

## ArevaEPRDCPEm Resource

---

**From:** Pederson Ronda M (AREVA NP INC) [Ronda.Pederson@areva.com]  
**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  
**Attachments:** RAI 285 Response US EPR DC.pdf

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](mailto: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:** 949

**Mail Envelope Properties** (5CEC4184E98FFE49A383961FAD402D3101637C60)

**Subject:** Response to U.S. EPR Design Certification Application RAI No. 285, FSAR Ch. 7  
**Sent Date:** 11/11/2009 6:11:16 PM  
**Received Date:** 11/11/2009 6:11:18 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  
"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

<b>Files</b>	<b>Size</b>	<b>Date &amp; Time</b>
MESSAGE	3710	11/11/2009 6:11:18 PM
RAI 285 Response US EPR DC.pdf		152941

**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),  
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 07.01-12:**

Follow-up to RAI Question 07.01-3

In the U.S. EPR DC-FSAR, provide additional detail in Figure 7.1-2, "U.S. EPR I&C Architecture," to show the interfaces from Level 2 to Level 3, and show all of the systems that are categorized at Level 0. Additionally, provide corresponding updates to the U.S. EPR FSAR.

The staff reviewed the AREVA NP response to RAI 07.01-3, and found that a supplemental RAI is necessary. 10 CFR 52.47 states that a description shall be sufficient to permit understanding of the system designs. Although FSAR Section 7.1.1.1 states in part "... The U.S. EPR I&C architecture is represented in Figure 7.1-2 - U.S. EPR I&C Architecture. The overall I&C architecture is categorized into four levels ... Other than interfaces provided from Level 2, these systems are not within the scope of this document and are not shown on Figure 7.1-2." The staff found that the interfaces from Level 2 to Level 3, which are within the scope, are not shown in Figure 7.1-2. Detail is needed in Figure 7.1-2, "U.S. EPR I&C Architecture," that shows the interfaces from Level 2 to Level 3. Additionally, the staff found that there are systems described in Section 7.1 that are categorized as Level 0, but are not shown in Figure 7.1-2. Additional detail is needed in Figure 7.1-2 U.S. EPR I&C Architecture that shows all of the systems that are categorized at Level 0.

**Response to Question 07.01-12:**

A response to this question will be provided by December 18, 2009.

**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:**

A response to this question will be provided by January 22, 2010.

**Question 07.01-14:**

Follow-up to RAI Question 07.01-5

Provide information in Section 7.1 of the U.S. EPR DC-FSAR concerning the plant fire alarm system (PFAS) and the communication system, so that there are appropriate pointers to Sections 9.5.1 and 9.5.2, which describes the PFAS and the communication systems. Additionally, provide corresponding updates to the U.S. EPR FSAR.

The staff reviewed the AREVA NP response to RAI 07.01-5, and found that a supplemental RAI is necessary. This additional information is needed to provide clarification since 10 CFR 52.47 states that a description shall be sufficient to permit understanding of the system designs. While it is appropriate to have detailed discussion of the plant fire alarm system (PFAS) and the communication system in other sections of the FSAR, the staff did not find any discussion of the PFAS and the communication system in the U.S. EPR FSAR Section 7.1. There are several sections in Standard Review Plan (SRP) Chapter 7 that mention plant fire alarm system and communication systems.

**Response to Question 07.01-14:**

References to the PFAS and the communication system will be added to U.S. EPR FSAR Tier 2, Section 7.1.1.5.

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 7.1.1.5 will be revised as described in the response and indicated on the enclosed markup.

**Question 07.01-15:**

Follow-up to RAI Question 07.01-6

Provide revisions to Table 1.9-3 and include the missing Instrumentation and Controls (I&C) issues as discussed below. Also, provide detailed information as to how the I&C issues in Table 1.9-3 are addressed and include drawings as appropriate. Additionally, provide corresponding updates to the U.S. EPR FSAR.

10 CFR 52.47(a)(22) requires design certification applications to include information necessary to demonstrate how operating experience insights have been incorporated into the plant design. The staff reviewed the applicant's Table 1.9-3, as well as NUREG-0933 dated July 31, 2007. In the original RAI, the staff provided one example of a generic issue that was missing from the applicant's table. It is incumbent on the applicant to ensure inclusion of all the issues related to I&C; this information was not provided in the response to the original RAI 07.01-6. The staff identified that the following issues are missing from the applicant's Table 1.9-3. Additional information is needed on the following:

- Issue 3 – Set Point Drift In Instrumentation
- Issue 45 – Inoperability of Instrumentation Due to Extreme Cold Weather
- Issue 64 – Identification of Protection System Instrument Sensing Lines
- Issue 142 – Leakage Through Electrical Isolators in Instrumentation Circuits
- Issue 145 – Actions to Reduce Common Cause Failures
- Issue 160 – Spurious Actuations of Instrumentation Upon Restoration of Power
- Issue 161 – Use of Non-Safety Related Power Supplies in Safety-Related Circuits
- Issue 200 – Tin Whiskers

The applicant states, "During development of the U.S. EPR FSAR, additional generic issues were evaluated ... however, these are not included in the table since they were either ranked "resolved" or "drop." The applicant needs to include the generic issues in their Table 1.9-3 even if they are designated as "resolved generic issues." The applicant mentions the designations "medium and high priority." Per NUREG-0933, as of 1999, the use of the safety priority rankings was discontinued. Although an issue has been "dropped" as a generic issue, it is still an issue important to safety, and needs to be addressed. An example of an issue important to safety pertains to Issue 200, "Tin Whiskers." The staff notes that component failure due to tin whiskers have occurred at nuclear power plants, ranging in severity from spurious alarms and faulty signals in protection systems to reactor trips.

**Response to Question 07.01-15:**

A response to this question will be provided by January 22, 2010.

**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:**

A response to this question will be provided by January 22, 2010.

**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:**

A response to this question will be provided by January 22, 2010.

**Question 07.02-30:**

Follow-up to RAI 07.02-9

As a follow-up to RAI No. 07.02-9, provide an exemption request to redefine the terms "detectable failure" and "non-detectable failure." In addition, justify the reasons for re-defining the terms.

IEEE Std. 603-1991 defines detectable failures as failures that can be identified through periodic testing or can be revealed by alarm or anomalous indication. Component failures that are detected at the channel, division, or system level are detectable failures. Also, identifiable, but non-detectable failures are failures identified by analysis that cannot be detected through periodic testing or cannot be revealed by alarm or anomalous indication.

FSAR 7.2.2.2 states:

"When referring to the nature of single failure, the terms detected and undetected as used in the context of the Protection System (PS) Failure Modes and Effects Analysis (FMEA) do not correspond to the definition of a detectable failure in IEEE 603-1998. All of the failures denoted undetected in the FMEA are detectable through periodic testing. The terms detected and undetected, as used in the FMEA, refer to the ability of the PS to automatically detect a failure through self-surveillance."

Since the application is changing definitions in the regulations (10 CFR 50.55a(h)), an exemption request is required. In addition, the staff views failures that are handled by the PS self-surveillance features as those revealed by alarm or anomalous indication, even if the PS accommodates the failure. In such case, the staff assumes that the PS will at least provide an anomalous indication to operators if a failure is detected by self-surveillance features. If the assumption is incorrect, this should be noted to the staff. Therefore, it appears that the current IEEE Std. 603-1991 definition would accommodate self-surveillance features of the PS. Also, the application defines non-detectable failures as those that can be identified through periodic testing, but not through self-surveillance. What is the purpose for the redefinition of non-detectable failures in this manner? Does the applicant not plan to perform periodic testing to identify failures that fall into such category?

**Response to Question 07.02-30:**

IEEE 603-1998 defines the terms "detectable" and "undetectable." The PS FMEA summaries in U.S. EPR FSAR Tier 2, Section 7.2 and Section 7.3 use the terms "detected" and "undetected." Clarification is provided in those sections, and in the Response to RAI 75, Question 07.02-9, that these similar terms do not have the same meaning.

The terms "detected" and "undetected" are not defined in IEEE 603-1998. AREVA NP has not redefined or changed the definitions in IEEE 603-1998, and an exemption request is not required.

Detected failures in the PS provide an indication to operators that a failure has occurred.

U.S. EPR FSAR Tier 2, Chapter 16, Technical Specifications, Section 3.3.1 describes periodic testing that will be performed on the PS.

**FSAR Impact:**

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

**Question 07.02-31:**

Follow-up to RAI Questions No. 07.02-13 and 07.02-23.

For FSAR Tier 1, Table 2.4.1-7, ITAAC 4.2 is worded only for automatically-initiated actions. What about manually-initiated engineered safety features (ESF) actions?

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. Clause 5.2 of IEEE Std. 603-1991 states, in part, that the safety systems shall be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features shall continue until completion. Table 2.4.1-7, ITAAC 4.2 states that "the PS generates automatic ESF signals. Tests will be performed on the as-installed PS using test signals to verify that a ESF signal is generated for the input variables listed in Table 2.4.1.-3 when a test signal reaches the trip limit. The PS generates a ESF signal after the test signal reaches the trip limit for input variables listed in Table 2.4.1-3. The ESF signals remain following removal of the test signal. The ESF signals are removed when test signals that represent the completion of the ESF function are present. Deliberate operator action is required to return the PS to normal." To satisfy IEEE 603-1991, Clauses 5.2, the staff requires a Completion of Protection Action ITAAC for manually-initiated ESF actions.

**Response to Question 07.02-31:**

A response to this question will be provided by December 18, 2009.

**Question 07.03-21:**

Follow-up to RAI Question No. 07.03-2

Provide specific details on the design capabilities of the self-testing features, and their intended use to fulfill IEEE Std. 603-1991, Clauses 5.1 and 5.7, and Technical Specification surveillances as stated in U.S. EPR DC-FSAR, Section 7.3.

In U.S. EPR DC-FSAR Section 7.3.2.3.6, Revision 1, AREVA NP mentions the self-testing features of the PS as a means of satisfying IEEE Std. 603-1991, Clause 5.7. This is also consistent with Section 14.10 of the U.S. EPR Digital Protection System Topical Report (ANP-10281P). Also, in DC-FSAR Section 7.3.2.3.1, Revision 1, AREVA NP details that the failure modes and effects analysis (FMEA) shown in Tables 7.3-2, 7.3-3, and 7.3-4 are used to demonstrate compliance with IEEE Std. 603-1991, Clause 5.1, Single Failure Criterion. For the FMEA, AREVA NP defines "detected" and "non-detected" failures by the self-testing features' ability to find failures in the Protection System (PS). If AREVA NP intends to use the self-testing features to satisfy Clauses 5.1 and 5.7 of IEEE Std. 603-1991 and for Technical Specification surveillance testing, the staff requires additional detail on the abilities of the self-testing features, as well as AREVA NP's intended design usage for the self-testing features.

1. Does AREVA NP intend to take credit for self-testing features of the PS in order to satisfy IEEE Std. 603-1991, Clause 5.7?
2. What are the exact coverage capabilities of the self-testing features? Are the self-testing features intended to find all failures/faults, hardware or software, within the PS including instrument channels?
3. Does AREVA NP have operating experience that can demonstrate the reliability and capability of the self-testing features to detect failures over a given period of time?
4. Are all failures, defined as "undetected" in DC-FSAR Section 7.3.2.2, be detected by other means, or during a Technical Specification surveillance? If not, what types of failures cannot be detected at all?
5. How does AREVA NP verify the operation of self-testing features on a periodic basis, such as a Technical Specification surveillance? If no surveillance is provided for self-test features, provide the basis for why the self-test feature would not fail for the life of the plant.

**Response to Question 07.03-21:**

A response to this question will be provided by January 22, 2010.

**Question 07.03-22:**

Follow-up to RAI No. 07.03-6

Provide additional detail and or design documentation on the 'failure states' for the Engineered Safety Features Actuation System (ESFAS) design. Also, address the requirements of 10 CFR Part 50, Appendix A, General Design Criteria (GDC) 23 in the development of the failure modes and effects analysis (FMEA) tables and its associated write-up in U.S. EPR DC-FSAR Section 7.3. Addressing how a system manages a single failure in a power supply is one aspect of the question. However, AREVA NP did not fully address GDC 23 which asks for the failure state of safety equipment and why is that acceptable (whether single failure or not). Additionally, the assumptions given in AREVA's original response to this question cannot be gained from reading Section 7.3.

1. Will there be ITAAC to verify the response of the system to failures listed in GDC 23? Loss of electrical power is one scenario in GDC 23. GDC 23 requires design in terms of postulated adverse environments such as extreme heat.
2. Page 28 of the Teleperm XS Digital Protection System Manual States:

“The TXS system automatically detects failures in the subracks, the function processors, the I/O modules, and the communication functions. Failures that affect the subrack internal power supplies or control of the backplane bus will cause a transition to predefined fault conditions (e.g., reset) on the function computers, which results in a nonresponsive state in relationship to other subracks. Additionally, the TXS system monitors cabinet temperatures and cabinet cooling fan speed and provides the plant operators with an alarm if setpoints are exceeded.”

How is the failure of a subrack due to temperature bounded by the FMEA? What failure state would the system enter into?

3. How does the FMEA documented in Section 7.3 bound all the potential failure vectors such as those listed in GDC 23?

**Response to Question 07.03-22:**

A response to this question will be provided by December 18, 2009.

**Question 07.03-23:**

Follow-up to RAI Question 07.03-7

Provide clarification on the response to RAI Question 07.03-7 concerning compliance with IEEE Std. 603-1991, Clause 5.1.

In the response to RAI Question 07.03-7, AREVA NP provided an ITAAC Mapping of I&C system requirements to its associated IEEE Std. 603-1991 requirement, located in RAI 78, Supplement 2, Question 14.03.05-4 for U.S. EPR DC-FSAR, Section 2.4.1, ITAAC Item 4.18. However, upon reviewing the revised ITAAC (Item 4.18), the staff requires more clarification. Specifically, AREVA NP provided a summary failure modes and effects analysis (FMEA) as part of Chapter 7 of the U.S. EPR DC-FSAR. The summary FMEA goes the level of detail of the Protection System sub-components (i.e., acquisition and processing unit (APU), actuation logic unit (ALU), etc.). Will the FMEA described in Item 4.18 go to a further depth of detail to verify that single failure assumptions in the summary FMEA still hold. For example, a hardware/software analysis of the Network APU-ALU would show that it is not be susceptible to a single hardware device failure within the Network APU-ALU that would prevent signals from that APU being marked as invalid. Clarify within Item 4.18 the scope of the FMEA proposed.

**Response to Question 07.03-23:**

A response to this question will be provided by December 18, 2009.

**Question 07.03-24:**

Follow-up to RAI Question 07.03-8

Provide clarification on bypassed or inoperable status indication in terms of the power systems supplying the Protection System (PS) to satisfy the requirements of IEEE Std. 603-1991, Clauses 5.7 and 6.7.

The PS ITAAC shown in RAI 78, Supplement 2, Question 14.03.05-4, Table 2.4.1-7, was modified to demonstrate a test for PS actuation in the presence of a maintenance bypass/inoperable status indication in the main control room to fulfill the requirements of IEEE Std. 603-1991, Clauses 5.7 and 6.7. Further clarification of AREVA NP's response is needed. Specifically, AREVA NP states, "The U.S. EPR has sufficient redundancy that a power system redundancy configuration of zero is unlikely; therefore, bypassed and inoperable status indication for power systems supporting digital I&C, as described in Clause 8.3 of IEEE 603-1991, is unnecessary."

1. How are the power systems configured such that a redundancy configuration of zero is unlikely?
2. What is meant by , ". . . power systems supporting digital I&C. . ." ? Are these power systems that supply power to the PS and its supporting components, or is it power supplies within the PS cabinets themselves?
3. What power source indication or statuses are available on any PS console? By what means does an operator know if any power source is bypassed and/or inoperable?

**Response to Question 07.03-24:**

A response to this question will be provided by December 18, 2009.

**Question 07.03-25:**

Follow-up to RAI Question 07.03-11

Provide clarification on the differences in U.S. EPR DC-FSAR, Section 14.2.12.12.10, Revisions 0 and 1. Per guidance from Standard Review Plan, Section 7.1-C-4, IEEE Std. 603-1991, Clause 4.4, requires the identification of system response times and accuracies. AREVA NP stated in their original response to RAI Question 07.03-11 that, "Protection System response times will be tested and verified as outlined in U.S. EPR FSAR Tier 2, Section 14.2.12.12.10 *Protection (Test #146)*". U.S. EPR DC-FSAR, Section 14.2.12.12.10, Test 146 only states that the reactor protection system response times are tested. This is stated in Rev. 0 of the DC-FSAR. Rev. 1 of this section is not the same test. In fact, it states it is now Test#156 for Pressurizer Pressure and Level and Control.

1. When AREVA states 'RPS' in Revision 0 of U.S. EPR DC-FSAR, Section 14.2.12.12.10, does AREVA NP intend that to mean both the reactor trip function and engineered safety features actuation system or just the reactor trip function alone?
2. Are the Revision 0 and 1 versions of U.S. EPR DC-FSAR, Section 14.2.12.12.10 intended to match identical tests? Also, for the Revision 0 test, there is no specific testing for engineered safety features functions in U.S. EPR DC-FSAR, Section 14.2.12.12.10. The testing revolves around verification of reactor trip function. Explain what test will verify this.
3. For Revision 1, where is the test for the Protection System? And will the engineered safety features actuation system time delays and response times be tested as AREVA NP stated in this RAI question's original response?

Does AREVA plan to create an ITAAC for the purposes of verifying system response times of the PS (i.e. to verify compliance with 10 CFR Part 50, Appendix A, General Design Criteria 20)? If not, then explain why it is not necessary to provide pre-fuel load testing when the response times of PS and its instrument channels will be affected by the new equipment being installed which may differ from the calculated response times provided in Chapter 15?

**Response to Question 07.03-25:**

A response to this question will be provided by February 26, 2010.

**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:**

A response to this question will be provided by January 22, 2010.

**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:**

A response to this question will be provided by January 22, 2010.

**Question 07.04-10:**

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

Identify any additional controls at the Remote Shutdown Station (RSS) that would be used to bring the plant to hot shutdown.

10 CFR Part 50, Appendix A, General Design Criteria 19 requires, in part, equipment at appropriate locations outside the control room to provide for (1) prompt, hot shutdown of the reactor, including necessary Instruments and Controls (I&C) to maintain the unit in a safe condition during hot shutdown, and (2) with a potential capability for subsequent cold shutdown of the reactor through the use of suitable procedures. The U.S. EPR Design Certification (DC) Final Safety Analysis Report (FSAR) Table 18.7-2 only identifies reactor trip and turbine trip as controls at the RSS. Are there any other controls not described in the RSS? If so, what are they and where are they identified in the FSAR?

**Response to Question 07.04-10:**

Refer to the Response to RAI 110, Supplement 3, Question 16-215, which clarified RSS controls and changed the U.S. EPR FSAR. Although U.S. EPR FSAR Tier 2, Table 18.7-2 identifies the reactor trip and the turbine trip as controls at the RSS, other controls available at the RSS are described in U.S. EPR FSAR Tier 2, Section 7.4.1.3.4. Remote shutdown capability is described in U.S. EPR FSAR Tier 2, Section 7.4.2.3.

**FSAR Impact:**

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

**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:**

A response to this question will be provided by January 22, 2010.

**Question 07.04-12:**

Follow-up to RAI Question No. 07.04-8

Update the list of Post-fire Safe Shutdown Systems listed in the U.S. EPR DC-FSAR, Section 7.4.1.3, to include Section 7.4.1.3.3, Fuel Pool Cooling System (FPCS).

10 CFR 52.6 requires, in part, that information provided to the NRC be complete and accurate in all material respects. As stated in the RAI response to Question 07.04-8, the FPCS described in DC FSAR Section 7.4.1.3.3 is included as a post-fire safe shutdown system. DC FSAR Section 7.4.1.3 list of post-fire safe shutdown system does not list FPCS as included.

**Response to Question 07.04-12:**

U.S. EPR FSAR Tier 2, Section 7.4.1.3 will be revised to include the following statement:

“The systems described in Section 7.4.1.2 and the additional systems listed in Sections 7.4.1.3.1 through 7.4.1.3.3 were identified as post-fire safe shutdown systems.”

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 7.4.1.3 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:**

A response to this question will be provided by January 22, 2010.

**Question 07.05-9:**

Follow-up to RAI Question No. 07.05-3.

The ITAAC identified in the RAI response to Question 07.05-3 are considered design acceptance criteria (DAC) and should be noted so.

10 CFR 52.47(a)(2) states “the application must contain a level of design information sufficient to enable the Commission to judge the applicant’s proposed means of assuring that construction conforms to the design and to reach a final conclusion on all safety questions associated with the design before the certification is granted.” SECY-92-053 provides guidance on meeting the requirements through DAC since advanced instrumentation and controls is identified as an area where the use of DAC is appropriate. The ITAAC for the post-accident monitoring instrumentation to develop the final list of variables, their accuracy and ranges, etc. should be identified as DAC in the ITAAC itself.

**Response to Question 07.05-9:**

A response to this question will be provided by December 18, 2009.

# U.S. EPR Final Safety Analysis Report Markups

Refer to Section 10.2 for further information on the TG I&C.

#### 7.1.1.5 Level 0 - Process Interface

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

The majority of the process interface equipment is included within the mechanical and electrical process systems that the I&C systems monitor and control. These systems are described in Chapter 5, Chapter 6, Chapter 8, Chapter 9, Chapter 10 and Chapter

07.01-14 →

11. Additionally, the plant fire alarm system (PFAS) and the Communication System are described in Chapter 9, Sections 9.5.1 and 9.5.2, respectively.

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

#### 7.1.1.5.1 Control Rod Drive Control System

##### Classification

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

##### Description

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

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

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

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

### 7.4.1.3 Post-fire Safe Shutdown Systems

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

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

The fire protection analysis described in Appendix 9A confirms the plant capability to safely shutdown following a fire. The systems described in Section 7.4.1.2 and the

07.04-12

additional systems listed in Section 7.4.1.3.1 through Section 7.4.1.3.3 and Section 7.4.1.3.2 were identified as post-fire safe shutdown systems.

#### 7.4.1.3.1 Main Feedwater System

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

#### 7.4.1.3.2 Chemical and Volume Control System

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

#### 7.4.1.3.3 Fuel Pool Cooling System

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

#### 7.4.1.3.4 Remote Shutdown Station

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