ArevaEPRDCPEm Resource

From:	Tesfaye, Getachew
Sent:	Tuesday, June 08, 2010 10:40 AM
To:	'usepr@areva.com'
Cc:	Truong, Tung; Morton, Wendell; Spaulding, Deirdre; Mott, Kenneth; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject:	Draft - U.S. EPR Design Certification Application RAI No. 414(4394, 4398,4752,4548), FSAR Ch. 7 OPEN ITEM
Attachments:	Draft RAI_414_ICE1_4394_4398_4752_4548.doc

Attached please find draft RAI No. 414 regarding your application for standard design certification of the U.S. EPR. If you have any question or need clarifications regarding this RAI, please let me know as soon as possible, I will have our technical Staff available to discuss them with you.

Please also review the RAI to ensure that we have not inadvertently included proprietary information. If there are any proprietary information, please let me know within the next ten days. If I do not hear from you within the next ten days, I will assume there are none and will make the draft RAI publicly available.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 1504

Mail Envelope Properties (0A64B42AAA8FD4418CE1EB5240A6FED11914510ECF)

Subject: Draft - U.S. EPR Design Certification Application RAI No. 414(4394, 4398,4752,4548), FSAR Ch. 7 OPEN ITEM
Sent Date: 6/8/2010 10:40:27 AM
Received Date: 6/8/2010 10:40:30 AM
From: Tesfaye, Getachew

Created By: Getachew.Tesfaye@nrc.gov

Recipients:
"Truong, Tung" <Tung.Truong@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Spaulding, Deirdre" <Deirdre.Spaulding@nrc.gov>
Tracking Status: None
"Mott, Kenneth" <Kenneth.Mott@nrc.gov>
Tracking Status: None
"Jackson, Terry" <Terry.Jackson@nrc.gov>
Tracking Status: None
"Canova, Michael" <Michael.Canova@nrc.gov>
Tracking Status: None
"Colaccino, Joseph" <Joseph.Colaccino@nrc.gov>
Tracking Status: None
"ArevaEPRDCPEm Resource" <ArevaEPRDCPEm.Resource@nrc.gov>
Tracking Status: None
"'usepr@areva.com'" <usepr@areva.com>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	727	6/8/2010 10:40:30 AM
Draft RAI_414_ICE1_4394_4398_4752_4548.doc		53754

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

Draft

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

6/08/2010

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)

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.

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.

07.03-30

OPEN ITEM

Follow-up to RAI 285, Question 07.03-25.

The staff requests that the applicant provide the following information:

1. 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.
2. Based upon the applicant's response to RAI Question 07.09.47, **e**xplain 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 14.2.12.12.10 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 compterized portions of the PS and the PACS, and implies that the response times would envelope all timing delays from sensor to final actuation device. Its 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 Quesiton 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 Crieteria 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.

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.

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.

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.

07.07-21

[Intentionally deleted]

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.