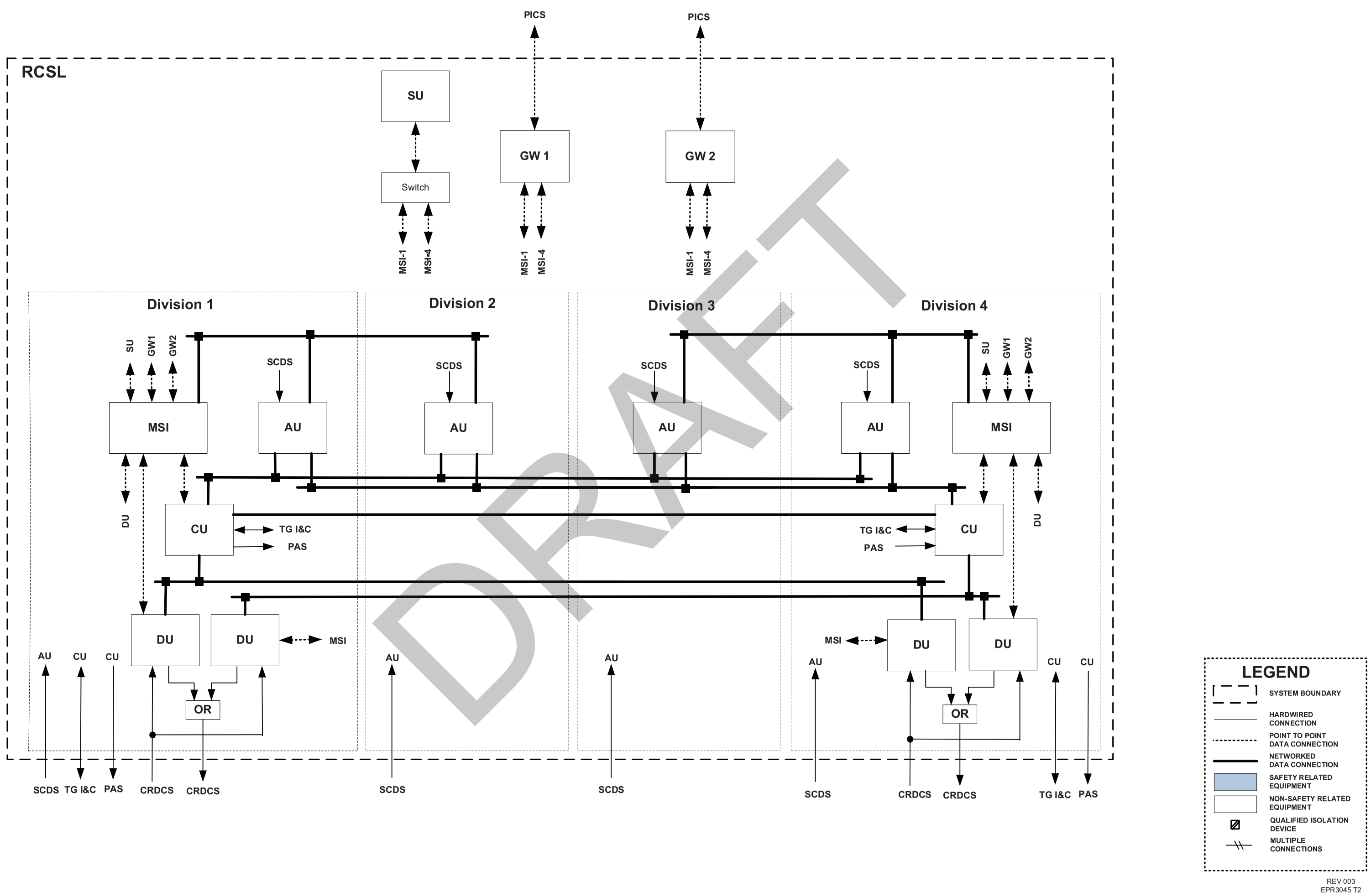


07.01-26

Figure 7.1-9—~~Severe Accident I&C System Architecture~~Deleted

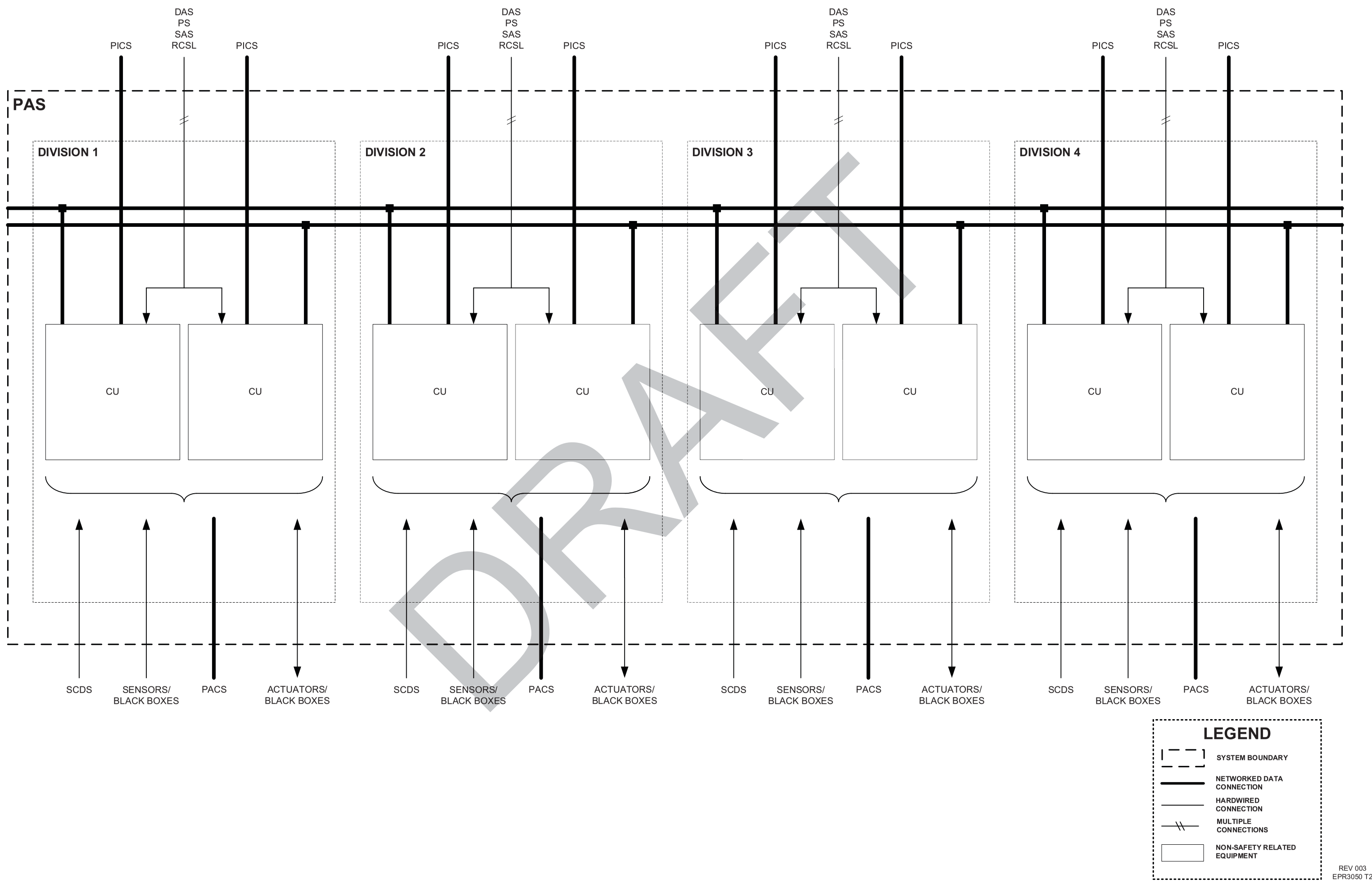
07.01-26

Figure 7.1-10—Reactor Control, Surveillance, and Limitation System Architecture



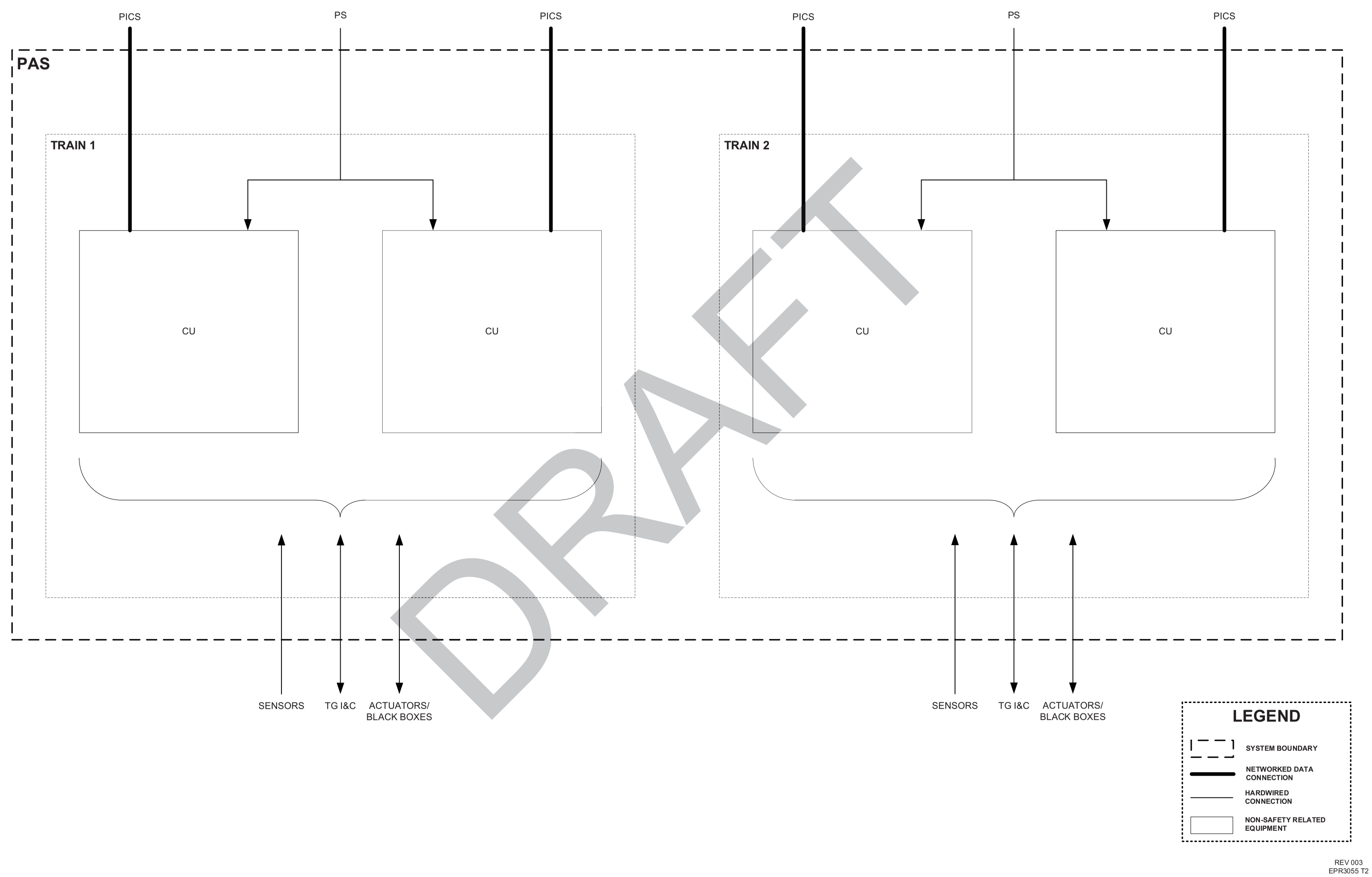
07.01-26

Figure 7.1-11—Process Automation System Architecture (Nuclear Island ~~Subsystem~~)



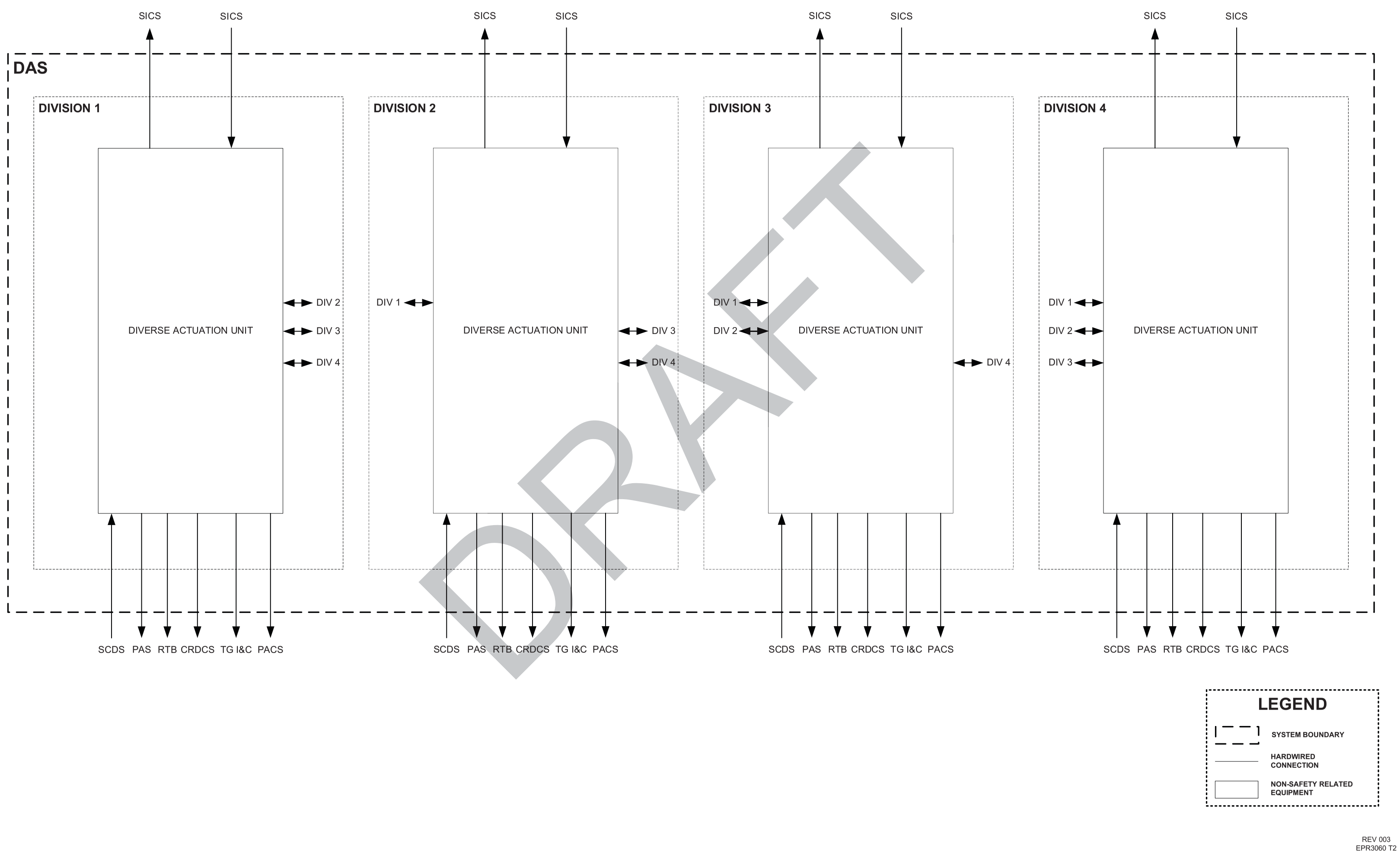
07.01-26

Figure 7.1-12—Process Automation System Architecture (Turbine Island and Balance of Plant ~~Subsystem~~)



07.01-26

Figure 7.1-13—Diverse Actuation System Architecture



Next File

Figure 7.1-14—Measuring Ranges of Excore Instrumentation

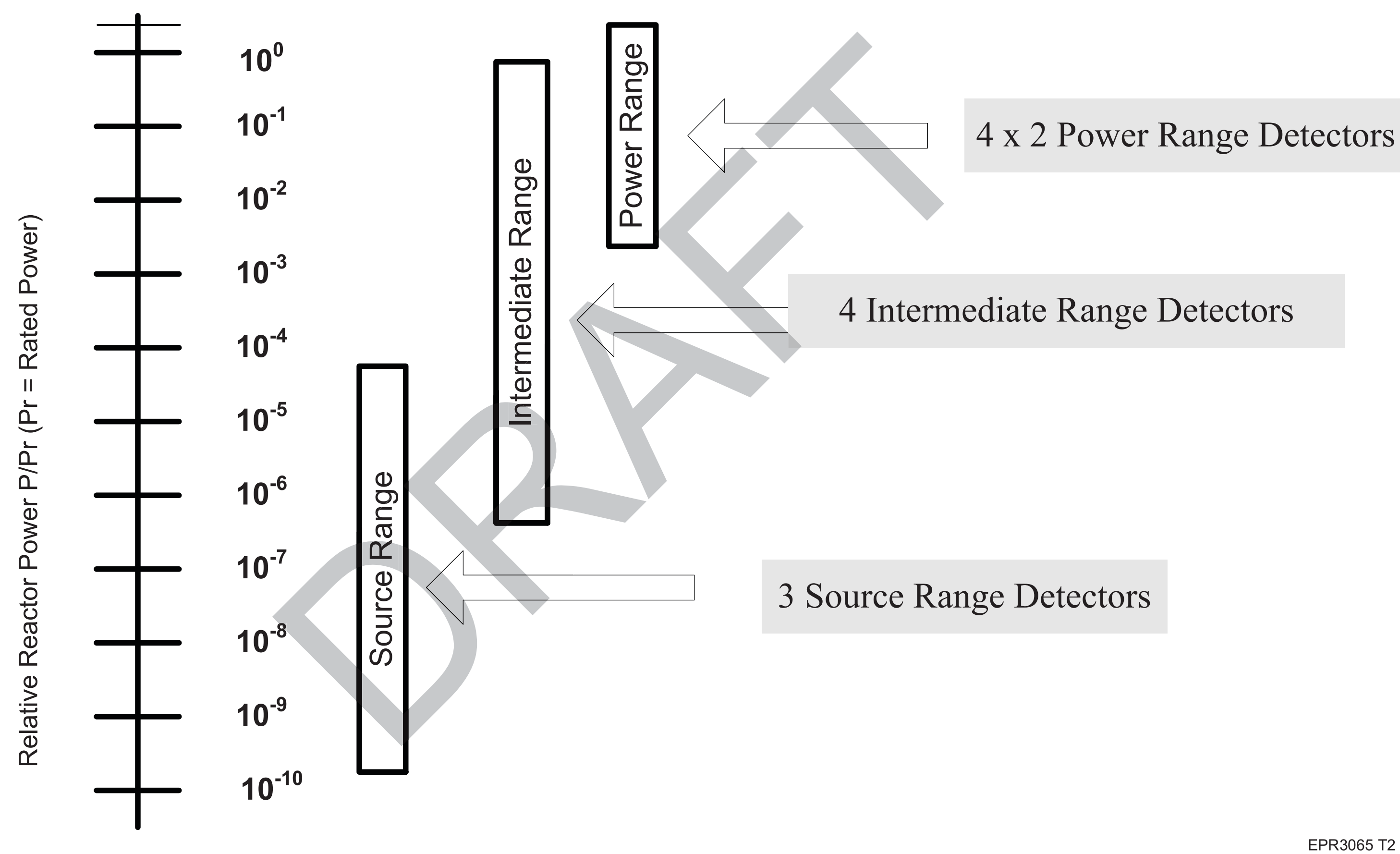
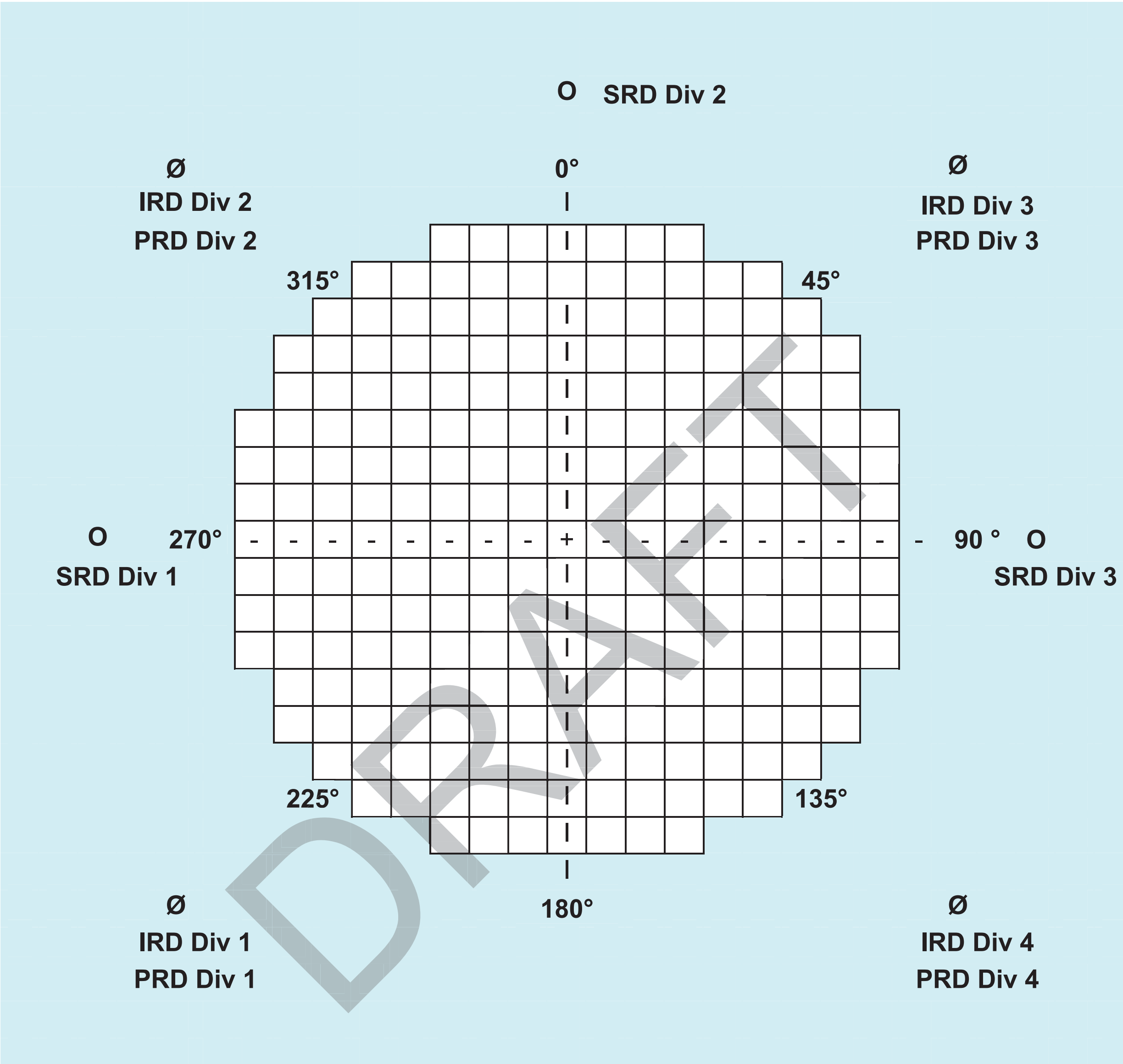


Figure 7.1-15—Excore Instrument Detector Locations



Notes:

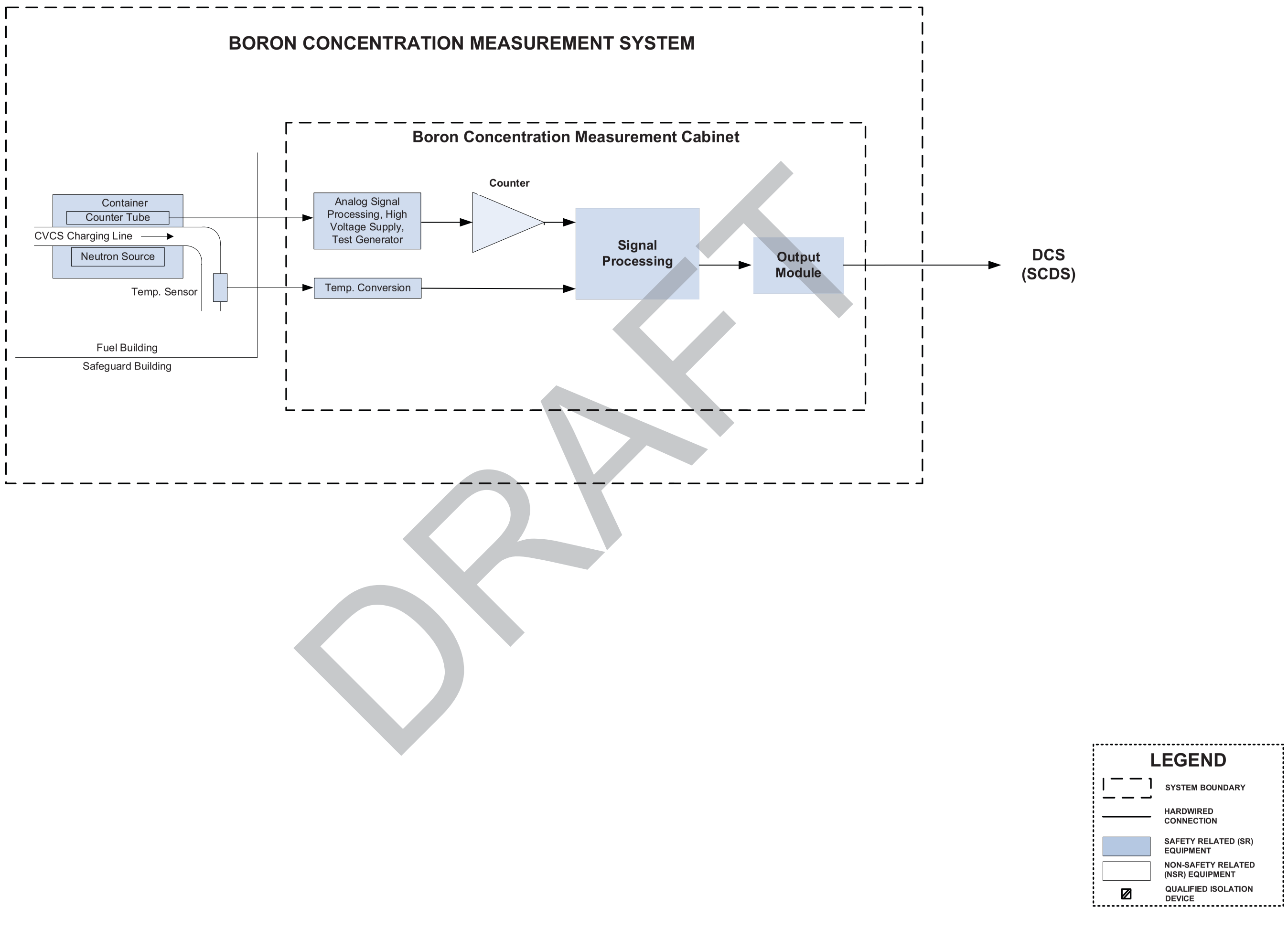
1. PRD : Ø Power Range Detector 4 locations of 2 detectors
2. IRD : Ø Intermediate Range Detector 4 locations of 1 detector
3. SRD : O Source Range Detector 3 locations of 1 detector

EPR3070 T2

Next File

07.01-26

Figure 7.1-16—Boron Concentration Measurement System Arrangement



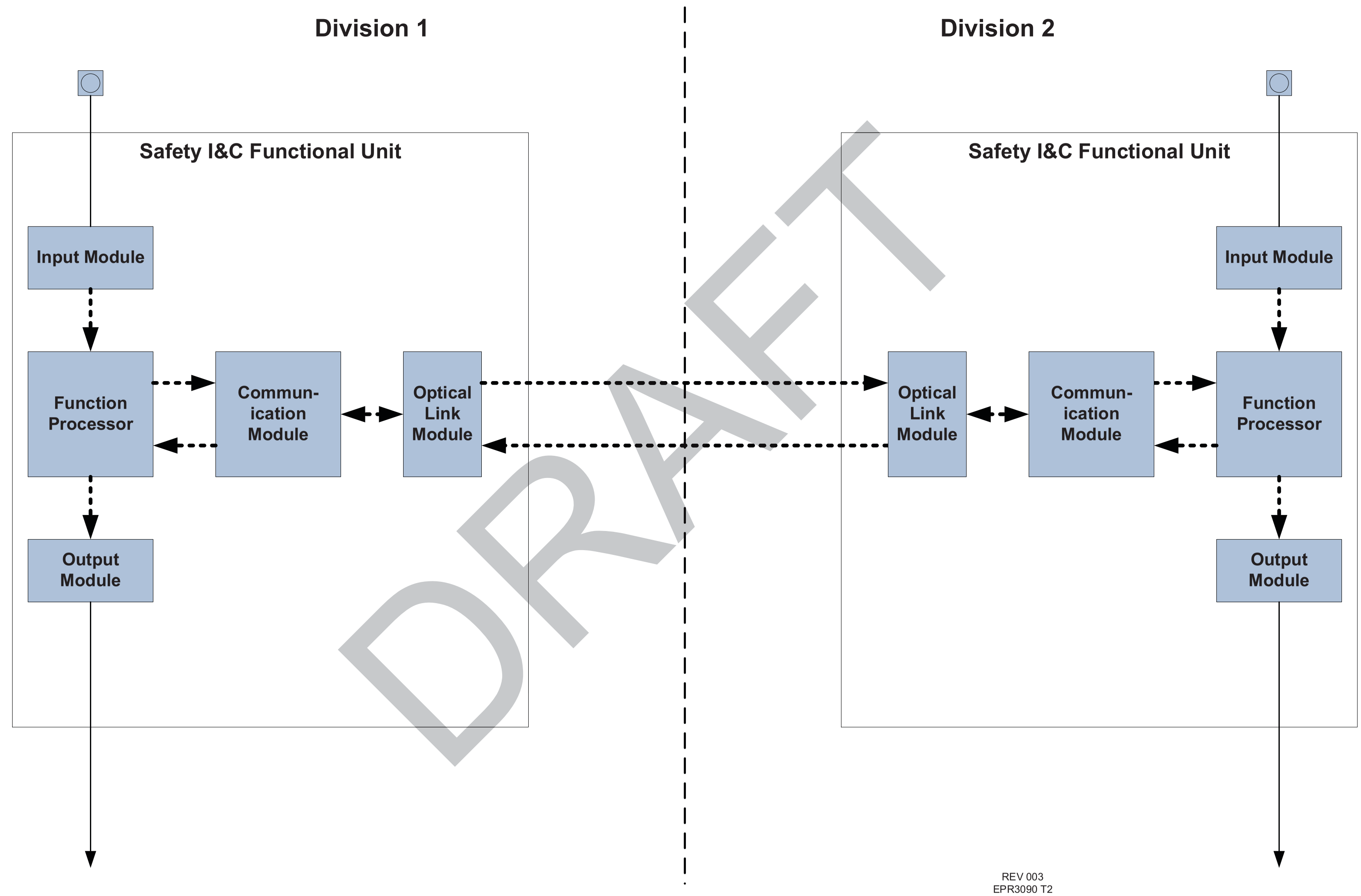
Next File

07.01-26

Figure 7.1-17—~~Implementation of Defense-In-Depth~~Deleted

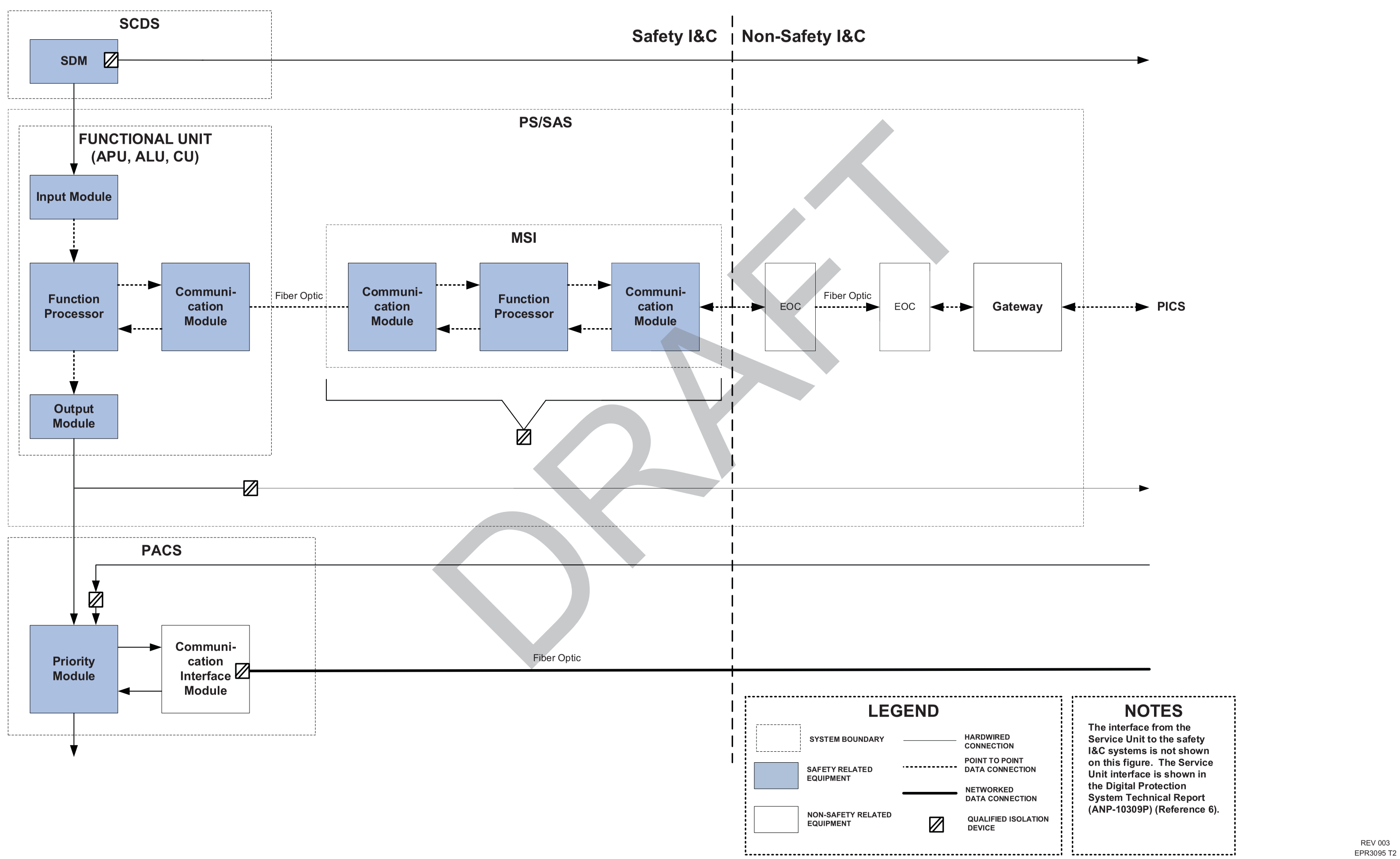
Figure 7.1-18—Deleted

Figure 7.1-19—Implementation of Independence Between Redundant Divisions



07.01-26

Figure 7.1-20—Implementation of Independence Between Safety and Non-Safety I&C

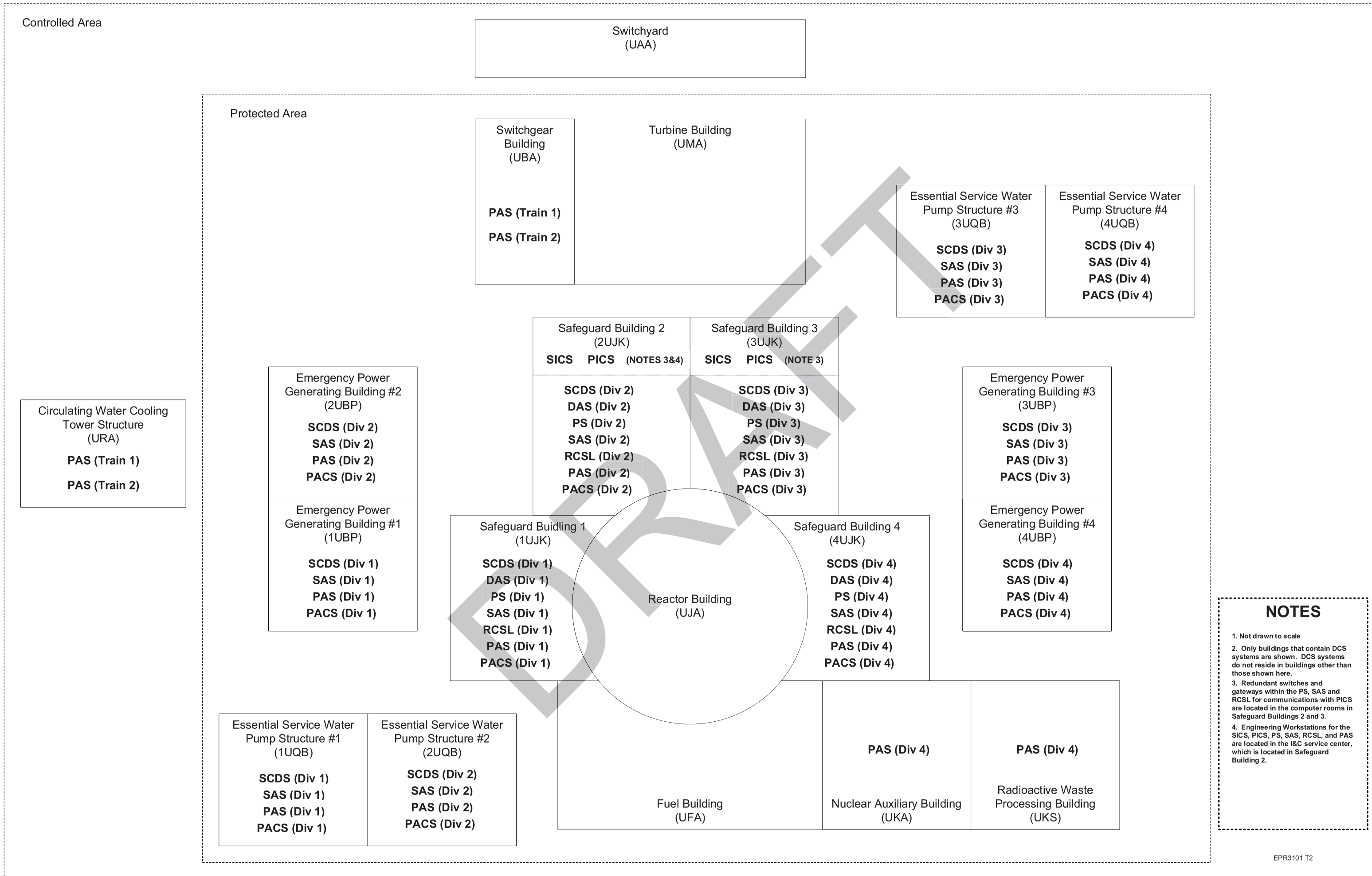


07.01-26

Figure 7.1-21—~~Levels of Defense for Cybersecurity~~Deleted

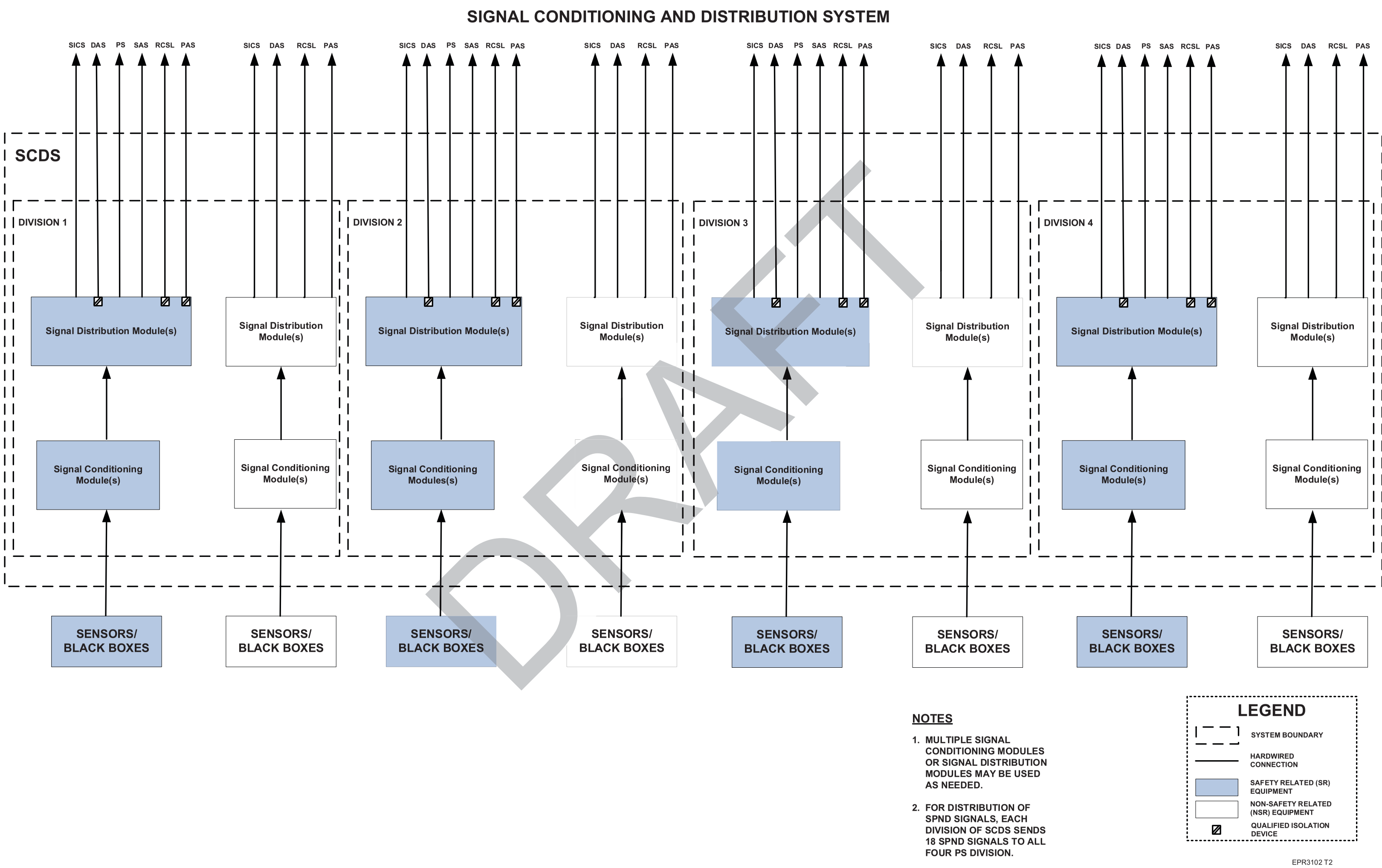
07.01-26

Figure 7.1-22—Distributed Control System Physical Architecture



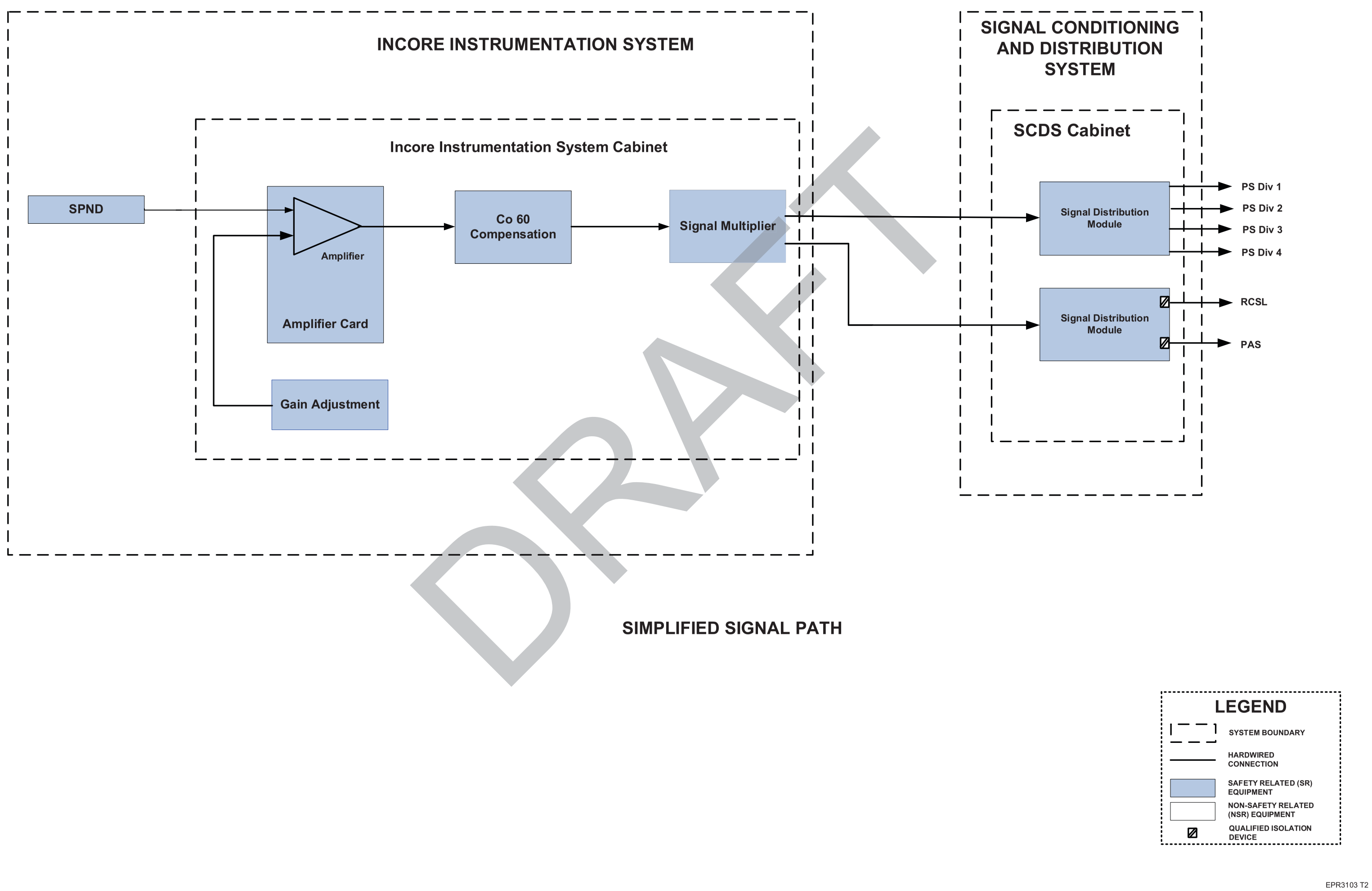
07.01-26

Figure 7.1-23—Signal Conditioning and Distribution System Architecture



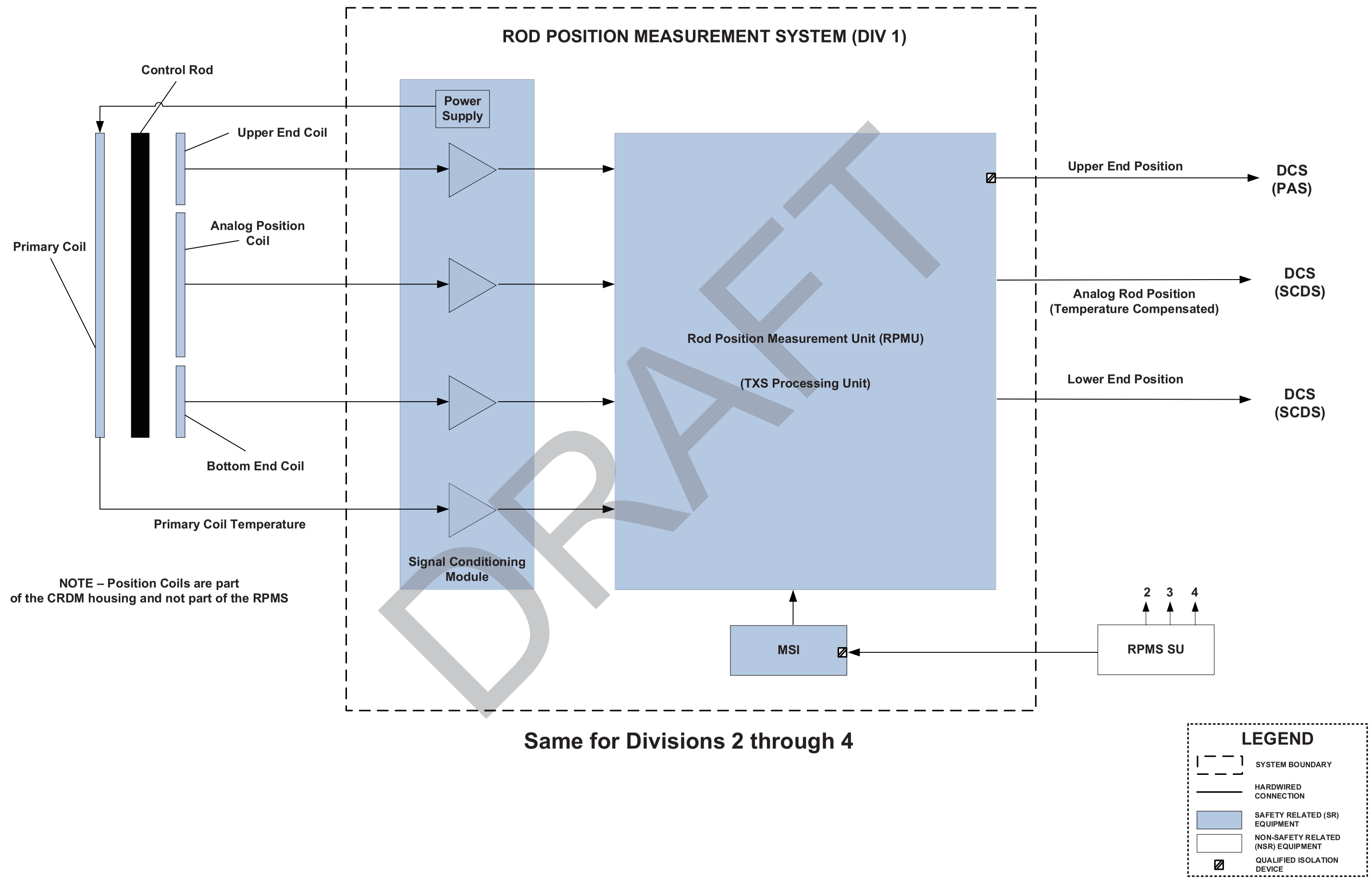
07.01-26

Figure 7.1-24—Self Powered Neutron Detector Functional Arrangement



07.01-26

Figure 7.1-25—Rod Position Measurement System Arrangement



Next File