ArevaEPRDCPEm Resource

From: Tesfaye, Getachew
Sent: Thursday, April 28, 2011 3:59 PM
To: 'usepr@areva.com'
Cc: Zhang, Deanna; Zhao, Jack; Spaulding, Deirdre; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: Draft - U.S. EPR Design Certification Application RAI No. 485 (5743), FSAR Ch. 7
Attachments: Draft RAI_485_ICE1_5743.doc

Attached please find draft RAI No. 485 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: 2905

Mail Envelope Properties (0A64B42AAA8FD4418CE1EB5240A6FED126A30DCA68)

Subject: Draft - U.S. EPR Design Certification Application RAI No. 485 (5743), FSAR Ch. 7
Sent Date: 4/28/2011 3:59:05 PM
Received Date: 4/28/2011 3:59:08 PM
From: Tesfaye, Getachew

Created By: Getachew.Tesfaye@nrc.gov

Recipients:
"Zhang, Deanna" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Zhao, Jack" <Jack.Zhao@nrc.gov>
Tracking Status: None
"Spaulding, Deirdre" <Deirdre.Spaulding@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	795	4/28/2011 3:59:08 PM
Draft RAI_485_ICE1_5743.doc	43002	

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

Draft

Request for Additional Information No. 485(5743), Revision 0

4/28/2011

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.09 - Data Communication Systems
Application Section: 7.9

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

07.09-68

Describe how the non-safety related switch between the protection system (PS) and safety automation system (SAS) monitoring and service interfaces (MSIs) and the process information and control system (PICS) provides sufficient independence and quality to serve as the isolation device between safety and non-safety systems to meet the requirements of Institute of Electrical and Electronics Engineers (IEEE) Std. 603-1998, Clause 5.6.3.

Clause 5.6.3 of IEEE Std. 603-1998 requires safety system design to be such that credible failures in and consequential actions by other systems to not prevent the safety systems from meeting the requirements of this standard. This clause is enumerated by several sub-clauses, including Sub-clause 5.6.3.1, which requires:

1) Equipment that is used for both safety and non-safety functions to be classified as part of the safety systems. Isolation devices used to effect a safety system boundary shall be classified as part of the safety system

2) No credible failure on the non-safety side of an isolation device shall prevent any part of a safety system from meeting its minimum performance requirements during and following any design basis event requiring that safety function. A failure in an isolation device shall be evaluated in the same manner as a failure of other equipment in a safety system.

The applicant submitted a closure plan for the U.S. EPR instrumentation and control (I&C) communication independence issues. Revision 4 of this closure plan (ADAMS Accession Number ML1032800470) states that the U.S. EPR I&C systems design will be modified such that only communication from the PS and SAS to PICS will be allowed. The communication paths will be restricted so that PICS cannot send information to the PS.

The description of these interfaces in Section 7.1.1.6.4 of the U.S. EPR Tier 2 FSAR, Interim Revision 3, and Technical Report ANP 10309, draft Revision 1, states that uni-directional communication flow from the PS and SAS to the PICS is maintained by, and conducted through, a non-safety switch. According to the staff's understanding, the uni-directional communication flow from PS/SAS to PICS was established to demonstrate independence between safety and non-safety systems. Per the requirements of IEEE Std. 603-1998, Clause 5.6.3.1, the isolation device between safety and non-safety systems must be classified as safety-related. As such, the staff finds that the non-safety related switch does not appear to meet the requirements of IEEE Std. 603-1998.

Describe how the non-safety related switch between the PS/SAS MSIs is of sufficient quality to serve as the isolation device between safety and non-safety systems to meet the requirements of IEEE Std. 603-1998, Clause 5.6.3.

07.09-69

Demonstrate that during a design basis event, the vulnerabilities for a postulated software common-cause-failure (SCCF) of all protection system (PS) division's actuation logic units (ALUs) "no-go" test, which continuously blocks the output of all applicable priority modules (PACS), have been adequately addressed and the required protective functions can be accomplished, as required by 10 CFR Part 50, Appendix A, GDC 22.

10 CFR Part 50, Appendix A, General Design Criterion (GDC) 22, "Protection System Independence," 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 protection function. The staff requirements memorandum to SECY-93-087, "Policy, Technical, and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," Item II.Q (ML003708056), Point 1, states that the applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed. Point 3 states that if a postulated common-mode failure could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function.

Each PS division contains four ALUs; two assigned to each subsystem. For engineered safety features actuation system (ESFAS) protective functions, the ALU logic performs voting, actuation logic (e.g., checking permissive conditions, sequencing), signal latching, and output of ESFAS actuation orders. Therefore, a postulated SCCF of the ALU logic could fail any one or all of these logic functions. Figure 2-5, "ESFAS "No-Go" Test Concept," in Technical Report ANP-10315, "U.S. EPR Protection System Surveillance Testing and TELEPERM XS Self-Monitoring Technical Report," Revision 0, shows that a SCCF of the ALU logic's no-go test blocking signal would block the ESFAS actuator initiation output signal of the PACS. The PACS collects the actuation signals from multiple I&C systems (both safety and non-safety related, including diverse actuation system,) and transfers the proper actuation order to the ESFAS actuator according to pre-defined priority assignments.

Technical Report ANP-10315, Section 2.2.5.1.1, states that the blocking signal lasts for 5 seconds and is overridden if, at any time during a 5-second period, a legitimate protection function is initiated. In addition, system-level manual ESFAS actuations initiated by the operator from the safety information and control system are sent to and combined with the ALU logic. It is the staff's understanding that the ALU performs both the blocking action and the release action for the PACS no-go test. According to NUREG/CR-6303, "Method for Performing Diversity and Defense-in-Depth Analyses of Reactor Protection Systems" (ML071790509), when postulating a system SCCF, it cannot be assumed that a failed PS component can produce incorrect and correct outputs. As stated in NUREG/CR-6303, Guideline 5, among other things, in blocks containing software, it is credible that outputs shall assume values irrespective of inputs because the only logic connecting inputs to outputs is software, and the effects of software failures on outputs are unpredictable.

As stated in NUREG/CR-6303, Guideline 6, analysis of defense-in-depth should be performed by postulating concurrent failures of the same block or identical blocks (as defined in Guideline 7) in all redundant divisions. Since several channels may pass through the same block or identical blocks, such common-mode failures have the potential to cause multiple channel failures in a single division, with the same failure replicated across all (four) protection system divisions. The output signals of the blocks thus postulated to fail should do so in accordance with Guideline 5. In other words, signals entering failed blocks assume the most adverse credible values on output, essentially losing their protective function at that point. Subject to Guidelines 7, 8, and 9, concurrent failure of each set of identical blocks in all divisions should be postulated in turn (until the list of diverse blocks has been exhausted), and the result of the failure should be documented as a finding of the analysis.

Given that the ALUs perform both the block and release function for the PACS no-go test, describe how a SCCF of the ALU that blocks and fails to release the PACS outputs is addressed.

07.09-70

The staff requests the applicant provide additional detail on the implementation of the service unit (SU) in terms of design functionality and administrative controls for plant operations.

10 CFR 52.47(a)(2) requires, in part, that the design descriptions of systems, structures and components shall be sufficient to permit understanding of the system design and their relationship to the safety evaluations. The staff understands that the SU is a non-safety tool that was originally planned to be permanently connected to the safety-related PS and SAS. To address independence between the non-safety SU and the safety systems, the design was altered, as described in interim Revision 3 of the U.S. EPR Design Control Document, Tier 2, Section 7.1, to have the SU disconnected during plant operation. The staff recognizes that the SU would need to be connected to support surveillance testing and maintenance similar to other maintenance and test equipment. However, administrative controls would need to be in place to ensure the SU is not connected beyond these circumstances since the credited independence mechanism between the SU and the safety systems is physical disconnection. Within interim Revision 3 Section 7.1, the staff noted that for the various operating modes of the TELEPERM XS-based safety systems (PS and SAS), when the SU is connected, the processors would be considered inoperable per Technical Specifications except for the cyclic processing mode. Currently, the staff does not see sufficient administrative controls to limit connection of the SU when the processors are in the cyclic processing mode (i.e., SU could be connected indefinitely in this mode).

Given the above-mentioned concerns, the staff requests the following items be addressed:

a. Provide sufficient criteria to limit SU connectivity to PS and SAS for the cyclic processing mode of the TELEPERM XS processors.

b. Provide an estimate of the amount of time per week, and per shift, that the SU would need to be plugged into a PS or SAS division to perform tasks that support plant operations and maintenance or for any other reasons.

c. Identify the specific tasks the SU would be performing, on a per function processor basis, and on a per function (PS and SAS) basis and match these tasks to their Technical Specification operability designation.

d. Explicitly state that the SU can only perform the functions stated in the U.S. EPR FSAR, and while the SU is not in use, it will be fully disconnected from safety-related structures, systems and components (SSCs).

e. Define in specific terms, what is meant when a function processor's outputs are disabled and differentiate in terms of divisional and system-level impact to PS acquisition and processing units (APUs) PS ALUs and SAS control units(CUs). Match this refined definition to specific tasks in which the SU will be performing (refer to item 3).