

## ArevaEPRDCPEm Resource

---

**From:** BRYAN Martin (EXTERNAL AREVA) [Martin.Bryan.ext@areva.com]  
**Sent:** Monday, November 29, 2010 3:21 PM  
**To:** Tesfaye, Getachew  
**Cc:** DELANO Karen (AREVA); ROMINE Judy (AREVA); PANNELL George (AREVA); BUDZIK Dennis (AREVA); SCHMUGGE Paul (AREVA); HALLINGER Pat (EXTERNAL AREVA); RYAN Tom (AREVA); DOYEL Chris (AREVA); SMALL Shelby (AREVA)  
**Subject:** DRAFT Response to U.S. EPR Design Certification Application RAI No. 414, FSAR Ch. 7 OPEN ITEM,  
**Attachments:** RAI 414 Supplement 1 Response US EPR DC-DRAFT.pdf

[Getachew,](#)

Getachew,

Attached is a draft response for RAI 414 for all questions EXCEPT 07.02-32. Let me know if the staff has questions or if this can be sent as a final response.

Thanks,

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:** Monday, November 29, 2010 2:35 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. 414, FSAR Ch. 7 OPEN ITEM, Supplement 2

Getachew,

AREVA NP provided a schedule on July 14, 2010 for a technically correct and complete response to RAI 414. Supplement 1 response was sent on October 28, 2010 to provide a revised schedule for all questions. To allow additional time to interact with the NRC staff, a revised schedule for six of the seven questions is provided. The schedule for Question 07.02-32 remains the same.

A complete answer is not provided for the 7 questions. The schedule for technically correct and complete responses to these questions is provided below.

Question #	Response Date
RAI 414 — 07.02-32	March 01, 2011
RAI 414 — 07.03-33	January 13, 2011
RAI 414 — 07.02-30	January 13, 2011
RAI 414 — 07.03-31	January 13, 2011
RAI 414 — 07.04-14	January 13, 2011
RAI 414 — 07.07-20	January 13, 2011
RAI 414 — 07.07-22	January 13, 2011

Sincerely,

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

---

**From:** BRYAN Martin (External RS/NB)  
**Sent:** Thursday, October 28, 2010 4:53 PM  
**To:** 'Tefaye, 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. 414, FSAR Ch. 7 OPEN ITEM, Supplement 1

Getachew,

AREVA NP provided a schedule on July 14, 2010 for a technically correct and complete response to RAI 414. To allow additional time to interact with the NRC staff, a revised schedule is provided.

A complete answer is not provided for the 7 questions. The schedule for technically correct and complete responses to these questions is provided below.

Question #	Response Date
RAI 414 — 07.02-32	March 01, 2011
RAI 414 — 07.03-33	November 29, 2010
RAI 414 — 07.02-30	November 29, 2010
RAI 414 — 07.03-31	November 29, 2010
RAI 414 — 07.04-14	November 29, 2010
RAI 414 — 07.07-20	November 29, 2010
RAI 414 — 07.07-22	November 29, 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 (EXT)  
**Sent:** Wednesday, July 14, 2010 6:32 PM  
**To:** 'Tefaye, Getachew'  
**Cc:** DELANO Karen V (AREVA NP INC); ROMINE Judy (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); RYAN Tom (AREVA NP INC)  
**Subject:** Response to U.S. EPR Design Certification Application RAI No. 414, FSAR Ch. 7 OPEN ITEM

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 414 Response US EPR DC.pdf" provides a schedule since technically correct and complete responses to the 7 questions are not provided.

The following table indicates the respective pages in the response document, "RAI 414 Response US EPR DC.pdf" that contain AREVA NP's responses to the subject questions.

Question #	Start Page	End Page
RAI 414 — 07.02-32	2	2
RAI 414 — 07.03-33	3	3
RAI 414 — 07.02-30	4	6
RAI 414 — 07.03-31	7	8
RAI 414 — 07.04-14	9	9
RAI 414 — 07.07-20	10	10
RAI 414 — 07.07-22	11	11

A complete answer is not provided for the 6 questions. The schedule for technically correct and complete responses to these questions is provided below.

Question #	Response Date
RAI 414 — 07.02-32	October 28, 2010
RAI 414 — 07.03-33	October 28, 2010
RAI 414 — 07.02-30	October 28, 2010
RAI 414 — 07.03-31	October 28, 2010
RAI 414 — 07.04-14	October 28, 2010
RAI 414 — 07.07-20	October 28, 2010
RAI 414 — 07.07-22	October 28, 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:** Tesfaye, Getachew [mailto:Getachew.Tesfaye@nrc.gov]  
**Sent:** Tuesday, June 15, 2010 4:58 PM  
**To:** ZZ-DL-A-USEPR-DL  
**Cc:** Truong, Tung; Morton, Wendell; Spaulding, Deirdre; Mott, Kenneth; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource  
**Subject:** U.S. EPR Design Certification Application RAI No. 414(4394,4398,4752,4548), FSAR Ch. 7 OPEN ITEM

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on June 8, 2010, and on June 15, 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 question in this RAI is an OPEN ITEM in the safety evaluation report for Chapter 7 for Phases 2 and 3 reviews. As such, the schedule we have established for your application assumes technically correct and complete responses prior to the start of Phase 4 review. For any RAI that cannot be answered prior to the start of Phase 4 review, it is expected that a date for receipt of this information will be provided 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:** 2309

**Mail Envelope Properties** (BC417D9255991046A37DD56CF597DB71085846D5)

**Subject:** DRAFT Response to U.S. EPR Design Certification Application RAI No. 414,  
FSAR Ch. 7 OPEN ITEM,  
**Sent Date:** 11/29/2010 3:20:43 PM  
**Received Date:** 11/29/2010 3:21:01 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  
"PANNELL George (AREVA)" <George.Pannell@areva.com>  
Tracking Status: None  
"BUDZIK Dennis (AREVA)" <Dennis.Budzik@areva.com>  
Tracking Status: None  
"SCHMUGGE Paul (AREVA)" <Paul.Schmugge@areva.com>  
Tracking Status: None  
"HALLINGER Pat (EXTERNAL AREVA)" <Pat.Hallinger.ext@areva.com>  
Tracking Status: None  
"RYAN Tom (AREVA)" <Tom.Ryan@areva.com>  
Tracking Status: None  
"DOYEL Chris (AREVA)" <Chris.Doyel@areva.com>  
Tracking Status: None  
"SMALL Shelby (AREVA)" <Shelby.Small@areva.com>  
Tracking Status: None  
"Teschaye, Getachew" <Getachew.Teschaye@nrc.gov>  
Tracking Status: None

**Post Office:** AUSLYNCMX02.adom.ad.corp

<b>Files</b>	<b>Size</b>	<b>Date &amp; Time</b>
MESSAGE	6274	11/29/2010 3:21:01 PM
RAI 414 Supplement 1 Response US EPR DC-DRAFT.pdf		453667

**Options**

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

**Response to**

**Request for Additional Information No. 414(4394, 4398, 4752, 4548), Revision 1**

**6/15/2010**

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

**AREVA NP Inc.**

**Docket No. 52-020**

**SRP Section: 07.02 - Reactor Trip System**

**SRP Section: 07.03 - Engineered Safety Features Systems**

**SRP Section: 07.04 - Safe Shutdown Systems**

**SRP Section: 07.07 - Control Systems**

**Application Section: FSAR Chapter 7**

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

**DRAFT**

**Question 07.02-32:**

**OPEN ITEM**

Address the rates of change of variables to be accommodated until proper completion of the protective action is ensured.

Clause 4.4 of IEEE Std. 603-1991 requires the documentation of the variables or combinations of variables, or both, that are to be monitored to manually or automatically, or both, control each protective action; the analytical limit associated with each variable, the ranges (normal, abnormal, and accident conditions); and the rates of change of these variables to be accommodated until proper completion of the protective action is ensured. Section 7.2.2.1.3 of U.S. EPR FSAR did not identify the rates of change of variables to be accommodated until proper completion of the protective action is ensured. Identify where in the U.S. EPR FSAR this information is addressed or provide this level of information.

**Response to Question 07.02-32:**

A response to this question will be provided by March 1, 2011.

DRAFT

**Question 07.02-33:****OPEN ITEM**

Identify how many buttons must be pressed to send a reactor trip signal from the Main Control Room and the Remote Shutdown Station.

Clause 6.2.1 of IEEE Std. 603-1991 states that means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1. Section 7.2.1.2.22 of U.S. EPR FSAR states the capability for manual reactor trip is provided to the operator through the Safety Information and Control System in both the Main Control Room and Remote Shutdown Station, and at each location, four manual reactor trip buttons are provided to correspond to the four Protection System divisions. In the Main Control Room, how many buttons must be pressed to send a trip signal? In the Remote Shutdown Room, how many buttons must be pressed to send a trip signal? Figure 7.2-3 of U.S. EPR FSAR shows manual reactor trip logic for one division. Please provide a logic diagram that incorporates how many divisional buttons must be pushed to initiate a reactor trip for both MCR and RSS. In the applicant's response, please update both U.S. EPR FSAR and U.S. EPR Digital Protection System Technical Report.

**Response to Question 07.02-33:**Reactor Trip Devices

As shown in U.S. EPR FSAR Tier 2, Figure 7.2-4, the reactor trip (RT) breakers are arranged in a "one out of two taken twice" configuration. This requires opening of RT breakers in the logical equation (1 or 2) and (3 or 4) to achieve a RT. Two buttons must be pressed for the RT breakers to de-energize the control rod drive mechanisms (CRDMs);, one in Divisions 1 or 2 and one in Divisions 3 or 4.

The RT contactors are shown in Figure 7.2-4. There are 23 sets of four contactors, each arranged in a standard two-out-of-four configuration. Two buttons must be pressed for the trip contactors to de-energize the CRDMs, in any two of the four divisions.

Main Control Room

As indicated in Section 7.6 of Reference 1, any two of four dedicated RT buttons in the main control room (MCR) together will actuate an RT. This is because the MCR RT buttons act on both the RT breakers and RT contactors, as illustrated in Figure 7-4 of Reference 1.

Remote Shutdown Station

As illustrated in Figure 7-4 of Reference 1, the four RT buttons in the remote shutdown station (RSS) act only on the RT breakers. Because of the RT breaker "one out of two taken twice" arrangement, the same logical arrangement applies to the four RT buttons: Div 1 or Div 2 and Div 3 or Div 4 to achieve RT.

U.S. EPR FSAR Tier 2, Section 7.2.1.2.22 will be revised to add the summary of manual RT buttons pressed to initiate the RT in both MCR and RSS.

**References:**

1. ANP-10309P, revision 0, "U.S. EPR™ Digital Protection System Technical Report," AREVA NP Inc., November 2009.

**FSAR Impact:**

U.S. EPR FSAR, Tier 2, Section 7.2.1.2.22 will be revised as described in the response and indicated on the enclosed markup.

DRAFT

**Question 07.03-30:****OPEN ITEM****Follow-up to RAI 285, Question 07.03-25.**

The staff requests that the applicant provide the following information:

2. Explain and/or clarify exactly what components are involved in the 'response time testing' of the PS in the PS ITAAC and surveillance testing. The Chapter 15 definition remains somewhat vague and the presentation by the applicant on surveillance testing says that the testing is from sensor to final actuating device. The applicant's response to RAI Question 07.09.47 would seem to be in conflict with this.
3. Based upon the applicant's response to RAI Question 07.09.47, explain and/or clarify why the applicant believes that the PACS does not need to be involved in the overall response time testing of the PS. The PACS modules are specific to ESFAS and ESFAS actuations cannot occur without the PACS. They are digital devices that are part of the overall logic chain for an ESFAS actuation.

**QUESTION BASIS:**

IEEE Std. 603-1998, Clause 4.d, requires, in part, that the U.S. EPR DCD document the variables or combinations of variables used by the ESF actuation system to be monitored manually or automatically. Also Clause 4.d requires the U.S. EPR DCD to document the analytical limit associated with each variable, the ranges and rates of change of these variables till completion of protective action is ensured.

The staff issued RAI 957, Question 07.03-11, in order to get clarification on this issue. The applicant provided an initial response to this RAI question in which it stated that ESF response times are documented in the U.S. EPR DCD Tier 2, Table 15.0-8, and that the PS response times will be tested and verified according to the ITAAC documented in the U.S. EPR DCD Tier 2, Section 14.2.12.10 Test #146. The applicant provided its response to RAI 78, Supplement 2, which contained the FSAR markups for Question 07.03-11.

Based upon the review of the applicant's response, the staff created a supplemental RAI 285, Question 07.03-25. In response to Question 07.03-25, the applicant commits to adding specific testing for ESF response times to support the Chapter 15 accident analyses.

In response to RAI Question 07.09.47, the applicant states the following:

*“ The bounding PS response times discussed in the Second Request for Additional Information for ANP-10281(P), Attachment B are consistent with the response time assumptions used in the accident analysis and listed in U.S. EPR FSAR Tier 2, Table 15.0-7 and Table 15.0-8. If needed, AREVA NP can provide supporting documentation, such as a function-by-function demonstration of consistency, for NRC audit. Refer to U.S. EPR FSAR Tier 1, Section 2.4.1, Item 4.24 and associated ITAAC , which has been added in the Response to RAI 285 Supplement 4, Question 07.03-25 and addresses verification that the PS response times support accident analysis assumptions.*

*The Second Request for Additional Information for ANP-10281(P), Attachment B, Paragraph one states: "The total response time for a given function consists of several sub-intervals that span from a process variable exceeding a pre-defined limit to completion of the protective function. The sub-interval addressed herein accounts for the computerized portion of the protection channel, and is defined as the time from sensor conditioning output to RT breaker input terminals for RT functions, or to input terminals of the PACS for ESF actuation functions." The priority and actuator control system (PACS) is not included in the PS response time analysis. Time delays introduced by the priority module in the PACS are included with the response time of the actuator it controls and is verified through response time testing of the actuator."*

US EPR DCD, Tier 2, Chapter 15, Page 15.0-58, states the time delays(response times):

"...Represents the total time for completion of the function. Includes sensor delay, I&C delay, and other delays as noted until the function is completed."

In addition, in a presentation made to the staff concerning continuous self-testing of the PS, the applicant stated:

"The Protection System response time shall be that time interval from when the monitored parameter exceeds its PS actuation setpoint at the division sensor until the PS equipment is capable of performing its safety function."

The applicant states that the PACS system has not been included in the response times. This appears to be in conflict with the definition of the response times for completion of ESF actuation in Chapter 15. The Chapter 15 definition makes no distinction between the computerized portions of the PS and the PACS, and implies that the response times would envelope all timing delays from sensor to final actuation device. It should also be noted that the PACS ITAAC in U.S. EPR DCD, Tier 1, Section 2.4.5 makes no mention of response timing. Emergency Feedwater (EFW) is an ESF. The ITAAC for EFW is in U.S. EPR DCD, Tier 1, Section 2.2.4. There is no mention of response timing, in terms of valve stroke time with the PACS module, mentioned in the ITAAC. There is also no mention of response time testing in order to meet the bounding times of the Chapter 15 safety analyses. This appears to be in conflict with what the applicant states in its response to RAI Question 07.09-47. If the response timing of the PACS is not listed in either the PS, PACS or any other ESF ITAAC, then the staff cannot have confidence that the as-built configuration of the PS will meet the bounding response times of the Chapter 15 safety analyses.

**Note:** The applicant has committed to meeting the guidance of Regulatory Guide 1.118, "Periodic Testing of Electric Power and Protection Systems". RG 1.118 cites 10 CFR Part 50, Appendix A, GDC 21, as a regulatory basis and endorses IEEE Std. 338-1987, "IEEE Standard Criteria for Periodic Surveillance Testing of Nuclear Power Generating Station Safety Systems". Section 6.3.5 of IEEE Std. 338-1987, "Logic System Functional Test" states:

"A logic system functional test shall test all logic components from sensor through to the actuated device. Logic components consist of relays, contacts, and solid-state logic elements of a logic circuit. The test may be performed by a series of sequential, overlapping, or total system tests so that an entire logic system is tested."

While the applicant does not consider the PACS as part of the computerized portions of the PS, it is a part of the 'entire logic system' for ESFAS and would be considered a part of a logic system functional test.

**Response to Question 07.03-30:**

The "response time testing" of the protection system (PS) in the PS ITAAC and surveillance testing is the testing of the "time delay" as defined in U.S. EPR FSAR Tier 2, Table 15.0-7 and Table 15.0-8. This "time delay" includes I&C delay. The I&C delay time listed includes PS equipment response time and PACS equipment response time.

The statement in the Response to RAI Question 07.09-47 does not contradict this statement because the context of RAI Question 07.09-47 is only the response time of the computerized portion of the PS, which as described does not include priority and actuator control system (PACS) equipment. The statement, "The...PACS is not included in the PS response time analysis," does not refer to the total response time of the overall I&C delay, which does include the PS equipment and PACS equipment, but only to the "computerized portion of the Protection System."

The response time testing does test the response time of the "entire logic system which includes the PAC's time response."

The term "I&C delay" in note 2 of U.S. EPR FSAR Tier 2, Table 15.0-7 and note 4 of U.S. EPR FSAR Tier 2, Table 15.0-8 will be clarified to include the PS computerized portion and PACS delays.

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Table 15.0-7 and Table 15.0-8 will be revised as described in the response and indicated on the enclosed markup.

**Question 07.03-31:****OPEN ITEM****Follow-up to RAI 285, Question 07.03-26.**

IEEE Std. 603-1998, Clause 4.k, requires documentation of equipment protective provisions that prevent the safety systems from accomplishing their safety functions. The staff used SRP Appendix 7.1-C as guidance in the review of conformance to Clause 4.k. Clause 4.k is not addressed in the U.S. EPR DCD Tier 2, FSAR Section 7.3. Per U.S. EPR DCD Tier 2, FSAR Section 7.1.2.6.10, U.S. EPR DCD Tier 2, FSAR Chapters 5, 6, 8, 9, 10 and 11 contain descriptions on this requirement. However, the applicant does not state whether there are, or are not, any equipment protective features that can prevent a safety actuation of ESF. As such, the staff found there was insufficient detail to finalize an evaluation for this clause. RAI 957, Question 07.03-14 (ML091630750) was issued to clarify the issue. In its response, the applicant states the functional requirements for the PS do not include any provisions for protective features that could prevent safety functions. The applicant goes on to state that should the design of the PS change in the future to add such a feature, that this would be documented consistent with IEEE Std. 603-1998, Clause 4.k. The applicant did not commit to clearly stating this fact in the FSAR.

The staff is looking for the applicant to clearly state in the FSAR that the current design of the U.S. EPR does not have any equipment features that would prevent a safety system from accomplishing its safety function. If, in the future, the design of the U.S. EPR introduces a protective feature that would prevent a safety system from accomplishing its safety function, then the applicant should take the necessary steps to document this fact in the FSAR and the staff would review that design change. That does not alleviate the responsibility of the applicant from clearly stating in the latest FSAR revision the design aspects of the current U.S. EPR PS design with respect to IEEE Std. 603-1998, Clause 4.k. The staff created RAI 285, Question 07.03-26, as a supplemental question. In its response, the applicant attempted to clarify its initial response by stating:

“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.”

The applicant's second response has provided valuable information that allowed the staff to better understand the applicant's position. The staff agrees with applicant's position that a failure to actuate due to an equipment protective feature would be bounded by the single failure analyses. With that said, this information should be added to the FSAR if the bounding single failure analyses is ultimately the reasons why the applicant believes the U.S. EPR PS system design has no equipment protective features that can prevent a safety system actuation. This supplemental question has been created to ensure that the applicant commits to stating in the

U.S. EPR DCD that there are no equipment protective features that prevent safety system actuation and provide more detail as to why this is true.

**Response to Question 07.03-31:**

U.S. EPR FSAR Tier 2, Section 7.1.2.6.9 will be revised to include the single failure criterion information requested in this question.

**FSAR Impact:**

U.S. EPR FSAR Tier 2, Section 7.1.2.6.9 will be revised as described in the response and indicated on the enclosed markup.

DRAFT

**Question 07.04-14:****OPEN ITEM****Follow-up to RAI 309, Question 07.09-60.**

The applicant provided information in response to the RAI 309 Question 07.09-60, which needs to be included in the U.S. EPR FSAR.

In its original RAI, the staff requested the applicant to demonstrate how the various data networks in the main control room (MCR), in the event of a control room fire, would not affect the capability to achieve safe shutdown, given that the plant data network, the terminal data network, and other components are shared between the MCR workstations and the Remote Shutdown Station (RSS) workstations.

10 CFR 50, Appendix R, III.G, "Fire Protection of Safe Shutdown Capability," requires, in part, fire protection features be provided for structures, systems, and components important to safe shutdown. Tier 2, Section 9.5.1.1 of the U.S. EPR Final Safety Analysis Report (FSAR) states that because of the MCR physical configuration, for a fire in the MCR, an independent alternative shutdown capability (RSS) that is physically and electrically independent of the MCR is used to achieve safe shutdown conditions. Tier 2, Section 7.1.1.3.1 and Section 7.1.1.3.2 of the U.S. EPR FSAR describe the capabilities of the SICS and PICS to achieve both hot and cold shutdown conditions from the RSS in case of a fire in the MCR. However, Tier 2, Figure 7.1-5 "Process Information and Control System Architecture" depicts the terminal data network being shared by both the MCR operator workstations and the RSS operator workstations. In addition, the terminal data network is connected to the plant data network through Process Units (PUs). Demonstrate that in the event of a fire in the MCR, the terminal data network, and the plant data network will not be impacted such that the RSS workstations maintain the capability for hot and cold shutdown to meet the requirements of 10 CFR 50, Appendix R, III.G.

The applicant provided a response to RAI 309 Question 07.09-60 and stated in part that the PUs and plant data network are physically located in a separate fire area from the MCR, and are therefore unaffected by fire in the MCR. The terminal data network hardware is located so that damage from a fire event in the MCR will be limited to network components required for the operation of MCR workstations and have no impact on the overall functionality of the terminal data network. Portions of the network required for operation from the RSS are located in a separate fire area from the MCR, so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not impact the ability to safely shutdown the plant from the PICS workstations in the RSS.

The staff requests that this information be included in the U.S. EPR FSAR.

**Response to Question 07.04-14**

The following paragraph will be added to U.S. EPR FSAR, Tier 2, Section 7.1.1.3.2:

"The PUs and plant data network are physically located in a separate fire area from the MCR, and are therefore unaffected by fire in the MCR. The terminal data network hardware is located so that damage from a fire event in the MCR will be limited to network components required for the operation of MCR workstations and have no impact on the

overall functionality of the terminal data network. Portions of the network required for operation from the RSS are located in a separate fire area from the MCR, so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not impact the ability to safely shutdown the plant from the PICS workstations in the RSS.”

**FSAR Impact:**

U.S. EPR FSAR, Tier 2, Section 7.1.1.3.2 will be revised as described in the response and indicated on the enclosed markup.

DRAFT

**Question 07.07-20:****OPEN ITEM**

Provide the design descriptions and design commitments for the RCSL software development process.

10 CFR 52.47(a)(2) requires, in part, that the description and analysis of the structures, systems, and components (SSCs) of the facility, shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. 10 CFR 52.47(a)(9) states, in part, that the application must contain a final safety analysis report (FSAR) that describes the facility, presents the design bases, and must include ... an evaluation of the standard plant design against the Standard Review Plan (SRP) revision in effect 6 months before the docket date of the application. The guidance of SRP 7.7 states that control system software should be developed using a structured process similar to that applied to safety system software and that elements of the review process may be tailored to account for the lower safety significance of control system software. U.S. EPR FSAR Tier 2, Section 7.1.1.4.5 state that there are no quality requirements or qualification requirements for RCSL equipment. The staff could not identify U.S. EPR FSAR design descriptions that would address the software quality development process for the RCSL control system that would address SRP 7.7 guidance. Therefore, the staff request the applicant to address the software quality guidance of SRP 7.7 for the RCSL control system software.

**Response to Question 07.07-20:**

The reactor control, surveillance and limitation (RCSL) control system is not an event mitigating system from U.S. EPR FSAR Tier 2, Chapter 15. As with any non-safety system design, quality requirements providing reliable and consistent system operation will be applied during software development. Potential malfunctions of this software are bounded by U.S. EPR FSAR Tier 2, Chapter 15 accident analyses resulting in mitigation of initiating events by the safety-related protection system

The intent of the quality and qualification statement in U.S. EPR FSAR Tier 2, Section 7.1.1.4.5 is not to indicate that there is no quality and qualification requirement for the RCSL but that the quality and qualification requirement for the RCSL is not equivalent to that of safety-related equipment.

The quality and qualification statement in U.S. EPR FSAR Tier 2, Section 7.1.1.4.5 for RCSL will be modified as follows:

**For qualification:**

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

For quality:

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

**FSAR Impact:**

The U.S. EPR FSAR Tier 2, Section 7.1.1.4.5 will be revised as described in the response and indicated on the enclosed markup.

DRAFT

**Question 07.07-22:****OPEN ITEM**

Define and describe the design for the Process Automation System (PAS) components that are referred to as "CU" in the U.S. EPR Final Safety Evaluation Report (FSAR).

10 CFR 52.47(a)(2) requires, in part, that the description and analysis of the structures, systems, and components (SSCs) of the facility, shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. The Chapter 7 Standard Review Plan (SRP) guidance states that the information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. The design bases should not contain contradictory requirements.

As an example, the reactor control, surveillance, and limitation system (RCSL) states that the CU components are called "Control Units." However, the RCSL system is a TXS-based system. The U.S. EPR FSAR Tier 1, Revision 1, Section 2.4.9, design description item 3.2, states that the PAS software and hardware are diverse from TXS based systems (i.e. Protection system and SAS). Also, the diversity, defense-in-depth technical report (D3-TR), "U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report," ANP-10304, Revision 1 [ML093420199], takes credit for the PAS system components being diverse from TXS-based system components. The D3-TR states, in part, that "The PAS equipment is specified to be an industrial control platform other than TXS" and that "This means the PAS equipment will be of fundamentally different design than the PS equipment."

Therefore, since the PAS design is credited with being diverse from TXS based components, such as the RCSL TXS based system, the staff is not able to conclude that the CU components in the PAS are the same CU components as described in the RCSL system. Further, the FSAR design descriptions do not sufficiently describe what the PAS CU components are.

**Response to Question 07.07-22**

"Control Unit (CU)" is a generic term used to identify functional units in various Level 1 I&C systems that perform the same generic types of functions. Any CU performs primarily open and closed loop controls on process components and interfaces with the associated Level 2 system. This term is not technology specific and was not intended to be associated with a specific platform. Each U.S. EPR FSAR Tier 2, 7.1 subsection that uses the term CU defines the individual functions of a CU that is used in that system. It is these functions that should be considered as the design basis of the I&C system in question, rather than the generic term "Control Unit".

Use of the term "Control Unit" is not intended to suggest that the same technology will be used across multiple I&C systems, nor does it invalidate or contradict any diversity and defense-in-depth commitments made by AREVA NP in ANP-10304 or other sources of regulatory commitments.

The following item will be added for clarity to the definition section U.S. EPR FSAR Tier 2, Section 7.1:

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

The diversity of the PAS from Teleperm XS (TXS) based systems will be addressed in the Response to RAI 413, Questions 07.08-10 and 07.08-11.

**FSAR Impact:**

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

DRAFT

# U.S. EPR Final Safety Analysis Report Markups

DRAFT

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

07.07-22

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

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

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

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

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

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

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

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

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

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

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

07.04-14

terminal data network. These networks implement periodic communications and message validation for robust data communications. Remote access of the PICS is not possible. The PUs and plant data network are physically located in a separate fire area from the MCR, and are therefore unaffected by fire in the MCR. The terminal data network hardware is located so that damage from a fire event in the MCR will be limited to network components required for the operation of MCR workstations and have no impact on the overall functionality of the terminal data network. Portions of the network required for operation from the RSS are located in a separate fire area from the MCR, so damage from a fire event in the MCR will be limited to the workstations in the MCR and will not impact the ability to safely shutdown the plant from the PICS workstations in the RSS.

### Power Supply

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

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

#### 7.1.1.4 Level 1 - System Automation

##### 7.1.1.4.1 Protection System

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

### Classification

The PS is classified as safety-related.

### Functions

The PS performs these functions:

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

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

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

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

### Equipment

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

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

07.04-14

#### *Qualification Requirements*

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

~~There are no qualification requirements for the RCSL equipment.~~

07.04-14

#### *Quality Requirements*

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

~~There are no quality requirements for the RCSL equipment.~~

#### *Diversity Requirements*

There are no diversity requirements for the RCSL equipment.

### Data Communications

Data communications implemented in the RCSL are:

- AU-CU – bi-directional, point-to-point data connections implemented with the TXS Profibus protocol.

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

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

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

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

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

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

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

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

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

07.03-31

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. 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. How the safety systems meet the requirements of the single failure criterion is explained in Section 7.1.2.6.12.

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

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

There are no operating bypasses associated with this function; any automatic SI actuation will result in RT.

Automatic actuation of the SIS is described in Section 7.3, and the logic for generation of the SI signal is shown in Figure 7.3-2—SIS Actuation. The logic combining the safety injection signal with the remainder of the RT signals is shown in Figure 7.2-24—RT Signal Generation.

#### 7.2.1.2.21 Reactor Trip on Emergency Feedwater System Actuation

This function is provided to trip the reactor when the emergency feedwater system (EFWS) is actuated by the PS due to low SG level.

In each division of the PS, when an EFWS actuation signal is generated due to low SG level (regardless of the EFWS train to be initiated), an RT signal is also generated in the same division.

The P13 permissive condition bypasses the RT on EFWS actuation function at low temperatures as measured in the hot legs. This bypass is automatically removed as hot leg temperature increases above the P13 setpoint. Generation of the P13 permissive signal is described in Section 7.2.1.3.

Automatic actuation of the EFWS is described in Section 7.3, and the logic for generation of the EFWS actuation signal is shown in Figure 7.3-3. The logic combining the EFWS actuation signal with the remainder of the RT signals is shown in Figure 7.2-24.

#### 7.2.1.2.22 Manual Reactor Trip

The capability for manual RT is provided to the operator through the SICS in both the MCR and RSS. At each location, four manual RT buttons are provided to correspond to the four PS divisions. Manual RT from the MCR is hardwired to bypass the electronics of the PS and act directly on the undervoltage coils of the RT breakers. The MCR initiation signal is also acquired by the PS and processed with the automatic RT functions. Manual RT from the RSS is hardwired to bypass the electronics of the PS and act directly on the shunt trip coils of the RT breakers. Manual RT initiation is illustrated in Figure 7.2-3. Manual RT is described further in Reference 1. The logic combining the manual RT signal from the MCR with the automatic RT signals is shown in Figure 7.2-24.

07.02-33

In the MCR, any two of four dedicated manual RT buttons together will actuate an RT, in the RSS, the following combination of the dedicated manual RT buttons in the RSS will actuate an RT: (Div 1 or Div 2) and (Div 3 or Div 4).

NP - Nominal power - it should be noted that other terms are also used to depict reactor power, thermal power, rated thermal power, etc. Under steady-state conditions, these are equivalent.

NF - Nominal flow

NS - Nominal speed

NR - Narrow range

07.03-30

2. For RT functions the time delay is from the time the value is sensed at the sensor until the stationary gripper releases. It includes sensor delay, I&C delay (includes PS computerized portion, and PACS delays), and the delay for the trip breakers to open and the stationary gripper to release.
3. FWLB has conservatively assumed a setpoint of 0% NR.
4. A TT is credited following an RT. The PS is designed to issue the trip signal to the turbine island system after a one-second delay.
5. The PS includes an RT on high containment pressure. This trip is not credited in the analysis presented in this section; however, it is credited in the containment analysis presented in Chapter 6.
6. This safety-related signal was not explicitly credited in the safety analyses. However, the Low Saturation Margin reactor trip function assures that the High Core Power Level trip function is not invalidated.
7. The pressure setpoint is variable and tracks the steam line pressure with a constant offset (102 psi). The setpoint has a limitation on its maximum pressure (1087.7 psia) and its maximum rate of decrease (29 psi/min). If the steamline pressure decreases more rapidly than the allowable rate, then the margin between the actual pressure and the setpoint decreases until the steam line pressure is less than the setpoint generating an RT.
8. The uncertainty related to this RT function is discussed in Reference 2.

**Table 15.0-8—Engineered Safety Features Actuation System (ESFAS)  
Functions Used in the Accident Analysis  
(Sheet 4 of 4)**

Function	Setpoint	Uncertainty (Normal/Degraded)	Time Delay (seconds) <sup>4</sup>
<b>MCR AC System isolation</b>			
MCR air intake activity > Max1p	3 X background		
<b>Turbine Trip on RT</b>			
Confirmation of RT	Following RT	Not Applicable	1.0
<b>EDG on LOOP or degraded voltage<sup>17</sup></b>			
EBS	Manual	Not Applicable	Not Applicable
<b>Hydrogen Mixing Dampers Opening</b>			
<u>Cont. Service Compartment Pressure (NR)</u>	<u>17.4 psia</u>	<u>±0.5 psia</u>	<u>18</u>
<u>Equipment Room and containment service compartment ΔP</u>	<u>0.5 psi</u>	<u>±30%</u>	<u>18</u>

**Notes:**

1. EFWS actuation on LOOP and SIS is assumed in the SGTR to minimize the margin to overfill. It is also credited in SBLOCA. This function does not have a specific setpoint, uncertainty, or delay.
2. The accident analysis does not credit automatic actions based on MSL activity but uses MSL activity for input to operator action. This function does not have a specific setpoint, uncertainty, or delay.
3. EFWS actuation also results in SG blowdown isolation.
4. Represents the total time for completion of the function. Includes sensor delay, I&C delay (includes PS computerized portion, and PACS delays), and other delays as noted until the function is completed.
5. The setpoints for the anti-dilution PS vary as a function of core burnup and are specified in the Core Operating Limits Report.
6. The first time accounts for time delays in trip processing, the second time accounts for the stroke time of the CVCS isolation valves.
7. A bounding uncertainty of 400 ppm is used.
8. Varies with boron concentration.
9. The partial cooldown actuation signal is initiated on the SIS signal and therefore does not have a specific setpoint, uncertainty, or delay.

07.03-30