ArevaEPRDCPEm Resource

From: Pederson Ronda M (AREVA NP INC) [Ronda.Pederson@areva.com]
Sent: Friday, June 12, 2009 6:49 PM
To: Tesfaye, Getachew
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); WELLS Russell D (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56, FSAR Ch 7, Supplement 5
Attachments: RAI 56 Supplement 5 Response US EPR DC.pdf

Getachew,

AREVA NP Inc. (AREVA NP) provided a schedule for a technically correct and complete response to RAI No. 56 on November 26, 2008. AREVA NP submitted Supplement 1 to the response on January 14, 2009 to address 14 of the remaining 45 questions. AREVA NP submitted Supplement 2 to the response on February 4, 2009 to address 5 of the remaining questions. AREVA NP submitted Supplement 3 to the response on March 3, 2009 to address 9 of the remaining questions. AREVA NP submitted Supplement 4 to the response on March 31, 2009 to address 9 of the remaining questions. The attached file, "RAI 56 Supplement 5 Response US EPR DC.pdf" provides technically correct and complete responses to 6 of the remaining 8 questions.

The two RAI responses, listed in the second table below, have been rescheduled due to a delay in obtaining adequate technical basis information for properly supporting the submittal.

The following table indicates the respective pages in the response document, "RAI 56 Supplement 5 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 56 — 07.09-9	2	4
RAI 56 — 07.09-26	5	5
RAI 56 — 07.09-31	6	7
RAI 56 — 07.09-40	8	10
RAI 56 — 07.09-42	11	12
RAI 56 — 07.09-43	13	14

The revised schedule for technically correct and complete responses to the remaining 2 questions is provided below:

Question #	Response Date
RAI 56 — 07.09-2	August 17, 2009
RAI 56 — 07.09-4	August 17, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935

Phone: 434-832-3694
Cell: 434-841-8788

From: WELLS Russell D (AREVA NP INC)
Sent: Tuesday, March 31, 2009 1:20 PM
To: 'Getachew Tesfaye'
Cc: Pederson Ronda M (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56, FSAR Ch 7, Supplement 4

Getachew,

AREVA NP Inc. provided a schedule for a technically correct and complete response to RAI No. 56 on November 26, 2008. AREVA NP submitted Supplement 1 to the response on January 14, 2009 to address 14 of the remaining 45 questions. AREVA NP submitted Supplement 2 to the response on February 4, 2009 to address 5 of the remaining 31 questions. AREVA NP submitted Supplement 3 to the response on March 3, 2009 to address 9 of the remaining 26 questions. The attached file, "RAI 56 Supplement 4 Response US EPR DC.pdf" provides technically correct and complete responses to 9 of the remaining 17 questions, as committed.

The following table indicates the respective pages in the response document, "RAI 56 Supplement 4 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 56 — 07.09-3	2	3
RAI 56 — 07.09-6	4	5
RAI 56 — 07.09-10	6	6
RAI 56 — 07.09-14	7	7
RAI 56 — 07.09-18	8	9
RAI 56 — 07.09-23	10	10
RAI 56 — 07.09-27	11	11
RAI 56 — 07.09-39	12	13
RAI 56 — 07.09-41	14	14

The revised schedule for technically correct and complete responses to the remaining 8 questions is provided below:

Question #	Response Date
RAI 56 — 07.09-2	June 12, 2009
RAI 56 — 07.09-4	June 12, 2009
RAI 56 — 07.09-9	June 12, 2009
RAI 56 — 07.09-26	June 12, 2009
RAI 56 — 07.09-31	June 12, 2009
RAI 56 — 07.09-40	June 12, 2009
RAI 56 — 07.09-42	June 12, 2009
RAI 56 — 07.09-43	June 12, 2009

Sincerely,

(Russ Wells on behalf of)

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
New Plants Deployment
AREVA NP, Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Tuesday, March 03, 2009 3:16 PM
To: Getachew Tesfaye
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56, Supplement 3

Getachew,

AREVA NP Inc. provided a schedule for a technically correct and complete response to RAI No. 56 on November 26, 2008. AREVA NP submitted Supplement 1 to the response on January 14, 2009 to address 14 of the remaining 45 questions. AREVA NP submitted Supplement 2 to the response on February 4, 2009 to address 5 of the remaining 31 questions. The attached file, "RAI 56 Supplement 3 Response US EPR DC.pdf" provides technically correct and complete responses to 9 of the remaining 26 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 56 Question 07.09-22.

The following table indicates the respective pages in the response document, "RAI 56 Supplement 3 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 56 — 07.09-8	2	2
RAI 56 — 07.09-13	3	4
RAI 56 — 07.09-15	5	5
RAI 56 — 07.09-16	6	8
RAI 56 — 07.09-20	9	9
RAI 56 — 07.09-21	10	10
RAI 56 — 07.09-22	11	12
RAI 56 — 07.09-24	13	13
RAI 56 — 07.09-38	14	14

The schedule for response to RAI 56 – 07.09-18 has been changed from March 3, 2009 to March 31, 2009. The schedule for technically correct and complete responses to the remaining 17 questions is unchanged, as indicated in the table provided below:

Question #	Response Date
RAI 56 — 07.09-2	March 31, 2009
RAI 56 — 07.09-3	March 31, 2009
RAI 56 — 07.09-4	March 31, 2009
RAI 56 — 07.09-6	March 31, 2009
RAI 56 — 07.09-9	March 31, 2009
RAI 56 — 07.09-10	March 31, 2009
RAI 56 — 07.09-14	March 31, 2009

RAI 56 — 07.09-18	March 31, 2009
RAI 56 — 07.09-23	March 31, 2009
RAI 56 — 07.09-26	March 31, 2009
RAI 56 — 07.09-27	March 31, 2009
RAI 56 — 07.09-31	March 31, 2009
RAI 56 — 07.09-39	March 31, 2009
RAI 56 — 07.09-40	March 31, 2009
RAI 56 — 07.09-41	March 31, 2009
RAI 56 — 07.09-42	March 31, 2009
RAI 56 — 07.09-43	March 31, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Wednesday, February 04, 2009 2:34 PM
To: 'Getachew Tesfaye'
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56, Supplement 2

Getachew,

AREVA NP Inc. (AREVA NP) submitted Response to RAI No. 56, Supplement 1 on January 14, 2009 to address 14 of the 45 questions. The attached file, "RAI 56 Supplement 2 Response US EPR DC.pdf" provides technically correct and complete responses to 5 of the remaining 31 questions, as committed.

The following table indicates the respective pages in the response document, "RAI 56 Supplement 2 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 56 — 07.09-29	2	3
RAI 56 — 07.09-34	4	6
RAI 56 — 07.09-36	7	9
RAI 56 — 07.09-37	10	12
RAI 56 — 07.09-44	13	14

The schedule for technically correct and complete responses to the remaining 26 questions is unchanged and provided below:

Question #	Response Date

RAI 56 - 07.09-2	March 31, 2009
RAI 56 - 07.09-3	March 31, 2009
RAI 56 - 07.09-4	March 31, 2009
RAI 56 - 07.09-6	March 31, 2009
RAI 56 - 07.09-8	March 3, 2009
RAI 56 - 07.09-9	March 31, 2009
RAI 56 - 07.09-10	March 31, 2009
RAI 56 - 07.09-13	March 3, 2009
RAI 56 - 07.09-14	March 31, 2009
RAI 56 - 07.09-15	March 3, 2009
RAI 56 - 07.09-16	March 3, 2009
RAI 56 - 07.09-18	March 3, 2009
RAI 56 - 07.09-20	March 3, 2009
RAI 56 - 07.09-21	March 3, 2009
RAI 56 - 07.09-22	March 3, 2009
RAI 56 - 07.09-23	March 31, 2009
RAI 56 - 07.09-24	March 3, 2009
RAI 56 - 07.09-26	March 31, 2009
RAI 56 - 07.09-27	March 31, 2009
RAI 56 - 07.09-31	March 31, 2009
RAI 56 - 07.09-38	March 3, 2009
RAI 56 - 07.09-39	March 31, 2009
RAI 56 - 07.09-40	March 31, 2009
RAI 56 - 07.09-41	March 31, 2009
RAI 56 - 07.09-42	March 31, 2009
RAI 56 - 07.09-43	March 31, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Wednesday, January 14, 2009 1:26 PM
To: 'Getachew Tesfaye'
Cc: PANNELL George L (AREVA NP INC); DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56, Supplement 1

Getachew,

The attached file, "RAI 56 Supplement 1 Response US EPR DC.pdf," provides technically correct and complete responses to 14 of the 45 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 56 Question 07.09-7.

The following table indicates the respective page(s) in the response document, "RAI 56 Supplement 1 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 56 - 07.09-1	2	3
RAI 56 - 07.09-5	4	4
RAI 56 - 07.09-7	5	7
RAI 56 - 07.09-11	7	8
RAI 56 - 07.09-12	9	9
RAI 56 - 07.09-17	10	13
RAI 56 - 07.09-19	14	14
RAI 56 - 07.09-25	15	16
RAI 56 - 07.09-28	17	18
RAI 56 - 07.09-30	19	19
RAI 56 - 07.09-32	20	20
RAI 56 - 07.09-33	21	22
RAI 56 - 07.09-35	23	23
RAI 56 - 07.09-45	24	24

The schedule for technically correct and complete responses to the remaining 31 questions is unchanged and provided below:

Question #	Response Date
RAI 56 - 07.09-2	March 31, 2009
RAI 56 - 07.09-3	March 31, 2009
RAI 56 - 07.09-4	March 31, 2009
RAI 56 - 07.09-6	March 31, 2009
RAI 56 - 07.09-8	March 3, 2009
RAI 56 - 07.09-9	March 31, 2009
RAI 56 - 07.09-10	March 31, 2009
RAI 56 - 07.09-13	March 3, 2009
RAI 56 - 07.09-14	March 31, 2009
RAI 56 - 07.09-15	March 3, 2009
RAI 56 - 07.09-16	March 3, 2009
RAI 56 - 07.09-18	March 3, 2009
RAI 56 - 07.09-20	March 3, 2009
RAI 56 - 07.09-21	March 3, 2009
RAI 56 - 07.09-22	March 3, 2009
RAI 56 - 07.09-23	March 31, 2009
RAI 56 - 07.09-24	March 3, 2009
RAI 56 - 07.09-26	March 31, 2009
RAI 56 - 07.09-27	March 31, 2009
RAI 56 - 07.09-29	March 3, 2009
RAI 56 - 07.09-31	March 31, 2009
RAI 56 - 07.09-34	March 3, 2009

RAI 56 - 07.09-36	March 3, 2009
RAI 56 - 07.09-37	March 3, 2009
RAI 56 - 07.09-38	March 3, 2009
RAI 56 - 07.09-39	March 31, 2009
RAI 56 - 07.09-40	March 31, 2009
RAI 56 - 07.09-41	March 31, 2009
RAI 56 - 07.09-42	March 31, 2009
RAI 56 - 07.09-43	March 31, 2009
RAI 56 - 07.09-44	March 3, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Wednesday, November 26, 2008 3:18 PM
To: 'Getachew Tesfaye'
Cc: PANNELL George L (AREVA NP INC); DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56, FSAR Ch 7, Revised Schedule

Getachew,

On October 10, 2008, AREVA NP provided a schedule for responding to the 45 questions in NRC's RAI No. 56. On October 22, 2008, a public meeting was held between AREVA NP Inc. and the NRC to discuss the U.S. EPR FSAR Chapter 7 and RAI No.'s 56 through 61.

A revised schedule for a technically correct and complete response to each of the 45 questions of RAI No. 56 is provided below.

Question #	Response Date
RAI 56 - 07.09-1	January 15, 2009
RAI 56 - 07.09-2	March 31, 2009
RAI 56 - 07.09-3	March 31, 2009
RAI 56 - 07.09-4	March 31, 2009
RAI 56 - 07.09-5	January 15, 2009
RAI 56 - 07.09-6	March 31, 2009
RAI 56 - 07.09-7	January 15, 2009
RAI 56 - 07.09-8	March 3, 2009
RAI 56 - 07.09-9	March 31, 2009
RAI 56 - 07.09-10	March 31, 2009

RAI 56 - 07.09-11	January 15, 2009
RAI 56 - 07.09-12	January 15, 2009
RAI 56 - 07.09-13	March 3, 2009
RAI 56 - 07.09-14	March 31, 2009
RAI 56 - 07.09-15	March 3, 2009
RAI 56 - 07.09-16	March 3, 2009
RAI 56 - 07.09-17	January 15, 2009
RAI 56 - 07.09-18	March 3, 2009
RAI 56 - 07.09-19	January 15, 2009
RAI 56 - 07.09-20	March 3, 2009
RAI 56 - 07.09-21	March 3, 2009
RAI 56 - 07.09-22	March 3, 2009
RAI 56 - 07.09-23	March 31, 2009
RAI 56 - 07.09-24	March 3, 2009
RAI 56 - 07.09-25	January 15, 2009
RAI 56 - 07.09-26	March 31, 2009
RAI 56 - 07.09-27	March 31, 2009
RAI 56 - 07.09-28	January 15, 2009
RAI 56 - 07.09-29	March 3, 2009
RAI 56 - 07.09-30	January 15, 2009
RAI 56 - 07.09-31	March 31, 2009
RAI 56 - 07.09-32	January 15, 2009
RAI 56 - 07.09-33	January 15, 2009
RAI 56 - 07.09-34	March 3, 2009
RAI 56 - 07.09-35	January 15, 2009
RAI 56 - 07.09-36	March 3, 2009
RAI 56 - 07.09-37	March 3, 2009
RAI 56 - 07.09-38	March 3, 2009
RAI 56 - 07.09-39	March 31, 2009
RAI 56 - 07.09-40	March 31, 2009
RAI 56 - 07.09-41	March 31, 2009
RAI 56 - 07.09-42	March 31, 2009
RAI 56 - 07.09-43	March 31, 2009
RAI 56 - 07.09-44	March 3, 2009
RAI 56 - 07.09-45	January 15, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR(TM) Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Friday, October 10, 2008 6:50 PM
To: 'Getachew Tesfaye'
Cc: DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); PANNELL George L (AREVA NP INC); DUNCAN Leslie E (AREVA NP INC); WELLS Russell D (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 56 (942), FSAR Ch7

Getachew,

The attached file, "RAI 56 Response US EPR DC.pdf" provides an interim response to each of the 45 questions.

A complete answer is not provided for 45 of the 45 questions.

A complete response to each of the questions will be provided by December 1, 2008.

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
New Plants Deployment
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Getachew Tesfaye [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Friday, September 12, 2008 5:44 PM
To: ZZ-DL-A-USEPR-DL
Cc: Deanna Zhang; Terry Jackson; Michael Canova; Joseph Colaccino; John Rycyna; Mario Gareri
Subject: U.S. EPR Design Certification Application RAI No. 56 (942), FSAR Ch7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 26, 2008, and on September 5, 2008, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. 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: 577

Mail Envelope Properties (5CEC4184E98FFE49A383961FAD402D31FC6024)

Subject: Response to U.S. EPR Design Certification Application RAI No. 56, FSAR Ch 7, Supplement 5
Sent Date: 6/12/2009 6:48:51 PM
Received Date: 6/12/2009 6:48:54 PM
From: Pederson Ronda M (AREVA NP INC)

Created By: Ronda.Pederson@areva.com

Recipients:
"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen V (AREVA NP INC)" <Karen.Delano@areva.com>
Tracking Status: None
"WELLS Russell D (AREVA NP INC)" <Russell.Wells@areva.com>
Tracking Status: None
"PANNELL George L (AREVA NP INC)" <George.Pannell@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	17650	6/12/2009 6:48:54 PM
RAI 56 Supplement 5 Response US EPR DC.pdf	133897	

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

Response to

Request for Additional Information No. 56, Supplement 5

9/12/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.09 - Data Communication Systems
Application Section: Section 7.1
ICE1 Branch

Question 07.09-9:

Address IEEE Std. 603-1991, Clause 5.4, equipment qualification requirements, and 10 CFR Part 50, Appendix A, General Design Criterion 4, requirements for the subracks, I/O modules, function processors, Optical Link Module, and qualified isolation devices used in the safety automation system (SAS). In addition, identify the corresponding ITAACs and how they verify that the Maintenance Service Interfaces (MSI)s provide adequate communication isolation between safety and non-safety systems to meet the requirements of IEEE Std. 603, Clause 5.6.3 and GDC 24.

DC FSAR, Tier 2, Section 7.1.1.4.2, states that within the SAS, the Control Units (CU)s and the MSIs generally consist of subracks, I/O modules, function processors, communication modules, optical link modules, and qualified isolation devices.

IEEE Std. 603-1991, Clause 5.4, provides equipment qualification requirements for safety systems. This clause requires safety system equipment to be qualified by type test, previous operating experience, or analysis, or any combination of these three methods, to substantiate that it will be capable of meeting, on a continuing basis, the performance requirements as specified in the design basis. Qualification of Class 1E equipment shall be in accordance with the requirements of IEEE Std 323-1983 and IEEE Std 627-1980. Provide more information regarding how the CUs and MSIs have been qualified to meet Clause 5.4 of IEEE Std. 603-1991. In addition, GDC 4, requires structures, systems, and components important to safety to be designed to accommodate the effects of and to be compatible with the environmental conditions associated with normal operation, maintenance, testing, and postulated accidents, including loss-of-coolant accidents. Demonstrate how the requirements of GDC 4 are met for the data communications components within the SAS.

In addition, IEEE 603-1991, Clause 5.6.3, requires independence between safety systems and other systems such that credible failures in and consequential actions by other systems shall not prevent the safety systems from completing their intended safety functions. GDC 24, “Separation of Protection and Control Systems” requires the protection system to be separated from control systems to the extent that failure of any single control system component or channel, or failure or removal from service of any single protection system component or channel which is common to the control and protection systems leaves intact a system satisfying all reliability, redundancy, and independence requirements of the protection system. Identify the ITAACs and describe how they verify that the MSI provides adequate communications isolation between safety and non-safety systems as required by GDC 24 and IEEE Std. 603-1991, Clause 5.6.3. In addition, provide more information on the specific hardware and software design of subracks, I/O modules, function processors, communications link modules, and qualified isolation devices used (i.e. whether they are the same hardware and software qualified and approved in the Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System, [Adams Accession No. ML003732662].)

Response to Question 07.09-9:

U. S. EPR FSAR Tier 2, Section 7.1.2.6.15 states that safety systems shall meet the requirements of Clause 5.4 of IEEE std 603-1998 and that equipment used shall be qualified using appropriate methods under the program described in U.S. EPR FSAR Tier 2, Section 3.11. U.S. EPR FSAR Tier 2, Section 3.11 provides the U.S. EPR approach to Environmental Qualification (EQ) of the equipment. This section also states the approach complies with GDC

1, 2, 4 and 23; 10 CFR 50, Appendix B, Quality Assurance Criteria III, XI, and XVII; and 10 CFR 50.49.

U.S. EPR FSAR Tier 2, Section 7.1.2.2.3 states applicable I&C systems listed in Table 7.1-2 shall be designed to meet the requirements for GDC 4. U.S. EPR FSAR Tier 2, Table 7.1-2 lists the Safety Automation System (SAS) to comply with GDC 4.

U.S. EPR FSAR Tier 2, Section 7.1.1.6.4 states the SICS, PS, SAS and PACS each consists of four independent divisions that are maintained using physical, electrical, and communications independence. This section also states the separation of communication modules from the function processors, separate send and receive data channels, and that the function processors and communications modules operate cyclically and asynchronous to each other in the MSI provide communications independence compliant with Clause 5.6.3.

U.S. EPR FSAR Tier 2, Section 7.1.2.2.13 states the applicable I&C systems listed in Table 7.1-2 are designed to meet the requirements for GDC 24. U.S. EPR FSAR Tier 2, Table 7.1-2 lists the Safety Automation System (SAS) to comply with GDC 24.

RAI 78 Question 14.03.05-4 provides revised ITAAC and an ITAAC mapping table. The ITAAC mapping table identifies ITAAC that addresses Clause 5.4 and Clause 5.6.3 of IEEE 603, and GDC 4 and GDC 24. See the response to RAI 78 Question 14.03.05-4 for details.

AREVA NP notes that design certification is intended to support combined construction and operating licenses for several future power plants. Accordingly, the U.S. EPR design certification application is intended to support current and future versions of the TXS platform, and it is not appropriate to submit information for design certification representing a specific and limited time in the evolution of the TXS platform.

The specific versions of TXS hardware and software designs will not be submitted as part of design certification since this could limit the ability of future COL applicants to use the most recent TXS technology. When a plant-specific version of equipment is selected, the appropriate documentation will be available for NRC audit. ITAAC in U.S. EPR FSAR Tier 1 provide a commitment to equipment qualification and the software development process.

This approach is consistent with the NRC's review process described in the Standard Review Plan (SRP). Specifically, SRP 7.0 states:

> "Review of DC applications should normally extend to cover detailed design. However for a digital computer-based I&C systems, it may be premature to complete final design details at the DC stage. Waiting until the COL stage to complete the final design of such systems allows the COL applicant/licensee to use the most recent technology for each plant. Therefore, the review of the DC applications for digital computer-based I&C systems may be limited to (1) a detailed review at the functional block diagram level, (2) a review of the applicant/licensee's commitment to prescribed limits, parameters procedures, and attributes for the detailed design process, and (3) ITAAC adequate to demonstrate that the as-built facility conforms to these commitments."

FSAR Impact:

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

Question 07.09-26:

Demonstrate how the instrumentation and control (I&C) systems listed Table 7.1-2 of the U.S. EPR DC-FSAR meet IEEE Std. 603-1991, Clauses 5.8.3.3 and 5.8.4.

IEEE Std. 603-1991, Clause 5.8.3.3, states that the capability shall exist in the control room to manually activate the display indications. In addition, IEEE Std. 603-1991, Clause 5.8.4, states that information displays shall be located accessible to the operator. Information displays provided for manually controlled protective actions shall be visible from the location of the controls used to effect the actions.

DC FSAR, Tier 2, Section 7.1.2.1.4, states that 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. Provide information to demonstrate that the U.S. EPR I&C design meets these two clauses of IEEE Std. 603-1991. Specifically, demonstrate that the capability exists in the control room to manually activate the display indications. In addition, provide a schematic of the location of the information displays and demonstrate how these displays are accessible to the operator.

Response to Question 07.09-26:

The capability to manually activate the display indications will be available to conform with the requirements of 10 CFR 50.34(f)(2)(v) and clauses 5.8.2, 5.8.3, and 5.8.4 of IEEE Std. 603-1991. The details of the location and accessibility of the information displays will be defined later in the design process.

The U.S. EPR human systems interfaces provide indication to the operator with regards to bypassed and operable status of safety related systems. This indication is provided to the operator at the controls on both safety information and control system (SICS) and process information and control system (PICS) as described in U.S. EPR FSAR Tier 2, Section 18.7.1.3.4.

FSAR Impact:

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

Question 07.09-31:

Demonstrate how access control is implemented to the U.S. EPR digital instrumentation and controls as required by IEEE Std. 603-1991, Clause 5.9.

IEEE Std. 603-1991, Clause 5.9, provides access control requirements for safety systems. This clause requires the design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

DC FSAR, Tier 2, Section 7.1.1.3.2, states that the processing units (PUs) within the Process Information and Control System (PICS) perform functions such as data message validation, short term data storage, and alarm management. The PUs transmit data to and receive data from the Level 1 instrumentation and control systems via the plant data network. The PUs, operator workstations, POP, and XUs exchange data via the terminal data network. These networks implement periodic communications and message validation for robust data communications. In addition, 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. A firewall is provided for unidirectional transfer of information from the XUs to Level 3 instrumentation and control systems. Remote access to the PICS is prohibited. Although the PICS is not a safety system, it does perform some safety-related functions and thus access control should be designed into the PICS. Provide additional information regarding the access control built into the PICS and plant data network, including information regarding the implementation of the unidirectional firewall, method for prohibiting remote access, network configurations to prevent unauthorized access and data storms, and methods for monitoring and detecting unauthorized access.

Response to Question 07.09-31:

The safety systems meet the requirements of IEEE Std. 603-1991, Clause 5.9, as described in the U.S. EPR FSAR Tier 2, Section 7.1.2.6.20.

The PICS is a non-safety related instrumentation and controls (I&C) system and is not credited to perform safety-related functions. However, both physical and administrative controls are used to provide access control to the PICS.

As discussed in U.S. EPR FSAR Tier 2, Section 18.7.2.5.2, for the PICS workstations that are located in the main control room (MCR), remote shutdown station (RSS), and the I&C Service Center (I&C SC), access is restricted to those rooms by electronic security devices. When the Technical Support Center (TSC) is activated during an emergency, an electronic security device restricts access to that room. Additionally, administrative controls require permission from the control room supervisor or member of management to enter these control rooms.

For PICS workstations that are located outside of the MCR—i.e., local control stations (LCS), TSC, I&C SC and RSS—PICS software controls restrict access to that workstation as well as to the rest of the plant data network. Login features limit access to only the information and controls that are allowed at that workstation.

The PICS provides a means for transfer of data via a unidirectional (one-way) firewall to systems external to the plant operating systems such as the Emergency Operations Facility

(EOF) and the emergency response data system. This communication link prohibits external access to the PICS or other I&C systems, thus precluding the capability of transferring control signals from an external system to the PICS. U.S. EPR FSAR Tier 2, Section 7.1.1.6.6 and Figure 7.1-21, provide details of the levels of defense for cyber security.

Specific implementation details will be available later in the design process of the PICS. Access control system details will be based on current technology at the time of implementation to provide the best technological solution.

FSAR Impact:

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

Question 07.09-40:

Demonstrate how the Maintenance Service Interface (MSI) meets IEEE Std. 603-1991, Clause 5.6.3.

IEEE Std. 603-1991, Clause 5.6.3, requires independence between safety systems and other systems. This clause requires the safety system be designed such that credible failures in and consequential actions by other systems shall not prevent the safety systems from performing their intended safety functions.

DC FSAR, Tier 2, Section 7.1.1.6.4, provides a description of the communications independence principles applied to the I&C design. This section states that 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.

Demonstrate that predefined allowable messages between the safety system and the non-safety systems will comply with IEEE Std. 603-1991, Clause 5.6.3, requirements. Provide a detailed list of all allowable predefined messages that is specific to each case in which communications are required between safety and non-safety systems.

Demonstrate that these predefined allowable messages will not allow the non-safety system to prevent the safety system from performing its safety functions. Provide the necessary ITAACs to verify that the MSI adequately supports the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.3.

Topical Report EMF-2110, Revision 1, TELEPERM XS: A Digital Reactor Protection System [Adams Accession No. ML003732662] section 4.2 states that serial data transmission between class 1E equipment and non class 1E equipment will be performed via a Class 1E qualified "message and service interface (MSI)" computer.

Is the MSI described in the U.S. EPR DC-FSAR the same class 1E qualified computer stipulated in the TELEPERM XS topical report? If not, how is the MSI described in the U.S. EPR DC-FSAR meeting the electrical isolation requirements of IEEE Std. 603-1991, Clause 5.6.3?

Response to Question 07.09-40:

For clarity, this question will be answered in 5 parts according to different topics of included in the question.

Part 1: *"Demonstrate how the Maintenance Service Interface (MSI) meets IEEE Std. 603-1991, Clause 5.6.3…Demonstrate that predefined allowable messages between the safety system and the non-safety systems will comply with IEEE Std. 603-1991, Clause 5.6.3, requirements*." Predefined messages alone do not provide communication independence, but are part of a larger group of features that together provide independence. All messages contain information about the sender and receiver location that is pre-defined at code generation. Messages from unexpected or unknown sources, or messages intended for unknown destinations are ignored. This aspect of communication independence addresses communication failures such as:

- Message may be inserted into the communication medium from unexpected or unknown source.

- Message may be sent to the wrong destination, which could treat the message as a valid message.

In summary, the use of pre-defined messages provides communication independence related to certain types of communication failures (identified in DI&C-ISG-04, Revision 1, "Task Working Group #4: Highly-Integrated Control Rooms- Communications Issues (HICRc)"). Other design features provide communication independence related to other types of communication failures.

Part 1 References:

1. DI&C-ISG-04, Revision 0, "Task Working Group #4: Highly-Integrated Control Rooms-Communications Issues (HICRc)," dated September 28, 2007.

Part 2: "Provide a detailed list of all allowable predefined messages that is specific to each case in which communications are required between safety and non-safety systems." It is not appropriate to submit design information such as a detailed list of pre-defined communication messages as part of the design certification application. This type of information is an output of the detailed software design process and will be available on a plant-specific basis.

Part 3: "Demonstrate that these predefined allowable messages will not allow the non-safety system to prevent the safety system from performing its safety functions" Please see Part 1 of this response for an explanation of the types of communication failures mitigated by the use of pre-defined messages.

Part 4: "Provide the necessary ITAACs to verify that the MSI adequately supports the communications independence requirements of IEEE Std. 603-1991, Clause 5.6.3" The response to RAI 78, Question 14.03.05-4 addresses the specific ITAAC entries that verify compliance with IEEE 603, Clause, 5.6.3.

Part 5: "Is the MSI described in the U.S. EPR DC-FSAR the same class 1E qualified computer stipulated in the TELEPERM XS topical report?"

The MSI described in the U.S. EPR FSAR performs the same functionality as part of a TXS system described in the TELEPERM XS topical report. The individual TXS components that comprise an MSI may be later versions of the specific components described in the TELEPERM XS topical report.

AREVA NP notes that design certification is intended to support combined construction and operating licenses for several future power plants. Accordingly, the U.S. EPR design certification application is intended to support current and future versions of the TXS platform,

and it is not appropriate to submit information for design certification representing a specific and limited time in the evolution of the TXS platform.

The specific versions of TXS hardware and software designs used as an MSI will not be submitted as part of design certification since this could limit the ability of future COL applicants to use the most recent TXS technology. When a plant-specific version of equipment is selected, the appropriate documentation will be available for audit. ITAAC is provided in U.S. EPR FSAR Tier 1 to verify equipment qualification and software design lifecycle.

This approach is consistent with the NRC's review process described in the Standard Review Plan (SRP). Specifically, SRP 7.0 states:

> "Review of DC applications should normally extend to cover detailed design. However for a digital computer-based I&C systems, it may be premature to complete final design details at the DC stage. Waiting until the COL stage to complete the final design of such systems allows the COL applicant/licensee to use the most recent technology for each plant. Therefore, the review of the DC applications for digital computer-based I&C systems may be limited to (1) a detailed review at the functional block diagram level, (2) a review of the applicant/licensee's commitment to prescribed limits, parameters procedures, and attributes for the detailed design process, and (3) ITAAC adequate to demonstrate that the as-built facility conforms to these commitments."

FSAR Impact:

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

Question 07.09-42:

Demonstrate how the developmental process of the TELEPERM XS platform and application software meets Regulatory Guide 1.152, regulatory positions C.2.1 through C.2.5.

10 CFR 52.47(a)(9) requires, in part, that for applications for light-water cooled nuclear power plants, an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application. The evaluation required by this section shall include an identification and description of all differences in design features, analytical techniques, and procedural measures proposed for a facility and those corresponding features, techniques, and measures given in the SRP acceptance criteria. Where such a difference exists, the evaluation shall discuss how the alternative proposed provides an acceptable method of complying with those rules or regulations of commission, or portions thereof that underlie the corresponding SRP acceptance criteria. SRP, Appendix 7.1D, "Guidance for Evaluation of the Application of IEEE Std 7-4.3.2," provides review acceptance criteria for Regulatory Guide 1.152 regulatory positions C.2.1 through C.2.9.

DC FSAR, Tier 2, Section 7.1.1.6.6, states that the cyber security controls for TELEPERM XS application software development fully meets the intent of Regulatory Positions C.2.1 through C.2.5 of Regulatory Guide 1.152. However, the description of the developmental process of the TELEPERM XS platform and application has not provided sufficient information regarding what measures are in place to scan for backdoors, hidden code, and malicious code in the system software as stipulated in Regulatory Guide 1.152, Regulatory Position C.2.4. The staff finds that additional information is required to determine the adequacy of the software developmental process for the TELEPERM XS system to address the acceptance criteria provided in the Standard Review Plan Appendix 7.1D. Specifically, provide information regarding the measures taken to scan for backdoors, hidden code, and malicious code in the TELEPERM XS platform and application software.

Response to Question 07.09-42:

TELEPERM XS (TXS) software consists of TXS system code and TXS application code. All TXS code is fully documented to the requirements specified for the software integrity level of the code. The standard TXS system is described in the TXS Topical Report, EMF-2110(NP)(A), which describes both the design features and development process for the TXS hardware platform and operating system. The cyber-security controls for the development of the TXS operating system software and function block library software are also discussed in the TXS Topical Report. Each software package is developed utilizing the same processes described in the TXS Topical Report.

Protection against malicious source code manipulations and undocumented source code is based on code inspection by peer developers. The code inspection assures that only functionality required by the previous development phases is implemented by the source code. Requirements, design descriptions, source code and comments are checked by at least one internal reviewer and by one independent assessor. Thus, any malicious manipulation or undocumented functionality at any step of the development process would be detected and corrected.

The development process for the qualified components of the TXS system platform includes comprehensive Validation and Verification (V&V) activities by the manufacturer, as well as an

external appraisal of the development and test results by test institutes (the German Society for Plant Safety and Reactor Safety and the Institute for Safety). The V&V activities which are performed during development comprise:

- Reviews of the development documentation and test specifications.
- Module tests of the vital software components – all possible branches within the function to be tested are executed in this process.
- Code inspections of the complete source code.
- Functional tests of the software components.

A qualification certificate is issued by the test institute for each qualified software module demonstrating that the module is qualified by test to the specified requirements.

The application of the SPACE (Specification and Coding Environment) engineering tools is mandatory to specify the safety functions together with the detailed architecture of the target system and to generate the application software, which is loaded to the processing units of the safety I&C target system (after compiling, linking and locating the code). The code generator tools have been designed and qualified for the creation of safety application software (ANSI C source code). The project specific software has to be generated entirely by means of these tools so that all design rules and interfaces defined for TXS application software functions are met. The use of the SPACE tool eliminates the direct human interface with the application software source code.

Cyclic redundancy checksum (CRC) checks are performed on the software using TXS software tools *reflist, scanmic* and *verify* so there is no possibility of malicious code hiding in the software package by unambiguously identifying all project files and directories immediately after a successfully compilation. CRCs are calculated based on file content and file size. CRCs are sensitive to changes of the file's content. To verify that a file was not modified, the CRC of the respective file is calculated and stored separately. The CRC can be recalculated at any time and compared with the originally stored CRC. If both CRC are the same, the file has not been modified. TXS provides the tools for calculating CRC checks for files and directories (*reflist*) and tools for reading CRC checks from the compiled mic-files (*scanmic*) and tools for reading CRC checksums from the loaded mic-files (*verify*). Virus scans are also performed on software items prior to entry into the Software Library including TXS application software.

The design documentation, internal V&V activities and independent qualification activities ensure that the system software, as developed, does not contain undocumented code, malicious code or other unwanted and undocumented functions. No third party or commercial off-the-shelf safety software is used in the TXS system. For this reason there are no hidden functions that need to be disabled or removed.

FSAR Impact:

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

Question 07.09-43:

Demonstrate how access control is achieved on the safety and non-safety data communications systems to meet IEEE Std. 603-1991 clause 5.9, access control requirements.

IEEE Std. 603-1991, Clause 5.9, provides access control requirements for safety systems. This clause requires the safety system design to permit the administrative control of access to safety system equipment. These administrative controls shall be supported by provisions within the safety systems, by provision in the generating station design, or by a combination thereof.

The applicant stated in DC FSAR, Tier 2, Section 7.1.1.6.6, and in AREVA NP Topical Report ANP-10272 that control of access outside the safety system and critical control systems is the responsibility of the Combined License (COL) applicant. However, the staff did not identify a COL information item addressing these access control provisions. If no COL information item is provided, demonstrate where cyber security control of access outside the safety system and critical control systems is addressed. Provide details regarding the implementation of the plant data network and the interface between the plant data network to the terminal data network. Provide additional information regarding the implementation of the uni-directional firewall and any associated intrusion detection and monitoring systems.

Response to Question 07.09-43:

The plant data network transmits data on the system automation level and is the communication link between safety and non-safety systems. It uses an Ethernet communication protocol rather than TCP/IP. TCP/IP is commonly exploited in cyber attacks and the use of Ethernet eliminates a possible cyber attack strategy. Fiber optic cabling is used for electrical isolation. There is no remote access to these systems.

Safety and critical control non-safety systems are insulated from the plant data network by a Gateway (GW) and Monitoring and Service Interface (MSI). This is the only physical connection that exists between the plant data network and the service unit and system computers. The GW provides an interface between the differing platforms running safety and non-safety systems. The MSI checks for and uses only data from expected messages as well as only checking configured communication channels. These design features provide assurance that unexpected or improper messages are ignored.

The MSI is also connected to the Service Unit (SU), which provides an interface to the service network. It is the central means for interventions into the safety relevant software of the function processors. The installed control mechanisms assure that only authorized persons may access the SU and only authorized interventions may be performed. Authorized persons are identified with a login/password and each authorized person is assigned certain user rights. The cabinets containing these SU are locked and opening any cabinet will result in an alarm in the main control room. Key lock switches protect modification to any safety software.

The terminal data network transmits data on the unit supervision and control level. It provides a communication link between components of the process information and control system (PICS). This terminal data network is connected to the plant data network via two redundant processing units (PU). Each PU performs data message validation and keeps a signal image of all acquired signals (value, quality-code and time stamp).

PICS interfaces with external computer systems on the business management system level via a single external unit (XU). A uni-directional firewall stands between the XU and the external computer systems. The XU allows one-way communication from PICS to the external computer systems and prevents any control signals from the external systems from entering PICS.

Refer to U.S. EPR FSAR Tier 2, Figure 7.1-21 for an illustration of the cyber-security levels of defense.

FSAR Impact:

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