From: Michael Canova
To: Ronda.Pederson@areva.com
Date: 9/27/2007 8:57:47 AM
Subject: Draft RAIs for ANP-10284, U.S. EPR D3 Topical Report

Ronda,
Attached please find a draft of the staff's questions on the subject topical report. 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.
Thanks,

Mike Canova
Project Manager, EPR Branch
Office of New Reactors
U.S. Nuclear Regulatory Commission
301-415-0737

CC: Getachew Tesfaye; John Smith; Norbert Carte

Mail Envelope Properties (46FBA8CB.A52 : 19 : 12190)

Subject:	Draft RAIs for ANP-10284, U.S. EPR D3 Topical Report
Creation Date	9/27/2007 8:57:47 AM
From:	Michael Canova
Created By:	MAC6@nrc.gov

Recipients	**Action**	**Date & Time**
areva.com	Transferred	9/27/2007 8:58:11 AM
Ronda.Pederson (Ronda.Pederson@areva.com)		
nrc.gov		
OWGWPO01.HQGWDO01	Delivered	9/27/2007 8:57:47 AM
NNC CC (Norbert Carte)		
nrc.gov		
TWGWPO02.HQGWDO01	Delivered	9/27/2007 8:57:54 AM
GXT2 CC (Getachew Tesfaye)	Opened	9/27/2007 9:10:21 AM
jms7 CC (John Smith)		

Post Office	**Delivered**	**Route**
OWGWPO01.HQGWDO01	9/27/2007 8:57:47 AM	areva.com nrc.gov
TWGWPO02.HQGWDO01	9/27/2007 8:57:54 AM	nrc.gov

Files	**Size**	**Date & Time**
MESSAGE	868	9/27/2007 8:57:47 AM
First RAIs D3 Topical.doc	55296	9/27/2007 8:22:08 AM

Options

Auto Delete:	No
Expiration Date:	None
Notify Recipients:	Yes
Priority:	Standard
ReplyRequested:	No
Return Notification:	None
Concealed Subject:	No
Security:	Standard
To Be Delivered:	Immediate
Status Tracking:	Delivered & Opened

DRAFT FIRST REQUEST FOR ADDITIONAL INFORMATION

ANP-10284, "U.S. EPR INSTRUMENTATION AND CONTROL

DIVERSITY AND DEFENSE-IN-DEPTH METHODOLOGY

TOPICAL REPORT" (TAC NO. MD5884)

PROJECT NO. 733

RAI 1. Please provide the Diversity and Defense-in-Depth (D3) analysis that is described in the methodology topical report (TR).

Section 1.1 states, "AREVA NP requests the approval of the following items in this report: ... The adequacy of the proposed design features to mitigate the consequences of a postulated CCF [common cause failure] in the safety I&C [Instrumentation and Control] systems."

However, NUREG-0800, Branch Technical Position (BTP) 7-19 states, "... the NRC has established the following four-point position on D3 ...

Point 1. The applicant/licensee should assess the D3 of the proposed I&C system to demonstrate that vulnerabilities to common-cause failures have been adequately addressed.

Point 2. In performing the assessment, the vendor or applicant/licensee should analyze each postulated common-cause failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate or SAR Chapter 15 analysis methods. The vendor or applicant/licensee should demonstrate adequate diversity within the design for each of these events."

Therefore BTP 7-19 states that the adequacy of proposed design features to mitigate the consequences of postulated CCF should be based on an assessment that has been performed.

In order to evaluate the proposed design features, an assessment, or a justification, as to how the alternative proposed (i.e. the methodology for performing the assessment) provides an acceptable method of complying with the rules or regulations, is needed.

RAI 2. Please provide a description of how adequate quality is achieved for the Diverse Actuation System (DAS).

One of the requirements that is addressed by BTP 7-19 is 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram [ATWS]." Section 50.62 (c)(1) states, "...This equipment must be designed to perform its function in a reliable manner..."

AREVA has stated that the DAS will be used to address ATWS requirements. (Section 4.2: "... ATWS evaluations to determine required functionality of the DAS for ATWS mitigation.")

Please provide a description of the DAS that describes how it is designed to perform its function in a reliable manner. (See Generic Letter 85-06 and NUREG-0800, Chapter 7, Section 7.8)

RAI 3. Please provide a description of how the DAS performs its function independent (from sensor output to the final actuation device) from protection system (PS).

One of the requirements that is addressed by BTP 7-19 is 10 CFR 50.62, "Requirements for Reduction of Risk from Anticipated Transients without Scram [ATWS]." Section 50.62 (c)(1) states, "...This equipment must... be independent (from sensor output to the final actuation device) from the existing reactor trip system."

AREVA has stated that the DAS will be used to address ATWS requirements. (Section 4.2: "... ATWS evaluations to determine required functionality of the DAS for ATWS mitigation.")

AREVA has not provided a description of the DAS that describes how it performs its function independent (from sensor output to the final actuation device) from the PS.

Section 2: "The I&C architecture for the U.S. EPR is depicted in Figure 2-1. The I&C architecture is arranged into three levels—Level 2 (Supervisory Control), Level 1 (System Level Automation), and Level 0 (Process Interface). In general, functions (both automatic and manual) are allocated to the various Level 1 systems depending on the safety classification of the function, and what the function is designed for (e.g., rod control, initiation of safety injection). Interfaces are provided within the Level 2 I&C systems for manual functions."

Section 2.5: "In general, the lines of defense apply to the architecture level 1 automation systems."

In the statements of consideration of the final rule for ATWS, the staff documented its understanding regarding the independence of ATWS and Reactor Trip System (RTS) sensors.

49 FR 26040: "Common cause failures in the diverse sensors of the existing reactor trip systems are considered sufficiently unlikely that additional sensor diversity in not necessary. Even though sensor diversity is not necessary, it is desirable that sensors in the existing reactor trip system not be used to provide the signals for the diverse equipment required by this amendment [ATWS Rule]. Use of the same sensors for the existing reactor trip system and the diverse equipment would result in interconnections between the two systems that are hard to analyze and could increase the potential common cause failure affecting both systems." 49 FR 26044: "Additional view of Commissioner Asselstine ... I am not satisfied that sufficient attention has been given to future reactors. It appears that significant additional reduction in the ATWS risk can be achieved without incurring

insurmountable economic costs if such measures are considered during the design phase."

Therefore, the assessment methodology proposed by AREVA does not seem address the regulatory basis, since Level 0 (Process Interface) is excluded from the analysis.

RAI 4. Please provide a description of why the DAS should be considered to be simple digital equipment.

BTP 7-19 identifies the Staff Requirements Memorandum (SRM) to SECY-93-087 as relevant regulatory guidance for addressing the regulatory requirements addressed by BTP 7-19. The SRM to SECY-93-087 approved the staff position in SECY-93-087 with minor changes.

SECY-93-087 states (Enclosure 1, bottom of page 56), "The staff has concluded that analyses that demonstrate adequate rather than equivalent, defense against the postulated common-mode failures would be allowed in the diversity assessment required of the applicant. ... The staff will not require only analog equipment and will consider allowing simple digital equipment."

AREVA has stated that the DAS will be used to address CCF. (Section 3.2.1.1: "The PS is the primary means of initiating RT [Reactor Trip]. Assuming a postulated CCF renders the PS inoperable ... If a RT is required to be automatically initiated, it is performed by the DAS, a subsystem of the PAS [Primary Actuation System].")

AREVA has not provided a description of the DAS to demonstrate why it should be considered simple digital equipment. The methodology described does not include an assessment of the simplicity of the DAS. (See also related RAI No. 13)

RAI 5. Please describe how the proposed design features or assessment methodology addresses sensor independence between the echelons of defense.

BTP 7-19 identifies NUREG/CR-6303 as relevant regulatory guidance, and acceptance criteria, for addressing the regulatory requirements addressed by BTP 7-19. NUREG/CR-6303, Section 2.2 states, "All four echelons depend upon sensors to determine when to perform their functions, and a serious safety concern is to ensure that no more than one echelon is disabled by a common sensor failure or its direct consequences." (See also quotation from NUREG-0493 in RAI No. 8)

Section 3.2.1.4: "The PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS [Safety Actuation System] software." This implies that the same sensors are used by both safety and non-safety systems (See also Figure 3-5).

AREVA has proposed to define different echelons of defense than those defined in NUREG/CR-6303. In addition, the analysis methodology proposed does not seem to address sensor independence (See also quotations from Section 2 and 2.5 in RAI No. 3 above). Therefore, the D3 TR does not appear to address the concern of sensor independence.

Note: NUREG-0800, Chapter 7, Section 7.5, "Information Systems Important to Safety," contains guidance for meeting regulatory requirements. The acceptance criteria contained in Section 7.5 include Regulatory Guide 1.97, Revision 4, which endorses IEEE STD 497-2002. IEEE 497, Clause 6.2, "Common Cause Failure," contains additional guidance for "instrumentation using microprocessor based sensors, data acquisition, or display equipment". For example:

1) "Common cause failures for the instrumentation channels shall be addressed at the variable level."

2) "System interaction between accident monitoring microprocessor-based instrumentation systems and other systems that may be served by the data acquisition and display system shall be considered as part of the common cause failure evaluation."

RAI 6. Please describe how the proposed design features or assessment methodology addresses display independence.

BTP 7-19 states, "This BTP has the objective of confirming that vulnerabilities to common-cause failures have been addressed in accordance with the guidance of the SRM on SECY-93-087, specifically: ... Verify that the displays and manual controls for critical safety functions initiated by operator action are diverse from computer systems used in the automatic portion of the protection systems."

AREVA has proposed to define different echelons of defense than those defined in BTP 7-19. In addition, the analysis methodology proposed does not seem to address display independence (See quotations from Section 2 and 2.5 in RAI No. 3 above).

RAI 7. Please describe how the proposed design features or assessment methodology addresses IEEE STD 603-1991 manual control independence requirements.

IEEE 603, Section 6.2.1 states, "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 2.1 states, "For the initiation of critical safety functions at the system level (e.g., reactor trip, safety injection), conventional means (i.e., buttons, switches) are provided on the SICS [Safety Instrumentation and Control System]. These signals bypass the TXS computers and are hardwired directly to actuation devices (e.g., reactor trip devices or priority actuation and control (PAC) modules)."

Section 4.3.1 states, "The inventory of hardwired controls on SICS is developed using the following requirements:

- System-level manual actuation for critical safety functions, which include: reactor shutdown, core inventory control, decay heat removal, containment isolation and containment integrity.

- System level manual actuation of those safety functions that were credited for manual operator action in Step 2."

It is not clear that "the automatically initiated protective actions" of IEEE 603 are a subset of "critical safety functions" as described in the D3 TR. If these are in fact two names for the same set of controls, then why use two different names?

AREVA uses different terms than those used in IEEE 603. In addition, the analysis methodology proposed by AREVA, does not seem to address assessment of IEEE 603 manual control independence (See quotations from Section 2 and 2.5 in RAI No. 3 above).

RAI 8. Please describe how the proposed methodology addresses the assessment of the separation of protection and control systems.

One of the requirements that is addressed by BTP 7-19 is 10 CFR Part 50, Appendix A, which states, "Criterion 24--Separation of protection and control systems. ... Interconnection of the protection and control systems shall be limited so as to assure that safety is not significantly impaired."

NUREG-0493 (first complete paragraph at the top of page 4-12) documents that a plant, has in the past, been accepted to "... be control from the same measurements with which it is protected ... " based on a " ...demonstration of insignificant impairment to safety."

Section 4.3.2 states, "Safety-related plant equipment will have the capability of being controlled manually at the component level from the PICS via the PAS and PACS. This will fulfill the requirement of performing manual functions that don't require system level manual actuation."

The description of the proposed design features does not address the regulatory requirement for separation of protection and control systems. In addition, the analysis methodology does not seem to address the demonstration of insignificant impairment to safety (nor assessment of the separation of protection and control systems). (See also RAI No. 5 above.)

RAI 9. Please provide additional documentation to support the assumption that the AV42 is not susceptible to CCF.

NUREG-0800, Chapter 7, Table 7.1 identifies "SRM to SECY-93-087 II.Q" as acceptance criteria for diversity and defense-in-depth assessments.

SECY-93-087, Enclosure 1, Page 54 states, "... digital I&C systems share more data transmission functions and shares more process equipment than their analog counter parts. Redundant trains of digital I&C systems may share databases (software) and process equipment (hardware). Therefore, a hardware design error, software design error, or software programming error may result in a common-mode or common-cause failure of redundant equipment."

It is now possible to design hardware by using software design methodologies (i.e. programmed in C, C++, or VHDL). Therefore, hardware that is designed by using software methodologies could be considered susceptible to CCF. The AV42 uses a Programmable Logic Device (PLD) and therefore could be considered susceptible to common mode failures.

Section 3.1.1.2 states, "Based on the design features and testing described above the AV42 is not susceptible to a CCF." However insufficient information has been provided to allow the NRC to reach this conclusion independently. The proposed methodology does not include any validation of this assumption.

A description of the PACS has not been submitted, but it is understood that the PACS will consist primarily of AV42 modules. Note: Section 3.0 states, "... the main line of defense consists of the automatic safety functions performed by ... PACS, and therefore these are the systems of interest when considering CCFs."

RAI 10. Are all of the Engineered Safety Features (ESF) functions as described in IEEE STD 603-1991, implemented in four systems: 1) PS, 2) SAS, 3) SICS, and 4) PACS? Are there any other safety systems that implement ESF functions?

Section 3.2.1.2: "The PS is the primary means of performing ESF actuations." Does this PS function fulfill the requirements of IEEE 603 Section 6.1?

Section 3.2.1.4: "The SAS is the primary means of performing ESF control functions." Does the SAS address IEEE 603 Section 6.2.2?

Section 3.2.1.2: "... manual means of actuating an ESF system is provided on the SICS in the MCR." Does this SICS function fulfill the requirements of IEEE 603 Section 6.2.1?

RAI 11. Please provide an explanation of how the D3 TR lines of defense are comparable to those of NUREG/CR-6303, since the lines have different scopes.

The scope of the AREVA lines of defense do not seem to include the sensors, displays or controls associated with the I&C systems (See quotes from Section 2 and 2.4. in RAI No. 3). In addition, Section 3.0 states, "... the main line of defense consists of the automatic safety functions performed by the PS, SAS, and PACS, and therefore these are the systems of interest when considering CCFs." The displays and controls are in the SICS or PICS and are therefore, not in the scope to the D3 TR.

Section 2.5: "The U.S. EPR lines of defense are compared to these four echelons of defense discussed in NUREG/CR-6303 in Table 2-2."

The scope of the lines of defense in NUREG/CR-6303 are clarified by the definitions for those system in NUREG-0493 and IEEE STD 603-1991. These lines of defense explicitly include sensors, displays and controls.

NUREG-0493, Section 1.2.2.1: "The scram system consists of sensors, signal processors, logic, and actuation initiation devices necessary to affect the reactor trip or scram, including essential auxiliary systems. This echelon of defense

performs a safety function. The scram system is also known as the reactor trip system."

NUREG-0493, Section 1.2.2.2: "The ESF system consists of sensors, signal processors, logic, and actuation initiation devices necessary to affect engineered safety features (for example, auxiliary feedwater, containment isolation, emergency core cooling, emergency power), including essential auxiliary systems. This echelon of defense performs a safety function."

NUREG-0493, Section 1.2.2.3: "The control system consists of all instrumentation and control equipment not included in the scram or ESF actuation systems, including automatic and manual process controls, presentation of information to the operator (plant monitoring system), and plant computer(s) that are not part of the scram or ESF actuation systems. This echelon of defense does not perform a safety function, but is nevertheless important to the defense-in-depth principle."

IEEE 603: See Figure 1 & 3

RAI 12. Figure 2-2 does not include the PACS as part of the main line of defense. However, Section 3.0 states, "... the main line of defense consists of the automatic safety functions performed by the PS, SAS, and PACS..." Please clarify. (See also related RAI No. 15)

RAI 13. Please provide a description of why the PAS should be considered to be simple digital equipment.

BTP 7-19 identifies the SRM on SECY-93-087 as relevant regulatory guidance for addressing the regulatory requirements addressed by BTP 7-19. The SRM on SECY-93-087 approved the staff position in SECY-93-087 with minor changes.

SECY-93-087 states (Enclosure 1, bottom of page 56): "The staff has concluded that analyses that demonstrate adequate rather than equivalent, defense against the postulated common-mode failures would be allowed in the diversity assessment required of the applicant. ... The staff will not require only analog equipment and will consider allowing simple digital equipment."

AREVA has stated that the PAS will be used to address CCF. (Section 3.2.1.3: "The SAS is the primary means of performing ESF control functions. Assuming a postulated CCF renders the SAS inoperable, the PAS is available as a diverse means of executing ESF control functions." Section 3.2.1.4: "The PAS provides diverse processing of sensor information because the PAS obtains sensor information independently of the PS and SAS software.")

AREVA has not provided a description of the PAS that describes why it should be considered to be simple digital equipment. The methodology described does not include an assessment of the simplicity of the PAS. (See also related RAI No. 4)

RAI 14. Do SICS displays address the requirements of IEEE STD 603-1991, Sections 5.8.1 and 5.8.4?

Section 3.2.1.4: "... including type A, B and C post accident monitoring variables as defined in Regulatory Guide 1.97 .. The PS and SAS are the credited means of processing these variables, and the SICS is the credited means for display."

RAI 15. Please list all safety systems that will be analyzed.

Section 2.4 states: "In general, the lines of defense apply to the architecture level 1 automation systems." However, Section 4.1 states, "An analysis of the safety I&C systems will be performed to determine their susceptibility to a CCF." Therefore, without an explicit list of the system that will be analyzed in Section 4.1, it is not clear if the PACS and SICS will be included in the D3 analysis. (See also related RAI No. 12)

RAI 16. How will the analysis methodology described in the D3 TR differ from the methodology in NUREG/CR-6303.

Section 4.1: "This analysis addresses Point 1 of NUREG-0800, BTP 7-19, and will be performed using NUREG/CR-6303 as a model." How is "using NUREG/CR-6303 as a model" different from following the methodology described in NUREG/CR-6303?

RAI 17. Please describe why a postulated failure of the TXS platform is more conservative than outputs assumed to fail in a manner that is credible but that produces the most detrimental consequences?

NUREG/CR-6303, Section 3.5, "Guideline 5 - Method of Evaluation" states, "Block output signals must be assumed to fail in a manner that is credible but that produces the most detrimental consequences when analyses in accordance with Guideline 9."

Section 4.1: "The following assumptions are to be used when performing this analysis: ... A CCF of the TXS platform is postulated (conservative assumption). This postulated CCF is such that the TXS based I&C systems do not perform their functions when required."