

## ArevaEPRDCPEm Resource

---

**From:** BRYAN Martin (EXTERNAL AREVA) [Martin.Bryan.ext@areva.com]  
**Sent:** Friday, December 03, 2010 4:50 PM  
**To:** Tesfaye, Getachew  
**Cc:** DELANO Karen (AREVA); ROMINE Judy (AREVA); BENNETT Kathy (AREVA); PANNELL George (AREVA)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch 7, Supplement 5  
**Attachments:** RAI 373 Supplement 5 Response US EPR DC - PUBLIC.pdf

Getachew,

On May 10, 2010, AREVA provided a schedule for technically correct and complete response to the 5 questions. To provide an opportunity to interact with the NRC, a revised schedule was provided on June 11, 2010, July 9, 2010, and August 13, 2010, and October 28, 2010.

The attached file, "RAI 373 Supplement 5 Response US EPR DC" provides technically correct and complete responses to 3 of the remaining 3 questions, as committed. In addition, the responses for questions 07.01-21 and 22 are also provided again, because the U.S EPR Final Safety Analysis Report markups were inadvertently not included with the RAI 373 Supplement 3 response. The U.S EPR Final Safety Analysis Report markups for questions 07.01-21 and 22 are appended to this file in redline-strikeout form.

This response contains changed pages from "Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report" ANP-10310P, Revision 0 previously transmitted via AREVA NP Inc. letter to NRC 09:111 dated October 30, 2009. That transmittal provided the affidavit that requested the entire document be considered proprietary. Therefore, in accordance with that previous determination, AREVA NP requests the document be maintained from public disclosure in accordance with 10 CFR 2.390 as stated in the prior affidavit. The proprietary portions of this response will be transmitted under separate email.

The following table indicates the respective pages in the response document, "RAI 373 Supplement 5 Resposne U.S. EPR DC" that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 373 — 07.01-21	2	4
RAI 373 — 07.01-22	5	5
RAI 373 — 07.01-23	6	6
RAI 373 — 07.01-24	7	8
RAI 373 — 07.01-25	9	9

This concludes the formal AREVA NP response to RAI 373, and there are no questions from this RAI for which AREVA NP has not provided responses.

Sincerely,

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

---

**From:** BRYAN Martin (External RS/NB)  
**Sent:** Thursday, October 28, 2010 4:41 PM  
**To:** 'Tesfaye, Getachew'  
**Cc:** DELANO Karen (RS/NB); ROMINE Judy (RS/NB); BENNETT Kathy (RS/NB); PANNELL George (CORP/QP)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch 7, Supplement 4

Getachew,

On May 10, 2010, AREVA provided a schedule for technically correct and complete response to the 5 questions. To provide an opportunity to interact with the NRC, a revised schedule was provided on June 11, 2010, July 9, 2010, and August 13, 2010. Additional time is needed to address comments and have additional interaction with the staff on the three remaining questions.

A complete answer is not provided for the remaining 3 questions. The schedule for a technically correct and complete response to these questions is changed and is provided below

Question #	Response Date
RAI 373 — 07.01-23	December 3, 2010
RAI 373 — 07.01-24	December 3, 2010
RAI 373 — 07.01-25	December 3, 2010

Sincerely,

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

---

**From:** BRYAN Martin (External RS/NB)  
**Sent:** Friday, August 13, 2010 4:31 PM  
**To:** 'Tesfaye, Getachew'  
**Cc:** DELANO Karen (RS/NB); ROMINE Judy (RS/NB); BENNETT Kathy (RS/NB); PANNELL George (CORP/QP)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch 7, Supplement 3

Getachew,

On May 10, 2010, AREVA provided a schedule for technically correct and complete response to the 5 questions. To provide an opportunity to interact with the NRC on the proposed responses, a revised schedule was provided on June 11, 2010 and July 9, 2010. A draft response was provided on June 15, 2010. Based on results of the August 10, 2010 telecom with the staff, enclosed are final responses to RAI 373 supplement 3, questions 7.1-21 and 7.1-22. Additional time is needed to address comments and have additional interaction with the staff on the three remaining questions.

A complete answer is not provided for the remaining 3 questions. The schedule for a technically correct and complete response to these questions is changed and is provided below

Question #	Response Date
RAI 373 — 07.01-23	October 28, 2010
RAI 373 — 07.01-24	October 28, 2010
RAI 373 — 07.01-25	October 28, 2010

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

---

**From:** BRYAN Martin (EXT)  
**Sent:** Friday, July 09, 2010 5:17 PM  
**To:** 'Tesyfaye, Getachew'  
**Cc:** DELANO Karen V (AREVA NP INC); ROMINE Judy (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); PANNELL George L (AREVA NP INC)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch 7, Supplement 2

Getachew,

On May 10, 2010, AREVA provided a schedule for technically correct and complete response to the 5 questions. To provide an opportunity to interact with the NRC on the proposed responses, a revised schedule was provided on June 11, 2010. A draft response was provided on June 15, 2010. To allow additional time to interact with the staff, a revised schedule is provided below.

Question #	Response Date
RAI 373 — 07.01-21	August 15, 2010
RAI 373 — 07.01-22	August 15, 2010
RAI 373 — 07.01-23	August 15, 2010
RAI 373 — 07.01-24	August 15, 2010
RAI 373 — 07.01-25	August 15, 2010

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

**From:** BRYAN Martin (EXT)  
**Sent:** Friday, June 11, 2010 3:31 PM  
**To:** 'Tesfaye, Getachew'  
**Cc:** DELANO Karen V (AREVA NP INC); ROMINE Judy (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); PANNELL George L (AREVA NP INC)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch 7, Supplement 1

Getachew,

On May 10, 2010, AREVA provided a schedule for technically correct and complete response to the 5 questions. To provide an opportunity to interact with the NRC on the proposed responses, a revised schedule is provided below.

A complete answer is not provided for 5 of the 5 questions. The schedule for a technically correct and complete response to these questions is changed and is provided below.

Question #	Response Date
RAI 373 — 07.01-21	July 9, 2010
RAI 373 — 07.01-22	July 9, 2010
RAI 373 — 07.01-23	July 9, 2010
RAI 373 — 07.01-24	July 9, 2010
RAI 373 — 07.01-25	July 9, 2010

Sincerely,

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

---

**From:** WELLS Russell D (AREVA NP INC)  
**Sent:** Monday, May 10, 2010 7:49 PM  
**To:** 'Getachew Tesfaye'  
**Cc:** BRYAN Martin (EXT); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 373 Response US EPR DC.pdf," provides a schedule since a technically correct and complete response to the 5 questions is not provided.

The following table indicates the respective pages in the response document, "RAI 373 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 373 — 07.01-21	2	2
RAI 373— 07.01-22	3	3
RAI 373 —07.01-23	4	4
RAI 373 —07.01-24	5	5
RAI 373 —07.01-25	6	6

A complete answer is not provided for 5 of the 5 questions. The schedule for a technically correct and complete response to these questions is provided below.

Question #	Response Date
RAI 373 —07.01-21	June 11, 2010
RAI 373— 07.01-22	June 11, 2010
RAI 373 —07.01-23	June 11, 2010
RAI 373 —07.01-24	June 11, 2010
RAI 373 —07.01-25	June 11, 2010

Sincerely,

(Russ Wells on behalf of)  
Martin (Marty) C. Bryan  
Licensing Advisory Engineer  
AREVA NP Inc.  
Tel: (434) 832-3016  
[Martin.Bryan.ext@areva.com](mailto:Martin.Bryan.ext@areva.com)

---

**From:** Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]  
**Sent:** Friday, April 09, 2010 4:16 PM  
**To:** ZZ-DL-A-USEPR-DL  
**Cc:** Suggs, LaDonna; Spaulding, Deirdre; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource  
**Subject:** U.S. EPR Design Certification Application RAI No. 373 (4393), FSAR Ch. 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on February 25, 2010, and on April 9, 2010, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

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

**Hearing Identifier:** AREVA\_EPR\_DC\_RAIs  
**Email Number:** 2330

**Mail Envelope Properties** (BC417D9255991046A37DD56CF597DB71085E1716)

**Subject:** Response to U.S. EPR Design Certification Application RAI No. 373, FSAR Ch  
7, Supplement 5  
**Sent Date:** 12/3/2010 4:49:55 PM  
**Received Date:** 12/3/2010 4:50:01 PM  
**From:** BRYAN Martin (EXTERNAL AREVA)  
**Created By:** Martin.Bryan.ext@areva.com

**Recipients:**

"DELANO Karen (AREVA)" <Karen.Delano@areva.com>  
Tracking Status: None  
"ROMINE Judy (AREVA)" <Judy.Romine@areva.com>  
Tracking Status: None  
"BENNETT Kathy (AREVA)" <Kathy.Bennett@areva.com>  
Tracking Status: None  
"PANNELL George (AREVA)" <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	10210	12/3/2010 4:50:01 PM
RAI 373 Supplement 5 Response US EPR DC - PUBLIC.pdf		307104

**Options**

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

**Response to**

**Request for Additional Information No. 373(4393), Supplement 5**

**10/28/2010**

**U.S. EPR Standard Design Certification**

**AREVA NP Inc.**

**Docket No. 52-020**

**SRP Section: 07.01 - Instrumentation and Controls - Introduction**

**Application Section: 7.1**

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

**Question 07.01-21:**

Provide clarification of the apparent discrepancy in the use and definition of firmware.

Section 7.1, Definitions, defines system software as referring to “relevant software including an operating system, firmware, and runtime software that is integrated to form a generic I&C platform.” Section 7.1.1.4.3 of the FSAR states that “the logic for the safety related priority module is implemented with firmware-only based devices (e.g. EEPROM) with no system software or application software.” This assertion in Section 7.1.1.4.3 that firmware is not considered software is inconsistent with the definition. Provide clarification of the apparent discrepancy.

**Response to Question 07.01-21:**

U.S. EPR FSAR Tier 2, Section 7.1, “Definitions” and Section 7.1.1.4.3, “Priority and Actuator Control System” will be revised to eliminate inconsistency regarding use of the term “firmware.”

The use of the term “firmware” in U.S. EPR FSAR Tier 2, Section 7.1.1.4.3 was intended to illustrate contrast between software that can be changed without replacing a hardware component, and the programmed logic used in the priority and actuator control system (PACS) priority module which cannot be changed without removing and replacing the priority module itself. U.S. EPR FSAR Tier 2, Section 7.1.1.4.3 will be revised to reflect this.

The definition of system software in Section 7.1, “Definitions,” was intended to illustrate contrast between layers of TXS software that do not change based on a specific application, and those that are configured uniquely for each specific application. Table 07.01-21-1 is a reproduction of EMF-2110NP(A), Figure 3.5 that provides graphical representation of the different layers of software on a TXS processor. The operating system and platform software layers shown in EMF-2110NP(A), Figure 3.5 are those considered “system software” in the TXS platform. The definition of “system software” in U.S. EPR FSAR Tier 2, Section 7.1 will be revised:

Institute of Electrical and Electronics Engineers (IEEE) Standard Glossary of Software Engineering Terminology, Std. 610.12-1990, defines firmware as follows:

“The combination of a hardware device and computer instructions and data that reside as read-only software on that device.”

Notes: (1) This term is sometimes used to refer only to the hardware device or only to the computer instructions or data, but these meanings are deprecated. (2) The confusion surrounding this term has led some to suggest that it be avoided altogether.”

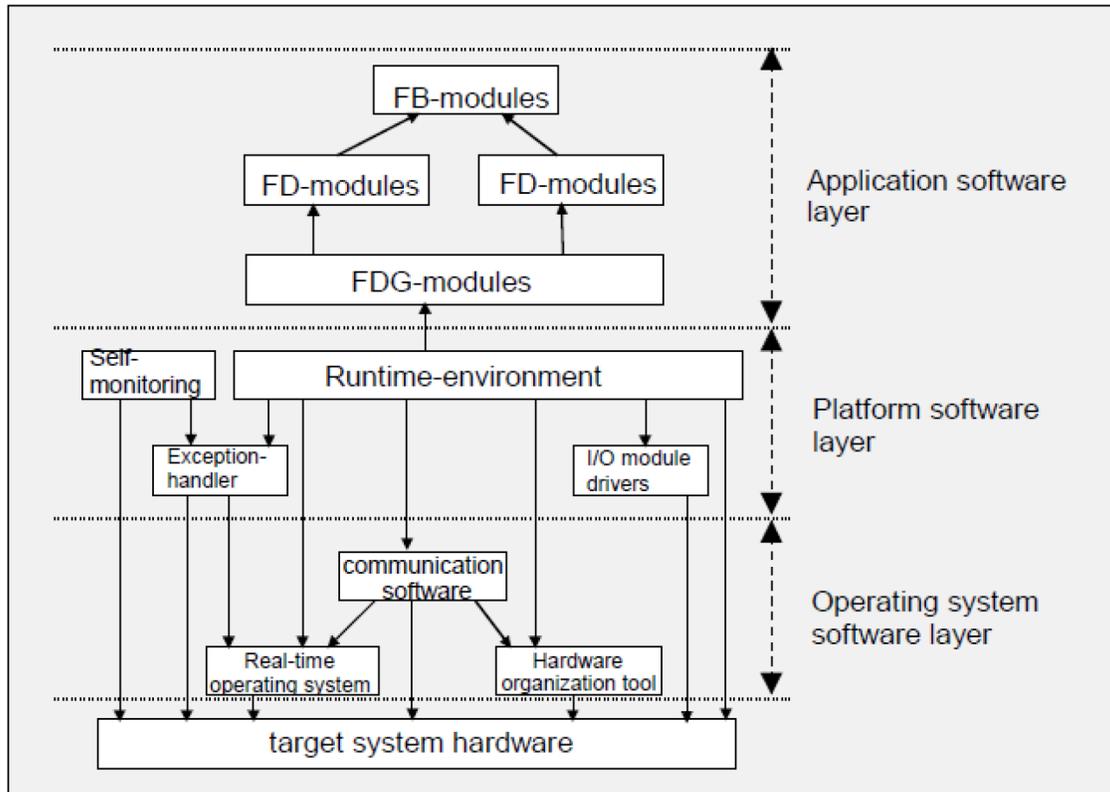
AREVA NP agrees with Note 2 contained in the IEEE definition of firmware. Use of the term “firmware” leads to confusion, and does not provide adequate understanding of the technology to be deployed in the U.S. EPR design. Therefore, the term “firmware” will be eliminated from the U.S. EPR FSAR.

It should be noted that a word-search of ANP-10310P, “Methodology for 100% Combinatorial Testing of the U.S. EPR Priority Module Technical Report” revealed no instances of the term “firmware” in the document. No revisions to ANP-10310P are required to address this topic.

**FSAR Impact:**

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

**Table 07.01-21-1—EMF-2110NP(A), Figure 3.5, “Software Layers of the Runtime System of One Processing Module”**



**Question 07.01-22:**

Provide a description of how the Priority Actuation and Control System (PACS) meets Criterion 5.2 "Completion of Protective Action" of IEEE Std. 603-1998.

The staff evaluated the completion of protective action characteristics of the PACS against Criterion 5.2 of IEEE Std. 603-1998 which requires the safety system to be designed so that, once initiated automatically or manually, the intended sequence of protective actions of the execute features continue until completion. The NRC staff was unable to locate specific information regarding completion of protective action for the PACS in the applicant's submittal and therefore requests that the applicant provide a description of how this requirement is being addressed in PACS.

**Response to Question 07.01-22:**

In the U.S. EPR design, the PACS does not perform any functionality needed to confirm completion of protective actions. Logic in the protection system (PS) upstream of the PACS, and electrical switchgear downstream of the PACS provide for completion of protective actions.

U.S. EPR FSAR Tier 2, Section 7.1.2.6.13 specifically addresses compliance with completion of protection action requirements. This section contains an inaccurate reference to U.S. EPR FSAR Tier 2, Section 7.3.2.2 for more detail. That detail is actually found in U.S. EPR FSAR Tier 2, Section 7.3.2.3. A revision will be made to correct this inaccuracy.

U.S. EPR FSAR Tier 2, Section 7.3.2.3.4 addresses compliance with completion of protection action requirements for engineered safety feature (ESF) actuations.

U.S. EPR FSAR Tier 1, Section 2.4.1, ITAAC commitment 4.2 verifies that features for completion of protective action exist in the as-built design.

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 7.1.2.6.13 will be revised as described in the response and indicated on the enclosed markup.

**Question 07.01-23:**

Are all internal states directly observable and will they all be tested as a part of the test cases?

Under 10 CFR 50.55a(a)(3), the applicant requested to use IEEE Std. 603-1998 in place of IEEE Std. 603-1991, as endorsed in 10 CFR 50.55a(h). Clause 5.3 of IEEE Std. 603-1998 requires, in part, that components and modules shall be of a quality that is consistent with minimum maintenance requirements and low failure rates. The staff used the guidance found in Digital Instrumentation and Controls - Interim Staff Guidance No. 4, "Highly Integrated Control Room - Communication," Revision 1, to evaluate how the applicant met Clause 5.3 for the Priority Actuation and Control System (PACS) as described in Technical Report ANP-10310P, "Methodology for 100% Combinatorial Testing of the US EPR Priority Module Technical Report," Revision 0. Digital Instrumentation and Control Interim Staff Guidance No. 4 states, in part, that 100 percent testing means that every possible combination of inputs and every possible sequence of device states is tested and all outputs are verified for every case and sequence of device states must be tested. Section 6.2 of Technical Report ANP-10310P states, in part, that the internal states specified for PC10 functionality have a very direct effect on the module outputs. Accordingly, the effect of these internal states is easily observed at the module outputs. However, additional test outputs may be provided that allow complementary checking of the behavior of the internal states. The NRC staff requests that the applicant provide a firm commitment that all internal states are directly observable by test equipment and will be tested as a part of the test cases in Technical Report ANP-10310P.

**Response to Question 07.01-23:**

In the U.S. EPR priority module design, internal states are directly observable for the purpose of testing, and will be included as outputs monitored in the 100 percent combinatorial testing of the module. ANP-10310P will be revised to include this commitment.

This will be accomplished by setting the logic of the priority module to include an output directly from each internal state to the diagnostic connector, or "test jack." Figure 5-5 of ANP-10310P provides an example of this, in which pins X2:9 and X2:22 directly monitor the state of the command flip-flops.

For each test case, the observed value of each internal state will be compared to the expected value by the test machine.

The outputs of the test jack representing the internal states will not be used during plant operation and are therefore not included in the manual verification of module outputs. The manual verification approach is described further in the Response to Question 07.01-24 of this RAI.

**FSAR Impact:**

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

ANP-10310P will be revised as indicated in the response and shown in the attached markups.

**Question 07.01-24:**

Provide clarification to explain how the sorting method employed in ANP-10310P does not impact the ability to provide 100 percent manual verification of all test results.

Under 10 CFR 50.55a(a)(3), the applicant requested to comply with IEEE Std. 603-1998 versus IEEE Std. 603-1991, as endorsed by 10 CFR 50.55a(h). Clause 5.3 of IEEE Std. 603-1998 requires, in part, that components and modules shall be of a quality that is consistent with minimum maintenance requirements. The staff used the guidance in Digital Instrumentation and Control Interim Staff Guidance No. 4, "Highly Integrated Control Room - Communications," Revision 1, to evaluate the acceptability of Priority Actuation and Control System as described in Technical Report ANP-10310P, "Methodology for 100% Combinatorial Testing of the US EPR Priority Module Technical Report," Revision 0. Section 2.8 of Interim Staff Guidance No. 4 states that if the tests are generated by any automatic test generation program then all the test sequences and test results should be manually verified. Technical Report ANP-10310P describes the applicant's approach for manual verification of testing results generated by the automatic test generation program. The methodology for manual verification describes a rule-based sorting of a subset of test cases involving priority logic only, which appears inconsistent with the requirement to manually verify all test sequences and test results. The NRC staff requests that the applicant provide clarification to explain that the sorting method does not impact the ability to provide 100 percent manual verification of all test results.

**Response to Question 07.01-24:**

The two separate issues identified in this question, application of the sorting method and manual verification of a subset of module outputs, are addressed separately as follows:

Application of the Sorting Method:

The manual verification proposed by AREVA NP includes manual verification of each test case. The sorting method does not impact the ability to manually verify each test case. This is stated in ANP-10310P, Section 7.2:

"Completeness is checked by manually verifying that every test case is addressed by at least one sorting rule and that every sorting rule addresses at least one test case."

The purpose of the sorting rules is to efficiently verify a large number of test cases while minimizing the possibility of human error occurring from the manual treatment of a large number of test cases. For example, after studying the intended priority logic, the verifier concludes that one particular input has the highest priority of the module inputs. Approximately half of the test cases will include a logic "1" for that input. Without any further analysis, the verifier can conclude that the expected output for those test cases correspond to the highest priority input being "1", regardless of any combinations of other inputs.

It should also be noted that the sorting rules themselves are created manually, based on the verifiers analysis of the intended priority logic. This is captured in the example provided to illustrate application of the sorting rules in ANP-10310P, Section 7.2:

"The test cases are sorted in eight successive steps, based on sorting rules that are derived by manual analysis of the intended priority logic."

### Manual Verification of a Subset of Module Outputs:

The manual verification proposed by AREVA NP includes manual verification of each test case. Within each test case, however, not all module outputs are subjected to manual verification. Section 7.1 of ANP-10310P states:

“The verifier defines the expected outputs of the priority logic for every input signal combination by manually entering the expected values in the table of test vectors provided by the automatic generation of the input signal combinations. Output of the priority logic refers to only the command outputs sent to the actuated device. Check-back signals processed for control room display (if processed by the logic) are not included in this check because they do not participate in the priority function itself.”

AREVA NP will modify this approach so that all safety-related outputs of the priority module will be included in the manual verification of the test cases.

The outputs of the priority module can be placed into one of three groups:

- Group 1 - outputs to the actuator that place the actuator in the correct state:

These outputs are safety-related and will be included in the manual verification of every test case. By subjecting these outputs to both automatic checking by the test machine and manual verification, reasonable assurance is provided that no common-cause failure mode results in the actuator being placed in an incorrect state.

- Group 2 - checkback outputs to the safety-related instrumentation and control (I&C) systems indicating the position of the actuator

These outputs are safety-related and will be included in the manual verification of every test case. These outputs are not used by the safety-related I&C systems to take any further automatic control action. They are processed by the safety-related I&C systems for display to the operator. By subjecting these outputs to both automatic checking by the test machine and manual verification, reasonable assurance is provided that no common-cause failure mode results in the operator taking an incorrect manual action based on incorrect display information.

- Group 3, outputs used for non-safety related purposes

These outputs are used for coordination of the non-safety-related communication module to the priority module, or for use in periodic testing. These outputs are not included in the manual verification, but are automatically compared to expected test results by the test machine for every test case.

In summary, AREVA NP will manually verify all outputs of the priority module that are used for safety-related functions, for all test cases.

### **FSAR Impact:**

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

ANP-10310P will be revised as indicated in the response and shown in the attached markups.

**Question 07.01-25:**

Provide additional information regarding the verification, validation, and timing analysis to address the potential for software common cause failures in the requirements or design phases of the Priority Actuation and Control System (PACS) development lifecycle.

Under 10 CFR 50.55a(a)(3), the applicant requested to comply with IEEE Std. 603-1998 versus IEEE Std. 603-1991, as endorsed by 10 CFR 50.55a(h). Clause 5.16 of IEEE Std. 603-1998 requires, in part, that plant parameters be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. In addition, 10 CFR Part 50, Appendix A, General Design Criteria 22, requires, in part, that design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protective function. In Technical Report ANP-10310P, "Methodology for 100% Combinatorial Testing of the US EPR Priority Module Technical Report," Revision 0, the applicant provided a methodology for 100 percent combination testing and manual verification of the PACS, which provides quality assurance and diminishes the likelihood of a software common cause failure in the design implementation phase. However, the 100 percent combination testing would not address potential design faults that may be introduced in the requirements specification or design specification stages of the PACS development lifecycle. The NRC staff requests that the applicant provide additional information regarding the requirements verification and validation and the timing analysis to address the potential for software common cause faults in the requirements and design specification phases of the PACS development.

**Response to Question 07.01-25:**

Consistent with its use in performing safety-related functions, the priority module is classified as safety-related and designed in accordance with applicable requirements, codes and standards. More specifically, the priority module is designed under the TELEPERM XS (TXS) quality assurance (QA) program, which complies with 10 CFR 50, Appendix B requirements. The TXS QA program guides all phases and activities of priority module life-cycle.

The TXS QA program is described in EMF-2110(NP)(A), Section 2.1. Procedures and instructions used to implement the QA program are described in Section 5.0 of EMF-2110(NP)(A). This QA program was reviewed and approved by NRC in the Safety Evaluation Report for EMF-2110(NP)(A).

**FSAR Impact:**

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

# U.S. EPR Final Safety Analysis Report Markups

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

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

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

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

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

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

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

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

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

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

07.01-21

~~System software~~—refers to relevant software including an operating system, firmware, and runtime software that is integrated to form a generic I&C platform. System software – The layers of software that are not configured uniquely for a specific I&C application. System software has a different functional purpose compared to “application software” (defined above) and is the same on all TXS processors. In contrast, application software is configured to reflect a nuclear power plant’s specific

safety system functional requirements, different application software functions reside on individual TXS processors within the overall TXS system. For TELEPERM XS, system software is defined as the operating system and platform software layers shown in Figure 3.5 of Reference 6.

## 7.1.1 U.S. EPR I&C Architecture

### 7.1.1.1 Overview

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

- Use of digital technology:

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

- Robust I&C architecture design:

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

- Automation of plant operation:

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

- State of the art design for human factors:

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

The 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:

- Level 3: business management systems – These consist of plant information management systems. Other than interfaces provided from Level 2, these systems are not within the scope of this document and are not shown on Figure 7.1-2.

The PAC module is described in ANP-10273P (Reference 7). The PACS equipment modules may be modified and upgraded as needed, but shall exhibit these characteristics.

07.01-21

- Each PAC module consists of two parts: a safety part and an operational part.
- The safety part consists of logic implemented with firmware only based devices (e.g., EEPROM), with no system software or application software. The priority module consists of logic that can not be modified while the module is installed. To modify the priority module logic, the module must be removed and replaced with another module containing the modified logic.
- The inputs and outputs of the safety part priority module are via hardwired connections.
- The logic of the safety part priority module is fully testable subject to 100 percent combinatory proof-of-design testing and not subject to software common cause failure.
- The operational part communication module is qualified as an associated circuit.
- The data communications from the PAS is only via the operational part communication module.

#### Qualification Requirements

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

#### Quality Requirements

Quality for the PAC modules is described in ANP-10273P (Reference 7). The PACS is designed under the TXS quality program described in Section 7.1.1.2.1.

#### Diversity Requirements

The PAC priority modules are diverse from the digital TXS function processors.

#### Data Communications

Non-safety-related, bidirectional, data connections are implemented between the operational part of the PAC communication modules and the PAS.

#### Power Supply

The PACS is powered from the Class 1E uninterruptible power supply (EUPS). The EUPS provides backup power with two-hour batteries and the EDGs in the case of a

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

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

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

#### 7.1.2.6.13 Completion of Protective Action (Clauses 5.2 and 7.3)

The safety systems meet the requirements of Clause 5.2 of IEEE Std 603-1998 (Reference 4). When initiated by a safety system, protective actions proceed to completion. Return to normal operation requires deliberate operator intervention.

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

07.01-22

Refer to [Section 7.3.2.2](#) [Section 7.3.2.3](#) for a description of completion of protection action for ESF actuation functions.

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

#### 7.1.2.6.14 Quality (Clause 5.3)

The safety systems meet the requirements of Clause 5.3 of IEEE Std 603-1998 (Reference 4). The safety systems are within the scope of the U.S. EPR quality assurance program (QAP) described in Section 17.5. The TXS hardware quality is described in EMF-2110(NP)(A) (Reference 6).

The digital safety systems meet the additional guidance of IEEE Std 7-4.3.2-2003 (Reference 21). This guidance addresses software quality processes for the use of digital technology in safety systems.

TXS system software is developed in accordance with the processes described in EMF-2110 (NP)(A) (Reference 6).

**Methodology for 100%  
Combinatorial Testing of  
the U.S. EPR Priority  
Module Technical Report  
Markups**

