ArevaEPRDCPEm Resource

From: Getachew Tesfaye
Sent: Friday, December 12, 2008 2:38 PM
To: Pederson Ronda M (AREVA NP INC)
Cc: Deanna Zhang; Deirdre Spaulding; Terry Jackson; Michael Canova; Joseph Colaccino; John Rycyna; ArevaEPRDCPEm Resource
Subject: Draft Third RAI - Digital Protection System TR - ANP-10281P
Attachments: Draft RAI-3 ANP-10281 DPS TR.doc

Ronda,
Attached please find a draft of the third round of RAIs for the Digital Protection System Topical Report (ANP-10281P). We will have our technical Staff available to discuss them with you as soon as you are ready. Please call me with a proposed date and time for the telecon.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 29

Mail Envelope Properties (C56E360E9D804F4B95BC673F886381E71827CB611E)

Subject: Draft Third RAI - Digital Protection System TR - ANP-10281P
Sent Date: 12/12/2008 2:37:35 PM
Received Date: 12/12/2008 2:37:37 PM
From: Getachew Tesfaye

Created By: Getachew.Tesfaye@nrc.gov

Recipients:
"Deanna Zhang" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Deirdre Spaulding" <Deirdre.Spaulding@nrc.gov>
Tracking Status: None
"Terry Jackson" <Terry.Jackson@nrc.gov>
Tracking Status: None
"Michael Canova" <Michael.Canova@nrc.gov>
Tracking Status: None
"Joseph Colaccino" <Joseph.Colaccino@nrc.gov>
Tracking Status: None
"John Rycyna" <John.Rycyna@nrc.gov>
Tracking Status: None
"ArevaEPRDCPEm Resource" <ArevaEPRDCPEm.Resource@nrc.gov>
Tracking Status: None
"Pederson Ronda M (AREVA NP INC)" <Ronda.Pederson@areva.com>
Tracking Status: None

Post Office: HQCLSTR02.nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	704	12/12/2008 2:37:37 PM
Draft RAI-3 ANP-10281 DPS TR.doc	35322	

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

DRAFT

THIRD REQUEST FOR ADDITIONAL INFORMATION (RAI)

ANP-10281P, "U.S. EPR DIGITAL PROTECTION SYSTEM

TOPICAL REPORT" (TAC NO. MD4977)

DOCKET NO. 52-020

RAI-37. Demonstrate that the U.S. EPR digital protection system (PS) design and architecture for providing Self Powered Neutron Detector (SPND) measurements between the remote acquisition units (RAU) and certain acquisition and processing units (APU) are not susceptible to single failure as required by General Design Criterion (GDC) 21 of 10 CFR 50, Appendix A.

GDC 21 states, in part, that the protection system shall be designed for high functional reliability and inservice testability commensurate with the safety functions to be performed. Redundancy and independence designed into the protection system shall be sufficient to assure that (1) no single failure results in loss of the protection function and (2) removal from service of any component or channel does not result in loss of the required minimum redundancy unless the acceptable reliability of operation of the protection system can be otherwise demonstrated. Section 6.3 of the U.S. EPR Digital Protection System Topical Report discusses the RAU-APU architecture. This section states that the measurements from the SPNDs are required for processing by the APU within each division of the PS. While the RAU in each division only acquires one-fourth of the SPND measurements, all 72 measurements are required by the APU in each division to accurately compute the 3-D power distribution. Therefore, communication from the RAU to the APU is established to satisfy this requirement. The RAU – APU architecture consists of five redundant ring topology networks. The first four networks each connect the RAU 1 of all four divisions to two APUs in one division. The fifth network connects the RAU 2 of the four divisions to the APU in the four divisions. Therefore, the fifth network is redundant to the first four networks collectively.

Provide information to demonstrate how GDC 21 is met. Specifically, given that when RAU1 within a division is removed from service and RAU2 within the same division has a single failure, demonstrate how the protective functions provided by the SPND measurements continue to be accomplished. Describe how many SPND measurements out of the 72 total measurements are required to complete the required protective function. In addition, provide a detailed description of the method by which the multiple measurements are used to arrive at the estimated power level and the method for determining the uncertainty in the measured power level. Include in the analyses the assumptions employed regarding the ability of the digital network to reliably acquire and transfer information, including timing considerations.

RAI-38. Describe the failure modes of the ring communications network employed in the U.S. EPR digital protection system (PS) to provide Self Powered Neutron Detector (SPND) measurements between the remote acquisition units (RAU) and certain acquisition

and processing units (APU) as required by General Design Criterion (GDC) 23 of 10 CFR 50, Appendix A.

GDC 23 states, in part, that the protection system shall be designed to fail into a safe state or into a state demonstrated to be acceptable on some other defined basis if conditions such as disconnection of the system, loss of energy (e.g., electric power, instrument air), or postulated adverse environments (e.g., extreme heat or cold, fire, pressure, steam, water, and radiation) are experienced." Section 6.3 of the U.S. EPR Digital Protection System Topical Report discusses the RAU-APU architecture. This section states that the measurements from the SPNDs are required for processing by the APU within each division of the PS. While the RAU in each division only acquires one-fourth of the SPND measurements, all 72 measurements are required by the APU in each division to accurately compute the 3-D power distribution. Therefore, communication from the RAU to the APU is established to satisfy this requirement. The RAU – APU architecture consists of five redundant ring topology networks. The first four networks each connect the RAU1 of all four divisions to two APUs in one division. The fifth network connects the RAU2 of the four divisions to the APU in the four divisions. Therefore, the fifth network is redundant to the first four networks collectively.

Describe how the system design of the APU can accommodate failure (e.g. loss of signal, or loss of confidence in signal) of any one of the first four ring networks (those connected to RAU1). Specifically, describe the methods used by the APU to detect the validity of the SPND measurements, and how measurements acquired from the redundant fifth network are used to provide the estimated power level.

RAI-39. Justify how the three typical implementations of manual system level actuation address IEEE Std. 603-1991, Criterions 5.14 and 6.2.1 and the guidance of Branch Technical Position (BTP) 7-19 and Regulatory Guide (RG) 1.62.

10 CFR 50.55a(h) endorses IEEE Std. 603-1991 as part of the regulations. IEEE Std. 603-1991, Criterion 6.2.1, 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. The staff guidance for addressing this requirement is provided in RG 1.62, Position 4, which states that equipment common to both manual and automatic initiation should be kept to a minimum. Additionally, acceptance criteria in BTP 7-19 of NUREG-0800, Standard Review Plan, states that a set of displays and controls located in the main control room should be provided for manual system-level actuation of critical safety functions and for monitoring of parameters that support safety functions. The displays and controls should be independent and diverse from the computer-based safety systems. Finally, IEEE Std. 603-1991, Criterion 5.14, states, in part, that human factors shall be considered at the initial stages and throughout the design process.

In the NRC staff's second request for additional information (RAI) of the U.S. EPR Digital Protection System (PS) Topical Report, RAI 18, requested the applicant describe the implementation of each manual system level actuation of ESF functions. In response, the applicant provided three typical implementations of ESF functions. Additionally, in the response to RAI 18, the applicant states since the submittal of the

PS Topical Report, regulatory developments in the area of D3 (e.g., interim staff guidance, statements made by the staff in the transcript for the September 13, 2007 ACRS Digital I&C System Subcommittee meeting) have indicated that component level controls implemented through a diverse, non-safety related system are adequate to satisfy BTP 7-19. The staff finds this response inadequate since the final recommendation within the interim staff guidance (Digital I&C-ISG-02 "Diversity and Defense-in-Depth (D3)"), as referred to by the applicant, states:

"In addition to the above, a set of displays and controls (safety or non-safety) should be provided in the main control room for manual system level actuation and control of safety equipment to manage plant critical safety functions, including reactivity control, reactor core cooling and heat removal from the primary system, reactor coolant system integrity, and containment isolation and integrity. The displays and controls should be independent and diverse from the RPS discussed above. However, these displays and controls could be those used for manual operator action as described above. Where they serve as backup capabilities, the displays and controls should also be able to function downstream of the lowest-level software-based components subject to the same common cause failure (CCF) that necessitated the diverse backup system; one example would be the use of hard-wired connections"

This ISG does not stipulate component level controls from a diverse non-safety system are adequate in satisfying BTP 7-19, Position 4. Furthermore, the proposed manual actuation means appears to use large portions of the automatic actuation equipment without adequate consideration for limiting common equipment. Finally, the topical report did not address all manual actuation methods in the control room and how human factors are considered in the proposed design. The staff requests the applicant to demonstrate how Criterions 5.14 and 6.2.1 of IEEE Std. 603-1991, Position 4 of BTP 7-19, Digital I&C ISG-02, as well as Regulatory Position 4 of RG 1.62, have been addressed in the three typical implementations of ESF actuation within the Digital Protection System.