

ArevaEPRDCPEm Resource

From: DUNCAN Leslie E (AREVA NP INC) [Leslie.Duncan@areva.com]
Sent: Friday, February 19, 2010 4:57 PM
To: Tesfaye, Getachew
Cc: DELANO Karen V (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); ROMINE Judy (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 285, FSAR Ch 7, Supplement 3
Attachments: RAI 285 Supplement 3 Response US EPR DC.pdf

Getachew,

AREVA NP Inc. (AREVA NP) provided responses to 4 of the 20 questions of RAI No. 285 on November 11, 2009. AREVA NP submitted Supplement 1 to the response on December 17, 2009 to address 6 of the remaining 16 questions. AREVA NP submitted Supplement 2 to the response on January 22, 2010 to provide a revised schedule for the remaining questions. The attached file, "RAI 285 Supplement 3 Response US EPR DC.pdf" provides technically correct and complete responses to 7 of the remaining 10 questions. The schedule for a technically correct and complete response to question 07.03-25 remains unchanged, and the schedule for technically correct and complete responses to questions 07.01-15 and 07.03-21 has been changed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which supports the response to RAI 285 Supplement 3 Questions 07.01-16, 07.03-27, 07.04-11, and 07.04-13.

The following table indicates the respective pages in the response document, "RAI 285 Supplement 3 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 285 — 07.01-13	2	3
RAI 285 — 07.01-16	4	5
RAI 285 — 07.01-17	6	8
RAI 285 — 07.03-26	9	11
RAI 285 — 07.03-27	12	13
RAI 285 — 07.04-11	14	14
RAI 285 — 07.04-13	15	17

The schedule for a technically correct and complete response to question 07.03-25 remains unchanged and provided below. The schedule for technically correct and complete responses to questions 07.01-15 and 07.03-21 has been changed and is provided below.

Question #	Response Date
RAI 285 — 07.01-15	March 5, 2010
RAI 285 — 07.03-21	April 16, 2010
RAI 285 — 07.03-25	February 26, 2010

Sincerely,

Les Duncan
Licensing Engineer
AREVA NP Inc.
An AREVA and Siemens Company

Tel: (434) 832-2849
Leslie.Duncan@areva.com

From: DUNCAN Leslie E (AREVA NP INC)
Sent: Friday, January 22, 2010 6:27 PM
To: 'Tesfaye, Getachew'
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. 285, FSAR Ch 7, Supplement 2

Getachew,

AREVA NP Inc. provided responses to 4 of the 20 questions of RAI No. 285 on November 11, 2009. AREVA NP submitted Supplement 1 to the response on December 17, 2009 to address 6 of the remaining 16 questions.

AREVA NP is unable to provide a response to the 9 RAI No. 285 questions with a commitment date of January 22, 2010. The commitment date for these nine questions has been changed to February 19, 2010 to allow time to incorporate comments and feedback from the upcoming 1/25/10-1/26/10 meeting with the NRC related to U.S. EPR FSAR Chapter 7.

The schedule for a technically correct and complete response to RAI 285 Question 07.03-25 is unchanged and provided below. The schedule for technically correct and complete responses to the other nine RAI questions has been changed and is provided below:

Question #	Response Date
RAI 285 — 07.01-13	February 19, 2010
RAI 285 — 07.01-15	February 19, 2010
RAI 285 — 07.01-16	February 19, 2010
RAI 285 — 07.01-17	February 19, 2010
RAI 285 — 07.03-21	February 19, 2010
RAI 285 — 07.03-25	February 26, 2010
RAI 285 — 07.03-26	February 19, 2010
RAI 285 — 07.03-27	February 19, 2010
RAI 285 — 07.04-11	February 19, 2010
RAI 285 — 07.04-13	February 19, 2010

Sincerely,

Les Duncan
Licensing Engineer
AREVA NP Inc.
An AREVA and Siemens Company
Tel: (434) 832-2849
Leslie.Duncan@areva.com

From: WELLS Russell D (AREVA NP INC)
Sent: Thursday, December 17, 2009 1:26 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. 285, FSAR Ch 7, Supplement 1

Getachew,

AREVA NP Inc. provided responses to 4 of the 20 questions of RAI No. 285 on November 11, 2009. The attached file, "RAI 285 Supplement 1 Response US EPR DC.pdf" provides technically correct and complete responses to 6 of the remaining 16 questions, as committed.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which supports the response to RAI 285 Questions 07.02-31 and 07.03-23.

The following table indicates the respective pages in the response document, "RAI 285 Supplement 1 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 285 — 07.01-12	2	2
RAI 285 — 07.02-31	3	3
RAI 285 — 07.03-22	4	5
RAI 285 — 07.03-23	6	6
RAI 285 — 07.03-24	7	8
RAI 285 — 07.05-9	9	9

The schedule for a technically correct and complete response to the remaining questions is unchanged and provided below.

Question #	Response Date
RAI 285 — 07.01-13	January 22, 2010
RAI 285 — 07.01-15	January 22, 2010
RAI 285 — 07.01-16	January 22, 2010
RAI 285 — 07.01-17	January 22, 2010
RAI 285 — 07.03-21	January 22, 2010
RAI 285 — 07.03-25	February 26, 2010
RAI 285 — 07.03-26	January 22, 2010
RAI 285 — 07.03-27	January 22, 2010
RAI 285 — 07.04-11	January 22, 2010
RAI 285 — 07.04-13	January 22, 2010

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: Wednesday, November 11, 2009 6:11 PM

To: Tesfaye, Getachew

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. 285, FSAR Ch. 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information RAI 285. The attached file, "RAI 285 Response US EPR DC.pdf" provides technically correct and complete responses to 4 of the 20 questions.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 285 Questions 07.01-14 and 07.04-12.

The following table indicates the respective page(s) in the response document, "RAI 285 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 285 — 07.01-12	2	2
RAI 285 — 07.01-13	3	3
RAI 285 — 07.01-14	4	4
RAI 285 — 07.01-15	5	5
RAI 285 — 07.01-16	6	6
RAI 285 — 07.01-17	7	8
RAI 285 — 07.02-30	9	10
RAI 285 — 07.02-31	11	11
RAI 285 — 07.03-21	12	12
RAI 285 — 07.03-22	13	13
RAI 285 — 07.03-23	14	14
RAI 285 — 07.03-24	15	15
RAI 285 — 07.03-25	16	16
RAI 285 — 07.03-26	17	17
RAI 285 — 07.03-27	18	18
RAI 285 — 07.04-10	19	19
RAI 285 — 07.04-11	20	20
RAI 285 — 07.04-12	21	21
RAI 285 — 07.04-13	22	23
RAI 285 — 07.05-9	24	24

A complete answer is not provided for 16 of the 20 questions. The schedule for a technically correct and complete response to these questions is provided below.

Question #	Response Date
RAI 285 — 07.01-12	December 18, 2009
RAI 285 — 07.01-13	January 22, 2010
RAI 285 — 07.01-15	January 22, 2010
RAI 285 — 07.01-16	January 22, 2010
RAI 285 — 07.01-17	January 22, 2010
RAI 285 — 07.02-31	December 18, 2009
RAI 285 — 07.03-21	January 22, 2010
RAI 285 — 07.03-22	December 18, 2009

RAI 285 — 07.03-23	December 18, 2009
RAI 285 — 07.03-24	December 18, 2009
RAI 285 — 07.03-25	February 26, 2010
RAI 285 — 07.03-26	January 22, 2010
RAI 285 — 07.03-27	January 22, 2010
RAI 285 — 07.04-11	January 22, 2010
RAI 285 — 07.04-13	January 22, 2010
RAI 285 — 07.05-9	December 18, 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: Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]

Sent: Tuesday, October 13, 2009 4:49 PM

To: ZZ-DL-A-USEPR-DL

Cc: Spaulding, Deirdre; Truong, Tung; Morton, Wendell; Cheung, Calvin; Jackson, Terry; Canova, Michael; Guardiola, Maria; Colaccino, Joseph; ArevaEPRDCPEm Resource

Subject: U.S. EPR Design Certification Application RAI No. 285(3560,3507,3552,3564,3565), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 25, 2009, and discussed with your staff on September 3, 2009. Draft RAI Question 07-01-13 was 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: 1158

Mail Envelope Properties (F322AA625A7A7443A9C390B0567503A10199C71C)

Subject: Response to U.S. EPR Design Certification Application RAI No. 285, FSAR Ch
7, Supplement 3
Sent Date: 2/19/2010 4:56:34 PM
Received Date: 2/19/2010 4:56:37 PM
From: DUNCAN Leslie E (AREVA NP INC)

Created By: Leslie.Duncan@areva.com

Recipients:

"DELANO Karen V (AREVA NP INC)" <Karen.Delano@areva.com>
Tracking Status: None
"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>
Tracking Status: None
"ROMINE Judy (AREVA NP INC)" <Judy.Romine@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: AUSLYNCMX01.adom.ad.corp

Files	Size	Date & Time
MESSAGE	10127	2/19/2010 4:56:37 PM
RAI 285 Supplement 3 Response US EPR DC.pdf		167781

Options

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

Response to

**Request for Additional Information No. 285 (3560, 3507, 3552, 3564, 3565),
Supplement 3, Revision 1**

10/13/2009

U. S. EPR Standard Design Certification

AREVA NP Inc.

Docket No. 52-020

SRP Section: 07.01 - Instrumentation and Controls - Introduction

SRP Section: 07.02 - Reactor Trip System

SRP Section: 07.03 - Engineered Safety Features Systems

SRP Section: 07.04 - Safe Shutdown Systems

SRP Section: 07.05 - Information Systems Important to Safety

Application Section: FSAR Ch. 7

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

Question 07.01-13:

Follow-up to RAI Question 07.01-4

Demonstrate that the requirements for independence are met by providing clarification and additional information which discusses and includes supporting descriptive drawings of the trip contactors that either (1) indicate classification of the trip contactors as non-safety related, if they are not needed to perform a safety function, or (2) address adequate separation and isolation between the safety-related trip contactors and the non-safety related Control Rod Drive Control System (CRDCS) or (3) classify the CRDCS as safety-related. Additionally, provide corresponding updates to the U. S. EPR FSAR.

The staff reviewed the AREVA NP response to RAI 07.01-4 and found that a supplemental RAI is necessary. AREVA NP indicated in their response that although the control rod drive control system (CRDCS) is classified as non-safety related, the trip contactor modules, which are a component of the CRDCS, are classified as safety-related. 10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. IEEE Std. 603-1991, Clause 5.6.3, requires, in part, that equipment that is used for both safety and non-safety functions shall be classified as part of the safety systems. Clarification and additional information is needed since the information provided in the response seems to contradict the requirements of IEEE 603. Additional information is needed to provide clarification of the design, so that the staff will be able to make a reasonable assurance determination concerning conformity of the facility design to NRC rules and regulations, particularly in regard to independence requirements.

Response to Question 07.01-13:

Safety classification of the CRDCS is based on the U.S. EPR safety classification methodology, which is detailed in the U.S. EPR FSAR Section 3.2. U.S. EPR FSAR Tier 2, Section 3.2 states:

“The U.S. EPR safety classification methodology makes a distinction between primary design functions and secondary design functions. A primary design function is a principal function for which an SSC must be included in the plant design. A secondary design function is a function that the SSC must be capable of fulfilling because of the position of that SSC within the plant design. Both primary and secondary design function can be, but need not be, safety-related.

Safety classification of systems considers only their primary design functions. Thus, systems are safety-related if any one of their primary design functions is safety-related.”

The primary design function of the CRDCS is to control the movement of the 89 rod cluster control assemblies (RCCAs) in the reactor vessel by providing current to the individual coils of the CRDM. This function is classified as a non-safety-related function. The trip contactors, as part of the CRDCS, also have the capability to interrupt power to the CRDMs when a trip signal is received from the PS, which is classified as a safety-related function. Therefore, the CRDCS is classified as a non-safety-related system since the primary design functions of the CRDCS are non-safety related.

The classification of the CRDCS system is consistent with IEEE Std. 603, Clause 5.6.3. The equipment in the CRDCS that performs both safety and non-safety functions (trip contactors)

are classified as safety related. The remainder of the equipment in the CRDCS system performs only non-safety-related functions and is classified as non-safety-related.

Isolation between the safety related protection system and the non-safety uninterruptible power supply system (NUPS) is provided by the trip contactors themselves. The trip contactors consist of contactors (primary side) and interposing relays (secondary side). The primary and secondary sides of the trip contactors are electrically isolated. Each trip contactor receives a signal from the PS on the primary side, which in turn controls the interposing relays on the secondary side. The secondary side interrupts power from the NUPS to the CRDMs via the interposing relays.

The design of the CRDCS cabinets provides for independence of the safety-related contactor modules from the non-safety-related components of the system consistent with the guidance of IEEE Std. 384 as committed by U.S. EPR FSAR Tier 2, Section 7.1.2.4.5.

FSAR Impact:

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

Question 07.01-16:

Follow-up to RAI Question 07.01-7

Identify the inspections, tests, analyses, and acceptance criteria (ITAAC) that will verify that the TELEPERM XS (TXS) platform is installed in accordance with the NRC staff approved TXS topical report, and as necessary, provide corresponding updates to the U.S. EPR FSAR.

The staff reviewed the AREVA NP response to RAI 07.01-7 (EPM RAI # 955-3366), and found that a supplemental RAI is necessary. In RAI 07.01-7, the NRC staff asked for details regarding any modifications to the TXS platform design, processes, hardware, and software since the TXS topical report was approved by the staff in May 2000. AREVA NP indicated in their response to RAI 07.01-7 that U.S. EPR FSAR design certification application does not contain this detailed information, and that the application is intended to support current and future versions of the TXS platform. The response also mentioned the use of ITAAC on a plant-specific basis. ITAAC are required so that the NRC staff can make a reasonable assurance determination such that if the ITAAC are performed, that the facility will be in conformity with NRC rules and regulations. Specifically, the staff needs to be able to make a reasonable assurance determination that any modifications to the TELEPERM XS (TXS) platform design processes, hardware, and software since the TXS topical report was approved in May 2000, to demonstrate that the system hardware, system software, and engineering tools development processes continue to meet the quality requirements of 10 CFR 50.55a(a)(1) and GDC 1. This includes software verification and validation (V&V) methods.

Response to Question 07.01-16:

Section 4.1.2 of the Software Program Manual, ANP-10272, Revision 1, provides the criteria for use of TXS hardware and system software developed or modified since the TXS topical report EMF-2110(NP)(A), was approved by NRC staff in May 2000. The criteria are:

- Changes do not modify or eliminate the key design principles as described in the TXS topical report.
- Changes do not modify or eliminate the key processing features as described in the TXS topical report.
- Changes do not modify or eliminate the key communication independence features as described in the TXS topical report.
- Changes to the TXS platform (hardware and software modules) do not result in more than a minimal increase in the likelihood of occurrence of a malfunction of the TXS software.
- Changes to the TXS hardware do not result in more than a minimal increase in the consequences of a malfunction in the TXS System.
- Changes to the TXS hardware do not create a possibility for a malfunction of a TXS System with a different result.
- Changes to the TXS development procedures do not result in a reduction in quality methods described in the TXS topical report.

Section 4.1.3 of the Software Program Manual, Revision 1, provides an evaluation process that specifies the TXS platform and procedure characteristics to be evaluated in support of the criteria identified in Section 4.1.2. Section 4.1.4 of the Software Program Manual provides a description of the change evaluation reports, which will contain the basis for the acceptance of any change.

U.S. EPR FSAR Tier 2, Section 7.1.1.2.1 will be modified to reference the TXS change process that is described in the Software Program Manual.

ITAAC will be added to Tier 1 that will verify that the all safety-related I&C systems using the TELEPERM XS platform are in accordance with the NRC staff approved TXS topical report. These ITAAC additions can be found in the following Tier 1 sections:

- 2.4.1 Protection System (PS)
- 2.4.2 Safety Information and Control System (SICS)
- 2.4.4 Safety Automation System (SAS)

FSAR Impact:

U.S. EPR FSAR, Tier 2, Section 7.1.1.2.1 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR FSAR, Tier 1, Sections 2.4.1, 2.4.2 and 2.4.4 will be revised as described in the response and indicated on the enclosed markup.

Question 07.01-17:

Follow-up to RAI Question 07-01-10

Identify and describe deviations taken from the TELEPERM XS topical report and provide sufficient detail on each deviation to demonstrate that the safety evaluation from May 2000 is still applicable.

The staff reviewed the response to RAI 07.01-10 and found that additional information is needed. The original RAI indicated that the U. S. EPR FSAR does not have sufficient discussion on deviations taken from the TELEPERM XS topical report (TR). The original RAI asked for the identification of all deviations taken from the TELEPERM XS TR and details on each deviation to demonstrate that the safety evaluation from May 2000 is still applicable. The response to the RAI indicated that there are no deviations from the design principles and methods that the staff approved. The staff identified an example of a deviation taken from the TELEPERM XS TR, in which it was indicated that communication between initiation trains to the plant process information system will be unidirectional using signal messages, whereas in the U. S. EPR design, this communication is bidirectional.

The staff found the deviation in the following paragraphs of the TELEPERM XS TR which states in part:

2.9.1 Specification of the Requirements

Specific communication methods are applied to ensure interference-free communication inside the TELEPERM XS system as well as to other systems e.g., the plant process information system. ...

a. Communication Between the Redundant Initiation Trains of a Safety I&C System

It is required that in case of a single failure of one of the redundant initiation trains ... or within one communication channel ... the trains still available will continue to operate as designed ...

b. Communication from the Initiation Trains to the Plant Process Information System

The Communication ... from the initiation trains of the safety I&C system to the plant process information system (PPIS) is done via the monitoring and service interface (MSI). This communication channel is only used unidirectionally by signaling messages to the plant process information system according to the application specifically designed messages. The intermediate monitoring and service interface serves as isolation means in conformity with the TELEPERM XS system architecture.

c. Communication Between the Initiation Trains and the Service Unit

The communication (Cs) between the initiation trains of the safety I&C system and the service unit has to be examined in two different ways:

- For normal cyclic operating, it has to be ensured that normal cyclic operating of all function processors (SVE1) can not be impaired as far as no specific release is given.

- In case of intended interventions from the service unit by the service personnel ...

It has to be ensured by the release logic independently processed by the service unit that only one of the redundant initiation trains of the safety I&C system can be influenced from the service unit at a time."

The staff requests that AREVA evaluate this apparant deviation, as well as other deviations, that may be taken from the TELEPERM XS topical report so as to provide a complete and accurate description of the U.S. EPR I&C design.

Response to Question 07.01-17:

The TELEPERM XS (TXS) topical report, EMF-2110(NP)(A) discussed many aspects of the TXS platform, and was sometimes unclear in differentiating which aspects were fundamental design features that would not change on an application-specific basis and which aspects could be modified to suit the needs of a specific plant application without adverse impact to safety.

The aspects of the TXS platform discussed in the topical report 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.

As technology evolves, the TXS platform hardware and software will be modified, upgraded, and new modules will be introduced. For this reason, a change evaluation process has been included in the TXS Software Program Manual (ANP-10272, Revision 1) to specifically address the differences between hardware and system software used in an as-built TXS system from what was described in the TXS topical report. This process is outlined in the Response to Question 07.01-16. As part of that response, an ITAAC was created that enables evaluation of differences in as-built hardware and system software against that described in the TXS topical report. This addresses categories 1 and 2.

Regarding category 3, it is not necessary to evaluate each application-specific system architecture for differences from the conceptual architectural aspects described in the TXS topical report. Instead, for each safety-related instrumentation and control (I&C) system using the TXS platform, an application-specific architecture (including external interfaces) is provided to the NRC for evaluation and review against the current NRC regulations and guidance. These application-specific submittals supersede the example system architectures that were included in the TXS topical report to provide context for the review of the generic TXS platform. The U.S. EPR FSAR contains the architecture for the I&C systems using the TXS platform, and describes how these application-specific implementations satisfy NRC regulations and guidance. For example, the response to RAI 286, Question 07.09-46 will address the plant-specific interface issue of bi-directional communication by explaining how communications independence is achieved consistent with DI&C-ISG-04 guidance.

FSAR Impact:

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

Question 07.03-26:

Follow-up to RAI Question 07.03-14

Provide specific equipment protective provisions that prevent the safety systems from accomplishing their safety functions.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 4.11 requires applicants to provide the equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The description in Section 7.1.2.6.10 of the U.S. EPR DC-FSAR, Revision 1, does not identify equipment protective provisions. The response to RAI 07.03-14 stated that the U.S. EPR DC-FSAR does not include provisions for equipment protection. Will the U.S EPR not provide equipment protective provisions such as over-current trips for safety-related electric motors? If there are no equipment protective provisions that prevent the safety systems from accomplishing their safety functions, please state so in the U.S. EPR DC-FSAR. If there are equipment protective provisions, please specifically identify them in the U.S. EPR DC-FSAR to satisfy Clause 4.11 of IEEE Std. 603-1991.

Response to Question 07.03-26:

For clarification, the response to RAI 07.03-14 stated that functional requirements of the protection system did not include any provisions for equipment protection that could prevent performance of safety functions, not that the U.S. EPR FSAR does not include provisions for equipment protection.

As stated in U.S EPR FSAR Tier 2, Section 7.1.2.6.10, descriptions of the process systems are located in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10, and Chapter 11. In these chapters, process system requirements are discussed, including equipment protection requirements that can impact safety.

For example, protective provisions for medium voltage electric motors are described in U.S. EPR FSAR Tier 2, Section 8.3.1.1.3.

The equipment protective functions for safety equipment consider environmental and system transient conditions in determining the trip settings for the protective device, for example an over-current device for a safety related motor. The protective device settings are conservatively biased toward accomplishing that safety function. However, there could be conditions which warrant a protective action because the random single failure could be an electrical fault or motor overload condition that must be cleared from the safety related power source to protect the motor from severe damage and also protect the associated cabling.

In some cases, protective functions that are active under non-emergency operation are temporarily bypassed/inhibited or completely bypassed/inhibited during emergency operation. The emergency diesel generator system provides a good example of how these design features can be effectively implemented in a safety system while still providing a reliable safety function.

U.S. EPR FSAR Tier 2, Section 8.3.1.1.5 describes the following:

Emergency Diesel Generator

Protective feature temporary bypass/inhibit during emergency operation:

Engine protection features active during all modes:

- Electrical overspeed.
- Engine mechanical overspeed.
- Low lube oil pressure.
- High jacket water temperature.
- The low essential service water pressure trip is bypassed during start-up for approximately 120 seconds.

Protective feature bypass/inhibit during entire duration of emergency operation:

Generator protection features active during test mode only, alarms are still active during emergency mode:

- Time over current.
- High bearing temperature.
- High winding temperature.
- Rotating diode failure.
- Excitation fault (over and under excitation).
- Reverse power during parallel (with the grid) operation.
- Generator field ground.

Design features/requirements for equipment protective devices have been successfully implemented in operating plants and will be implemented in the same manner in the U.S. EPR. Appropriate protective device settings will be determined and applied with a bias (additional margin) toward safety function success while still providing adequate safety equipment protection if needed.

It should be noted that if a piece of safety equipment is prevented from performing its function (for example, 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. These FMEAs are presented in the chapters of the U.S. EPR FSAR where the process systems are described. From this perspective, it can be said that no single equipment protective function (equivalent to single failure of the equipment) can prevent performance of a safety function.

FSAR Impact:

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

Question 07.03-27:

Follow-up to RAI Question 07.03-18

Clarify the technical position concerning manual initiation of a steam generator (SG) isolation due to a steam generator tube rupture event.

In the U.S. EPR DC-FSAR, Section 15.0.03.7, operator actions are credited for isolating an affected SG during a steam generator tube rupture event (SGTR). U.S. EPR DC-FSAR, Section 7.3.1.2.14, describes how the PS will automatically perform an isolation of an affected SG during a SGTR. The description in Chapter 7 of the U.S. EPR DC-FSAR does not address the crediting of manual actions for a SGTR event, which would include discussion of how the design meets IEEE Std. 603-1991, Clause 5.8.1 and 6.2.2.

1. Identify the indications and controls needed and specifically and state in the FSAR that credit is taken for manual actions for SG Isolation to address IEEE Std. 603-1991, Clauses 5.8.1 and 6.2.2.
2. Explain why credit is being taken for manual SG isolation in the accident analyses for a SGTR when automatic mechanisms are available.

Response to Question 07.03-27:

The response to this question is provided in two parts corresponding to the numbered requests in the question.

Part 1:

IEEE 603-1998, Clause 5.8.1 states: "The display instrumentation provided for manually controlled actions for which no automatic control is provided and the display instrumentation required for the safety systems to accomplish their safety functions shall be part of the safety systems and shall meet the requirements of IEEE Std 497-1981."

U.S. EPR FSAR Tier 2, Section 7.1.2.6.19 states: "The safety systems meet the requirements of Clause 5.8 of IEEE Std 603-1998. Displays and controls are provided by the SICS for those manual actions described in Section 15.0. The displays meet the requirements of IEEE Std 497-2002." Therefore, AREVA NP believes that compliance with Clause 5.8.1 is adequately addressed.

U.S. EPR FSAR Tier 2, Section 7.1.2.6.29 describes compliance with IEEE 603-1998 Clause 6.2.b. AREVA NP acknowledges that Section 7.1.2.6.29 provides reference to Section 7.3 for manual controls credited in the accident analyses, and that Section 7.3 does not specifically acknowledge manual actions credited in the accident analysis. Therefore, section 7.3 will be revised to clarify this point.

Part 2:

As described in U.S. EPR FSAR Tier 2, Sections 15.0.0.3.7 and 15.6.3, the plant safety analysis credits manual action to mitigate a design basis SGTR.

The U.S. EPR protection system design does include an automatic function to isolate a steam generator (SG) in case of tube rupture, as described in U.S. EPR FSAR Tier 2, Section 7.3.

As described in U.S. EPR FSAR Tier 2, Chapter 15, the design basis SGTR progresses relatively slowly and does not require mitigation within the first 30 minutes following occurrence of the rupture. The automatic SG isolation function is acknowledged in U.S. EPRFSAR Tier 2, Section 15.6.3.1 which states, "Although high activity in a steam line (or high SG level) in combination with the initiation of partial cooldown isolates the affected SG, this function is not credited in the SGTR analysis." The decision to not credit the automatic isolation function is conservative and takes into account the following:

- The nature of the event (slow progression and the range of possible plant responses) makes it difficult to determine exactly when the automatic function would be actuated.
- If the automatic function were to initiate prior to 30 minutes, the event results are more favorable.
- The slow progression of the event allows credit to be taken for manual actions after 30 minutes.

The key action required to mitigate the consequences of the SGTR is to isolate the affected steam generator and establish pressure equilibrium between the affected steam generator and the reactor coolant system. As noted above, the U.S. EPR design includes an automatic feature that performs the steam generator isolation in the presence of either a steam line high activity or high steam level coincident with the initiation of partial cooldown. A Safety Injection (SI) signal initiates partial cooldown. The high activity signal under potential scenarios varies as does the timing of SI in each scenario. For example, if the CVCS continues to function, it can provide sufficient make-up for the loss of inventory through the ruptured tube. In this case the operator follows the emergency operating procedures to manually trip the reactor or maneuver the plant through a controlled shutdown. Under this condition, although the high steam line activity signal may be present, SI or high steam generator level may be significantly delayed, resulting in a delay to isolate the affected steam generator and challenging offsite dose limits. In contrast, if CVCS is not available the reactor automatically trips following the SGTR and a SI signal occurs shortly after reactor trip. The SI signal initiates partial cooldown and in combination with high steam line high activity automatically isolates the affected steam generator. The single failure evaluated (e.g. stuck open MSRT) could also impact the timing of SI.

Credit for operator action removes the uncertainty associated with the timing of the high steam line activity signal and coincident functions required to isolate the affected steam generator for the range of possible plant response. Maintaining credit for operator action provides consistency of response for the range of possible scenarios and is consistent with guidelines established in the industry for SGTR events

FSAR Impact:

U.S. EPR FSAR, Tier 2, Sections 7.3.1, 7.3.1.1, and 7.3.2.1.4 will be revised as described in the response and indicated on the enclosed markup.

Question 07.04-11:

Follow-up to RAI Question No. 07.04-4.

Describe the design of remote shutdown station (RSS) control transfer switches to address guidance in 10 CFR Part 50, Appendix A, General Design Criteria 3? Where are they located relative to the main control room (MCR) and the RSS to provide accessibility during evacuation of the MCR? Can the common database for the MCR and the RSS be affected by fire?

GDC 3 and RG 1.189 address fire protection. GDC 3 requires systems important to safety to be “designed and located to minimize, consistent with other safety requirements, the probability and effect of fires and explosions.” DC FSAR Section 7.4 describes the function of the control transfer switches and their location in a separate fire zone that the MCR. However, additional detail is required to address the safety requirements related to fire as addressed by these criteria.

Response to Question 07.04-11:

The RSS control transfer switches maintain divisional independence, so that an electrical failure in one safety division cannot affect another safety division. Additionally, the RSS control transfer means cannot be disabled by a single active failure coincident with a loss of offsite power. Access to the RSS control transfer switches results in annunciation of an alarm in the Main Control Room (MCR). This information is found in U.S. EPR FSAR Tier 2, Section 7.4.1.3.4.

The RSS transfer means are located in a separate fire area from the MCR to allow transfer of control without entry into the MCR, as stated in U.S. EPR FSAR Tier 2, Section 7.4.2.3.

As described U.S. EPR FSAR Tier 2, Section 7.4.2.3. the transfer switches also provide isolation between the RSS and the MCR. Therefore, no single credible event will cause the MCR to be evacuated and cause the RSS to malfunction.

The requirements of GDC 3 and the guidance of RG 1.189 are thus addressed.

The common database for the MCR and the RSS cannot be affected by fire due to the redundancy of the equipment and the location separate from the MCR and RSS.

Inspections, tests, analyses, and acceptance criteria have been added to U.S. EPR FSAR Tier 1, Sections 2.4.2 and 2.4.10 to verify that the transfer switches exist in a fire area separate from the MCR for evacuation of the MCR.

FSAR Impact:

U.S. EPR FSAR, Tier 1, Section 2.4.2 and 2.4.10 will be revised as described in the response and indicated on the enclosed markup.

Question 07.04-13:

Follow-up to RAI Question No. 07.04-9.

Update the U.S. EPR DC-FSAR to include the quoted portion of the RAI response to Question 07.04-9 (included below). Define the word “significantly” as used in RAI responses to Questions 07.04-9 and 07.07-8 when stating, “data on PICS differs significantly from data on SICS.” Also, provide further detail on operator surveillance of the Plant Information and Control System (PICS) versus the Safety Information and Control System (SICS) to ensure operability.

10 CFR Part 50, Appendix A, General Design Criteria 13, addresses I&C issues relating to anticipated ranges for both normal and accident conditions. An update to the FSAR to include the quoted response below clearly defines the SICS as the credited human-system interface (HSI) system and provisions for addressing and identifying PICS failures. Staff finds that including this portion of the response in the FSAR is important in addressing the requirements. The RAI response below provides criteria of identifying faults in the PICS and should be included in the DC-FSAR:

Portion of AVERA NP’s response to RAI Question 07.04-9

“SICS is safety-related and is designed and qualified in accordance with IEEE Class 1E standards. The PICS is a non-safety-related system. The main difference between achieving safe shutdown from the different HSI systems is that more non-safety-related plant equipment can be operated from the PICS. The SICS includes the basic functional capabilities for the operator to monitor plant conditions and control appropriate plant systems to perform the credited safe shutdown path. However, more flexibility in the path to safe shutdown is available from the PICS due to the increase in HSI for both safety-related and non-safety-related systems.

Failures in PAS will be indicated on PICS. PAS failures resulting in the unavailability of the PICS need not be distinguished from failures in PICS resulting in the unavailability of PICS. The PICS will be used in all plant conditions, as long as it is available. The PICS is declared unavailable if less than two of the four operator workstations are in an available condition. A PICS workstation is declared unavailable if one or more of the following conditions exist:

- Three or more monitors at a workstation are unusable. The workstation in the Shift Supervisor office is not considered an operator workstation.
- Data communication is not working satisfactorily (i.e., expected feedback not received in the expected timeframe or inputs do not respond in the expected manner).
- Correlating information on PICS displays at the different workstations is not consistent.
- Information on PICS displays and relevant SICS indications are not consistent (i.e., data on PICS differs significantly from data on SICS).
- Operators will respond to these issues by procedure and training and will be alerted to perform the above verifications by the features on PICS that:

- Inform an operator through alarms or status indicators when individual or multiple data is not valid.
- Inform an operator through alarms or status indicators that critical I&C hardware is not working properly.
- Inform an operator through alarms or status indicators when system logic has not produced the expected results."

In addition to including the portion of the RAI response, describe what is considered to be significant data differences between PICS and SICS. Also; operators are alerted to PICS failures due to alarms and status indicators, which is an acceptable means for identification of a PICS failure. However, the identification mechanism should include periodic surveillance between PICS and SICS for such events as display freeze, etc.

Response to Question 07.04-13:

U.S. EPR FSAR Tier 2, Section 18.7.1.2.2 will be updated to include the requested information.

The word "significantly" in the statement: "data on PICS differs significantly from data on SICS" refers to a numerical value of deviation between corresponding data displayed on PICS and SICS that is unacceptable (i.e., significant difference between primary system pressure values being displayed simultaneously on both the SICS and PICS).

The PICS is normally used by the operator to monitor and control process systems, and SICS is used in the unlikely event that the PICS is not available. During normal operating conditions, the status of plant operation is displayed on both the PICS and SICS, which allows for verification that the information displayed is consistent.

There are two mechanisms that prompt a manual comparison of data on PICS and SICS to verify consistency.

1. A periodic verification will be performed as part of normal operating procedures to verify consistency between PICS and SICS. The frequency of this verification will be determined through analysis.
2. If, while performing operations from PICS, an operator detects a potential error in data displayed by PICS, the operator will perform a comparison of data between PICS and SICS. This comparison will be performed by employing the same procedure used for periodic verification of consistency. If an acceptable deviation value is exceeded, then operators will discontinue use of the PICS and a transfer to SICS will be initiated. The acceptable deviation value is specified in the procedure.

In addition to the manual verifications described above, automated features will be capable of detecting failures within the PICS. These features include self-checks on data quality for the PICS displays. If an error is detected, alarms and indications will be provided to the operator. Additionally, a "heartbeat" indication will be displayed on PICS to indicate failures such as processor lock-up or inactive communications that could result in frozen or inaccurate display information.

FSAR Impact:

U.S. EPR FSAR, Tier 2, Section 18.7.1.2.2 will be revised as described in the response and indicated on the enclosed markup.

U.S. EPR Final Safety Analysis Report Markups

Table 2.4.1-79—Protection System ITAAC (5-12 Sheets)

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
<p>4.23 <u>The PS hardware and software are designed to conform to the key TELEPERM XS principles, features, and quality methods.</u></p>	<p><u>A TELEPERM XS platform changes analysis will be performed on the PS hardware and software to verify its conformance to the key TELEPERM XS principles, features, and quality methods.</u> {}DAC{}</p>	<p><u>A report exists and concludes that the PS hardware modules and system software modules:</u> A report exists and concludes that the PS hardware and software are designed to conform to the key TELEPERM XS principles, features, and methods. {}DAC{}</p> <p>a. <u>Conform to the key TELEPERM XS design principles.</u> {}DAC{}</p> <p>b. <u>Conform to the key TELEPERM XS processing features.</u> {}DAC{}</p> <p>c. <u>Conform to the key TELEPERM XS communication independence features.</u> {}DAC{}</p> <p>d. <u>Do not introduce more than a minimal increase in the likelihood of occurrence of a software malfunction relative to predecessor modules.</u> {}DAC{}</p> <p>e. <u>Do not introduce more than a minimal increase in the consequences of a malfunction relative to predecessor modules.</u> {}DAC{}</p> <p>f. <u>Do not create the possibility for a malfunction with a different result relative to predecessor modules.</u> {}DAC{}</p>

07.01-16

Table 2.4.1-79—Protection System ITAAC (5-12 Sheets)

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
<p>4.24 <u>The PS response time for RT and ESF signals is less than the value required to satisfy the design basis safety analysis response time assumptions.</u></p>	<p>a. <u>Analyses will be performed to determine the required response time from sensor to ALU output, including sensor delay, which supports the safety analysis response time assumptions for the RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3.</u></p> <p>b. <u>Tests, analyses, or a combination of tests and analyses will be performed on the PS equipment that contributes to RT and ESF signal response times.</u></p>	<p>g. <u>Were developed according to procedures that do not result in a reduction in the TELEPERM XS quality methods.</u> {{DAC}}</p> <p>a. <u>A report exists and identifies the required response time from sensor to ALU output which supports the safety analysis response time assumptions for the RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3.</u></p> <p>b. <u>A report exists and concludes that PS response times from sensor to ALU output support the safety analysis response time assumptions for the RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3.</u></p>
<p>5.1 The Class 1E PS components identified as Class 1E in Table 2.4.1-1 are powered from the a Class 1E division as listed in Table 2.4.1-1 in a normal or alternate feed condition.</p>	<p>a. Testing will be performed for components identified as Class 1E in Table 2.4.1-1 by providing a test signal in each normally aligned division.</p> <p>b. Testing will be performed for components identified as Class 1E in Table 2.4.1-1 by providing a test signal in each division with the alternate feed aligned to the divisional pair.</p>	<p>a. The test signal provided in the normally aligned division is present at the respective Class 1E components identified in Table 2.4.1-1.</p> <p>b. The test signal provided in each division with the alternate feed aligned to the divisional pair is present at the respective Class 1E components identified in Table 2.4.1-1.</p>

07.01-16



g. Were developed according to procedures that do not result in a reduction in the TELEPERM XS quality methods.
{{DAC}}

2.4.2 Safety Information and Control System

1.0 Description

The safety information and control system (SICS) provides the human-machine interface (HMI) means to perform control and information functions needed to monitor the plant safety status and bring the unit to and maintain it in a safe shutdown state in case of the inoperability of the process information and control system (PICS).

In case of the unavailability of the PICS, the SICS provides the following safety related functions:

- Manual actuation of reactor trip in the main control room (MCR) and remote shutdown station (RSS).
- Manual actuation of engineered safety features (MCR only).
- Monitoring and control of systems required to achieve and maintain safe shutdown (MCR ~~and RSS~~).
- Display of Type A through Type C post-accident monitoring variables (MCR only).

2.0 Arrangement

2.1 ~~The location of the~~ SICS equipment is located as listed in Table 2.4.2-1—Safety Information and Control System Equipment.

2.2 Deleted.

3.0 Mechanical Design Features

3.1 Equipment identified as Seismic Category I in Table 2.4.2-1 can withstand seismic design basis loads without loss of safety function.

4.0 I&C Design Features, Displays and Controls

07.04-11



4.1 The capability to transfer control of the SICS from the MCR to the RSS exists in a fire area separate from the MCR. The transfer switches are each associated with a single division of the safety-related control and allow transfer of control without entry into the MCR.

4.2 Deleted.

4.3 Electrical isolation is provided on connections between the ~~safety~~ ~~safety~~-related parts of the SICS and ~~the non-Class 1E equipment, safety I&C systems.~~

4.4 ~~The Class 1E~~ SICS equipment ~~classified as Class 1E in Table 2.4.2-1~~ can perform its safety function when subjected to electromagnetic interference (EMI), radio-frequency interference (RFI), electrostatic discharges (ESD), and power surges.

**Table 2.4.2-2—Safety Information and Control System ITAAC
(4-8 Sheets)**

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.1	The location of the SICS equipment is <u>located</u> as listed in Table 2.4.2-1.	Inspection will be performed of the location of the <u>SICS</u> equipment.	The <u>SICS</u> equipment listed in Table 2.4.2-1 is located as listed in Table 2.4.2-1.
2.2	Deleted.	Deleted.	Deleted..
3.1	Equipment identified as Seismic Category I in Table 2.4.2-1 can withstand seismic design basis loads without loss of safety function.	a. Type tests, analyses or a combination of type tests and analyses will be performed on the equipment listed as Seismic Category I in Table 2.4.1-1 using analytical assumptions, or under conditions, which bound the Seismic Category I design requirements. b. Inspections will be performed of the as-installed Seismic Category I equipment listed in Table 2.4.2-1 to verify that the equipment including anchorage is installed as specified on the construction drawings.	a. Tests/analysis reports exist and conclude that the equipment listed as Seismic Category I in Table 2.4.1-1 can withstand seismic design basis loads without loss of safety function. b. Inspection reports exist and conclude that the as-installed Seismic Category I equipment listed in Table 2.4.2-1 including anchorage is installed as specified on the construction drawings.
4.1	The capability to transfer control of the SICS from the MCR to the RSS exists <u>in a fire area separate from the MCR. The transfer switches are each associated with a single division of the safety-related control and allow transfer of control without entry into the MCR.</u>	a. Inspections will be performed to verify the existence of procedures. b. Tests will be performed to verify that control of the SICS can be transferred from the MCR to the RSS. c. <u>An inspection will be performed to verify the existence of the SICS RSS transfer switches in a fire area separate from the MCR, each associated with a single division of the safety-related control.</u>	a. A report exists and concludes that procedures exist for transfer of control of the SICS from the MCR to the RSS. b. A report exists and concludes that the test results confirm that control of the SICS can be transferred from the MCR to the RSS. c. <u>Transfer switches exist in a fire area separate from the MCR, each associated with a single division of the safety-related control.</u>

07.04-11

**Table 2.4.2-2—Safety Information and Control System ITAAC
(4-8 Sheets)**

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
		<p>b. <u>Tests will be performed to verify the proper operation of the locking mechanisms on the SICS cabinet doors located outside of the MCR.</u></p>	<p>b. <u>The locking mechanisms on the SICS cabinet doors located outside of the MCR operate properly.</u></p>
		<p>c. <u>Tests and inspections will be performed to verify an indication exists in the MCR when a SICS cabinet door located outside of the MCR is in the open position.</u></p>	<p>c. <u>Opened SICS cabinet doors located outside of the MCR are indicated in the MCR.</u></p>
4.13	<p><u>Key lock switches on the QDS restrict connections between the QDS and the QDS service unit.</u></p>	<p><u>Tests will be performed to verify that the key lock switches on the QDS restrict modifications to the SICS software.</u></p>	<p><u>Key lock switches on the QDS restrict modifications to the SICS software.</u></p>
4.14	<p><u>The SICS is capable of performing its safety function when one of the SICS divisions is out of service. Out of service divisions of SICS are indicated in the MCR.</u></p>	<p>a. <u>A test of the SICS will be performed to verify the SICS can perform its safety function when one of the SICS divisions is out of service.</u></p> <p>b. <u>Inspections will be performed to verify the existence of indications in the MCR when a SICS division is placed out of service.</u></p>	<p>a. <u>The SICS can perform its safety functions when one of the SICS divisions is out of service.</u></p> <p>b. <u>Out of service divisions of SICS are indicated in the MCR.</u></p>
4.15	<p><u>The SICS hardware and software are designed to conform to the key TELEPERM XS principles, features, and quality methods.</u> {{DAC}}</p>	<p><u>A TELEPERM XS platform changes analysis will be performed on the SICS hardware and software to verify its conformance to the key TELEPERM XS principles, features, and quality methods.</u> {{DAC}}</p>	<p><u>A report exists and concludes that the PS hardware modules and system software modules:</u> <u>A report exists and concludes that the SICS hardware and software are designed to conform to the key TELEPERM XS principles, features, and methods.</u> {{DAC}}</p>

↑
07.01-16

Table 2.4.2-2—Safety Information and Control System ITAAC
(4-8 Sheets)

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
		<p>a. <u>Conform to the key TELEPERM XS design principles.</u> {{DAC}}</p> <p>b. <u>Conform to the key TELEPERM XS processing features.</u> {{DAC}}</p> <p>c. <u>Conform to the key TELEPERM XS communication independence features.</u> {{DAC}}</p> <p>d. <u>Do not introduce more than a minimal increase in the likelihood of occurrence of a software malfunction relative to predecessor modules.</u> {{DAC}}</p> <p>e. <u>Do not introduce more than a minimal increase in the consequences of a malfunction relative to predecessor modules.</u> {{DAC}}</p> <p>f. <u>Do not create the possibility for a malfunction with a different result relative to predecessor modules.</u> {{DAC}}</p> <p>g. <u>Were developed according to procedures that do not result in a reduction in the TELEPERM XS quality methods.</u> {{DAC}}</p>

↑
07.01-16

Table 2.4.4-5—Safety Automation System ITAAC (3-9 Sheets)

Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
<p>4.16 <u>The SAS hardware and software are designed to conform to the key TELEPERM XS principles, features, and quality methods.</u> }} </p>	<p><u>A TELEPERM XS platform changes analysis will be performed on the SAS hardware and software to verify its conformance to the key TELEPERM XS principles, features, and quality methods.</u> }} </p>	<p><u>A report exists and concludes that the PS hardware modules and system software modules:</u> A report exists and concludes that the SAS hardware and software are designed to conform to the key TELEPERM XS principles, features, and methods. }}</p> <p>a. <u>Conform to the key TELEPERM XS design principles.</u> }}</p> <p>b. <u>Conform to the key TELEPERM XS processing features.</u> }}</p> <p>c. <u>Conform to the key TELEPERM XS communication independence features.</u> }}</p> <p>d. <u>Do not introduce more than a minimal increase in the likelihood of occurrence of a software malfunction relative to predecessor modules.</u> }}</p> <p>e. <u>Do not introduce more than a minimal increase in the consequences of a malfunction relative to predecessor modules.</u> }}</p> <p>f. <u>Do not create the possibility for a malfunction with a different result relative to predecessor modules.</u> }}</p>

07.01-16



Table 2.4.4-5—Safety Automation System ITAAC (3-9 Sheets)

Commitment Wording		Inspections, Tests, Analyses	Acceptance Criteria
5.1	<p>The Class 1E SAS components identified as Class 1E in Table 2.4.4-1 are powered from the a Class 1E division as listed in Table 2.4.4-1 in a normal or alternate feed condition.</p>	<p>07.01-16 →</p> <p>a. Testing will be performed for components identified as Class 1E in Table 2.4.4-1 by providing a test signal in each normally aligned division.</p> <p>b. Testing will be performed for components identified as Class 1E in Table 2.4.4-1 by providing a test signal in each division with the alternate feed aligned to the divisional pair.</p>	<p><u>g. Were developed according to procedures that do not result in a reduction in the TELEPERM XS quality methods.</u> {{DAC}}</p> <p>a. The test signal provided in the normally aligned division is present at the respective Class 1E components identified in Table 2.4.4-1.</p> <p>b. The test signal provided in each division with the alternate feed aligned to the divisional pair is present at the respective Class 1E components identified in Table 2.4.4-1.</p>

2.4.10 Process Information and Control System

1.0 Description

The process information and control system (PICS) is a digital human machine interface (HMI). It provides monitoring and control of plant systems. The PICS is non-~~safety~~ safety-related and is provided in both the main control room (MCR) and the remote shutdown station (RSS).

2.0 I&C Design Features

2.1 The system hardware and software in the PICS is diverse from the safety-related system hardware and software in the Safety Information and Control System (SICS).

2.2 Deleted.

2.3 Deleted.

2.4 Electrical isolation is provided on PICS connections between the RSS and the MCR ~~for the PICS~~.

2.5 The capability to transfer control of the PICS from the MCR to the RSS exists in a fire area separate from the MCR and allows transfer of control without entry into the MCR.

3.0 System Inspections, Tests, Analyses, and Acceptance Criteria

Table 2.4.10-~~1~~2 lists the PICS ITAAC.

07.04-11



**Table 2.4.10-1—Process Information and Control System
ITAAC (2 Sheets)**

	Commitment Wording	Inspections, Tests, Analyses	Acceptance Criteria
2.5	<p><u>The capability to transfer control of the PICS from the MCR to the RSS exists in a fire area separate from the MCR and allows transfer of control without entry into the MCR.</u></p>	<p>a. <u>Inspections will be performed to verify the existence of procedures.</u></p> <p>b. <u>Tests will be performed to verify that control of the PICS can be transferred from the MCR to the RSS.</u></p> <p>c. <u>An inspection will be performed to verify the existence of the PICS RSS transfer means in a fire area separate from the MCR.</u></p>	<p>a. <u>A report exists and concludes that procedures exist for transfer of control of the PICS from the MCR to the RSS.</u></p> <p>b. <u>A report exists and concludes that the test results confirm that control of the PICS can be transferred from the MCR to the RSS.</u></p> <p>c. <u>Transfer means exist in a fire area separate from the MCR.</u></p>

07.04-11



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 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.

7.1.1.2.1 TXS Platform Design

07.01-16

The TXS platform is described in the Reactor Protection System Topical Report (EMF-2110(NP)(A) (Reference 6). Because of advances in technology and rapid obsolescence of components, the various modules described in EMF-2110(NP)(A) (Reference 6) will be modified and upgraded over time, and new modules will be

developed. ~~However, the principles and methods described in EMF-2110(NP)(A) (Reference 6) and summarized below apply to the application of the TXS platform for the U.S. EPR.~~

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, SAS and SICS 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 5) 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 nodules conform to the key TXS principles, features, and methods.

The U.S. EPR-specific I&C system architectures that will be implemented using TXS hardware and software are described in Section 7.1 for NRC review against the current

07.01-16

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.

- ~~Platform design using four building blocks, which include:~~
 - ~~System hardware.~~
 - ~~System software.~~
 - ~~Application software.~~
 - ~~Engineering tools to configure the application.~~
- ~~System hardware, system software, and engineering tools development processes that meet the quality requirements of 10 CFR 50.55a(a)(1) and GDC 1. This includes software verification and validation (V&V) methods.~~
- ~~Processing principles that provide for system integrity, which include:~~
 - ~~Real-time, static operating system.~~
 - ~~Cyclic processing.~~
 - ~~Interference-free communications.~~
 - ~~Self-monitoring and diagnostics.~~
 - ~~Fail-safe design.~~
- ~~Control of access principles, including service unit (SU) maintenance interfaces.~~

~~The TXS product family also extends to other modules and components outside of those described in EMF-2110(NP)(A) (Reference 6). Examples include the priority module described in AV42 Topical Report (ANP-10273P) (Reference 7), and the qualified display system (QDS). The QDS is a video display unit designed for use in nuclear safety-related applications. Modules and components that are developed for use in I&C systems design shall be consistent with the requirements described in this chapter.~~

7.1.1.2.2 Application of the TXS Platform

TELEPERM XS Software Topical Report (ANP-10272) (Reference 8) describes the lifecycle processes for application software development used in safety-related applications of the TXS platform for the U.S. EPR, as well as software V&V processes. These phases are listed below along with the primary documentation generated at the end of each phase:

- Basic design phase:

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 0¹, "Software Program Manual TELEPERM XS™ Safety Systems," AREVA NP Inc., ~~December 2006~~ August 2009.
6. ANP-~~10281~~10309P, Revision 0, "U.S. EPR Digital Protection System ~~Topical~~Technical Report," AREVA NP Inc., ~~March 2007~~November 2009.
7. ANP-10287P, Revision 0, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," AREVA NP Inc., November 2007.
8. ~~ANP-10284, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007~~ ANP-10304P, Revision 1, "U.S. EPR Diversity and Defense-In-Depth Assessment Topical Report," AREVA NP Inc., November 2009.
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.

07.01-16



5. ANP-10272, Revision 0¹, "Software Program Manual TELEPERM XS™ Safety Systems," AREVA NP Inc., ~~December 2006~~ August 2009.

6. ANP-~~10281~~10309P, Revision 0, "U.S. EPR Digital Protection System ~~Topical~~Technical Report," AREVA NP Inc., ~~March 2007~~November 2009.

7. ANP-10287P, Revision 0, "Incore Trip Setpoint and Transient Methodology for U.S. EPR Topical Report," AREVA NP Inc., November 2007.

8. ~~ANP-10284, Revision 0, "U.S. EPR Instrumentation and Controls Diversity and Defense-in-Depth Methodology Topical Report," AREVA NP Inc., June 2007~~ ANP-10304P, Revision 1, "U.S. EPR Diversity and Defense-In-Depth Assessment Topical Report," AREVA NP Inc., November 2009.

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.

7.3 Engineered Safety Features Systems

7.3.1 Description

The U.S. EPR provides safety-related instrumentation and controls to sense accident conditions and automatically initiate the engineered safety features (ESF) systems. ESF systems are automatically actuated when selected variables exceed setpoints that are indicative of conditions that require protective action. Additionally, the ability to manually initiate ESF systems is provided in the main control room (MCR). Manual

07.03-27

system-level actuation of ESF systems initiates all actions performed by the corresponding automatic actuation, including starting auxiliary or supporting systems and performing required sequencing functions. Component-level control ESF system actuators is also provided in the MCR.

7.3.1.1 System Description

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

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

Actuation orders are sent from the PS to the PACS priority module associated with each actuator required for the function. Exceptions to this are the emergency diesel generator (EDG) start function and the turbine trip function. These actuation orders are received by the associated control system (EDG or turbine controls) and do not involve the PACS module. The PS and the PACS are discussed in Section 7.1.

The safety automation system (SAS) performs closed loop automatic controls of certain ESF systems following their actuation by the PS. These controls are described in Section 7.3.1.2 with their associated actuation functions. The SAS is described in Section 7.1.

The capability for manual system-level ESF actuations is available to the operator through the safety information and control system (SICS) in the MCR. These manual actuations ~~either~~ are acquired by the ALUs in the protection system and combined with the automatic actuation logic, ~~or are implemented to bypass the computerized portions of the protection system.~~ The manual actuations are described with the corresponding automatic function in Section 7.3.1.2.

07.03-27

07.03-27

The capability for component-level control of ESF system actuators is available to the operator on both the PICS and the SICS. Commands from the PICS are processed by the PAS and sent to the PACS for prioritization. Commands from the SICS are processed by the SAS and sent to the PACS for prioritization. For any ESF actuator commands from the SICS have priority over those from the PICS.

The capability for manual reset of sense and command ESF actuation outputs is provided on both the process information and control system (PICS) and the SICS. Not all ESF actuations require a manual reset. There are cases where a sense and command output is cleared after the PS determines that the initiating condition has cleared. The reset functionality related to each ESF actuation is described in Section 7.3.1.2. Further description of the operation of the PICS and SICS is presented in Section 7.1.

7.3.1.2 Engineered Safety Features Actuation Functional Descriptions

7.3.1.2.1 Safety Injection System Actuation

To mitigate a loss of coolant accident (LOCA) or overcooling event, a safety injection signal is required to actuate the appropriate ESF and support systems and to isolate non-qualified reactor coolant system (RCS) piping.

In case of a decrease in RCS water inventory due to a LOCA, the RCS is supplied by medium head safety injection (MHSI) in the high pressure phase of the event and low head safety injection (LHSI) in the low pressure phase.

In case of an overcooling event, boron addition via MHSI can offset positive reactivity insertion if the RCS pressure decreases below the shut-off head of the MHSI pumps.

The operation of the MHSI and LHSI systems is described in Section 6.3.

either directly or as inputs to a calculation to actuate an ESF system. The range to be monitored for each of these variables is also listed in Table 7.3-1.

7.3.2.1.4 Design Basis: Manual ESF System Actuation (Clause 4.e of IEEE Std 603-1998)

07.03-27

The capability for manual system-level actuation and manual component level control of ESF actuators is available to the operator as described in Section 7.3.1.1. Manual actions credited to mitigate design basis events are identified in Section 15.0. ~~The capability for manual system level actuation of ESF functions is available to the operator as described in Section 7.3.1.1. The function-specific implementation of system level actuation is described for each function in Section 7.3.1.2.1 through Section 7.3.1.2.17.~~ The variables to be displayed to the operator to use in manual ESF actuation are determined as part of the methodology used for selecting Type A variables as described in Section 7.5.

7.3.2.1.5 Design Basis: Spatially Dependent Variables (Clause 4.f of IEEE Std 603-1998)

The U.S. EPR design uses no spatially dependent variables as inputs to ESF actuation functions.

7.3.2.1.6 Design Basis: Critical Points in Time or Plant Conditions (Clause 4.j of IEEE Std 603-1998)

The PS initiates operation of ESF systems when selected variables exceed the associated setpoints. The plant conditions that define the proper completion of the safety function performed by an ESF system are defined on an event-by-event basis in the Chapter 15 analyses. The actions of the execute features for an ESF actuation function are complete when, for example, a valve has reached its full open or full closed position, or required flow has been established by a pump.

The ESF actuation logic generally allows ESF actuation outputs generated by the PS to be reset after completion of the actions of the execute features. The reset of the ESF actuation signal does not result in change of state (return to normal) of the ESF actuator. Plant specific operating procedures govern the point in time when the ESF actuators can be returned to normal following their actuation.

7.3.2.2 Failure Modes and Effects Analysis

A system-level failure modes and effect analysis (FMEA) is performed on the PS to identify potential single point failures and their consequences. The architecture of the PS as defined in the U.S. EPR Digital Protection System ~~Topical~~ Technical Report (Reference 1) is used as the basis for the analysis. The FMEA considers each major part of the system, how it may fail, and the effect of the failure on the system.

For the U.S. EPR, each division of safety-related mechanical and electrical components has its own safety-related screen-based HSI (i.e., qualified display system (QDS)). A minimum of four separate QDSs are used to control the four trains of safety-related components. A dedicated QDS capable of receiving all four trains of data is used to give the operator an overview of the plant. The dedicated overview QDS is for monitoring only, with one way communication, and cannot impact the plant. See Section 7.1.1.2.1 for more information on safety-related HSI.

18.7.1.2.1 Alarm Management Hierarchy

The alarms on the PICS are prioritized into levels. The PICS provides the ability to display, record, and acknowledge alarms and warnings that are necessary for the operators. A color scheme is associated with the prioritization of the alarm to inform the operator of the nature of the alarm and the priority level. The operator uses the alarm text to view alarm details. A direct navigation link associated with the alarm is also available to the operator. Direct navigation links are used along with the alarm management system to allow the operator quick access to related information and controls.

~~For high alarm priority functions, grouped alarm annunciation is also provided on the safety information and control system (SICS).~~

18.7.1.2.2 Loss of Non-Safety Computerized HSIs

The U.S. EPR is normally controlled from PICS, the non-safety HSI. An independent safety-related HSI back-up, SICS, provides the ability to control and monitor the plant for a limited amount of time to keep it in a safe and steady power condition. If PICS is not available or directly recoverable, the plant is shut down. The SICS consists of QDSs and selected hardwired controls and alarms. The QDS is also safety qualified for controlling and monitoring the plant.

07-04-13

SICS is safety-related and is designed and qualified in accordance with IEEE Class 1E standards. The PICS is a non-safety-related system. The main difference between achieving safe shutdown from the different HSI systems is that more non-safety-related plant equipment can be operated from the PICS. The SICS includes the basic functional capabilities for the operator to monitor plant conditions and control appropriate plant systems to perform the credited safe shutdown path. However, more flexibility in the path to safe shutdown is available from the PICS due to the increase in HSI for both safety-related and non-safety-related systems.

Failures in PAS will be indicated on PICS. PAS failures resulting in the unavailability of the PICS need not be distinguished from failures in PICS resulting in the unavailability of PICS. The PICS will be used in all plant conditions, as long as it is available. The PICS is declared unavailable if less than two of the four operator

07-04-13 →

workstations are in an available condition. A PICS workstation is declared unavailable if one or more of the following conditions exist:

- Three or more monitors at a workstation are unusable. The workstation in the Shift Supervisor office is not considered an operator workstation.
- Data communication is not working satisfactorily (i.e., expected feedback not received in the expected timeframe or inputs do not respond in the expected manner).
- Correlating information on PICS displays at the different workstations is not consistent.
- Information on PICS displays and relevant SICS indications are not consistent (i.e., data on PICS differs significantly from data on SICS).

Operators will respond to these issues by procedure and training and will also be alerted to perform the above verifications by the features on PICS that:

- Inform an operator through alarms or status indicators when individual or multiple data is not valid.
- Inform an operator through alarms or status indicators that critical I&C hardware is not working properly.
- Inform an operator through alarms or status indicators when system logic has not produced the expected results.

The PICS is normally used by the operator to monitor and control process systems, and SICS is used in the unlikely event that the PICS is not available. During normal operating conditions, the status of plant operation is displayed on both the PICS and SICS, which allows for verification that the information displayed is consistent.

There are two mechanisms that prompt a manual comparison of PICS and SICS to verify consistency.

- A periodic verification will be performed as part of normal operating procedures to verify consistency between PICS and SICS.
- If, while performing operations from PICS, an operator detects a potential error in data displayed by PICS, the operator will perform a comparison of data between PICS and SICS. This comparison will be performed by employing the same procedure used for periodic verification of consistency. If an acceptable deviation value is exceeded, then operators will discontinue use of the PICS and a transfer to SICS will be initiated. The acceptable deviation value is specified in the procedure.

~~Section 4.3.1.1 of Reference 2 describes the criteria to determine PICS availability.—
The operator verifies PICS data against SICS data when necessary.—~~The PICS also has status lights indication to assist the operators in determining availability. ~~The operator~~