

ArevaEPRDCPEm Resource

From: Tesfaye, Getachew
Sent: Thursday, February 25, 2010 11:38 AM
To: 'usepr@areva.com'
Cc: Suggs, LaDonna; Spaulding, Deirdre; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
Subject: Draft - U.S. EPR Design Certification Application RAI No. 373 (4393), FSAR Ch. 7
Attachments: Draft RAI_373_ICE1_4393.doc

Attached please find draft RAI No. 373 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: 1172

Mail Envelope Properties (0A64B42AAA8FD4418CE1EB5240A6FED10E0E8CDC29)

Subject: Draft - U.S. EPR Design Certification Application RAI No. 373 (4393), FSAR Ch.
7
Sent Date: 2/25/2010 11:37:55 AM
Received Date: 2/25/2010 11:37:54 AM
From: Tesfaye, Getachew

Created By: Getachew.Tesfaye@nrc.gov

Recipients:

"Suggs, LaDonna" <LaDonna.Suggs@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	732	2/25/2010 11:37:54 AM
Draft RAI_373_ICE1_4393.doc	39418	

Options

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

Draft

Request for Additional Information No. 373(4393), Revision 1

2/25/2010

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)

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.

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.

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.

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.

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.