ArevaEPRDCPEm Resource

From:	WELLS Russell D (AREVA NP INC) [Russell.Wells@areva.com]
Sent:	Tuesday, March 31, 2009 2:33 PM
To:	Getachew Tesfaye
Cc:	Pederson Ronda M (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)
Subject:	Response to U.S. EPR Design Certification Application RAI No. 75, FSAR Ch 7, Supplement 3
Attachments:	RAI 75 Supplement 3 Response US EPR DC.pdf

Getachew,

AREVA NP Inc. provided responses to 12 of the 31 questions of RAI No. 75 on November 3, 2008 . AREVA NP submitted Response to RAI No. 75, Supplement 1 on January 14, 2009 to address 5 of the remaining 19 questions. AREVA NP submitted Response to RAI No. 75, Supplement 2 on February 4, 2009 to address 1 of the remaining 14 questions. The attached file, “RAI 75 Supplement 3 Response US EPR DC.pdf” provides technically correct and complete responses to 7 of the remaining 13 questions, as committed.

The following table indicates the respective pages in the response document, “RAI 75 Supplement 3 Response US EPR DC.pdf,” that contain AREVA NP’s response to the subject questions.

Question #	Start Page	End Page
RAI 75 — 07.02-11	2	2
RAI 75 — 07.02-17	3	4
RAI 75 — 07.02-18	5	6
RAI 75 — 07.02-20	7	7
RAI 75 — 07.02-27	8	8
RAI 75 — 07.08-5	9	10
RAI 75 — 07.08-6	11	12

Based upon feedback from the NRC staff, AREVA NP is modifying the I&C architecture. Therefore, AREVA NP is unable to provide technically correct and complete responses to the questions that were scheduled to be completed by March 31, 2009. The revised schedule for technically correct and complete responses to the remaining 6 questions is provided below:

Question #	Response Date
RAI 75 — 07.02-7	June 12, 2009
RAI 75 — 07.02-10	June 12, 2009
RAI 75 — 07.02-15	June 12, 2009
RAI 75 — 07.02-21	June 12, 2009
RAI 75 — 07.02-22	June 12, 2009
RAI 75 — 07.08-4	June 12, 2009

Sincerely,

(Russ Wells on behalf of)
Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
New Plants Deployment

AREVA NP, Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Wednesday, February 04, 2009 2:42 PM
To: Getachew Tesfaye
Cc: BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC); PANNELL George L (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 75, Supplement 2

Getachew,

AREVA NP Inc. (AREVA NP) provided responses to 12 of the 31 questions of RAI No. 75 on November 3, 2008. AREVA NP submitted Response to RAI No. 75, Supplement 1 on January 14, 2009 to address 5 of the remaining 19 questions. The attached file, “RAI 75 Supplement 2 Response US EPR DC.pdf” provides technically correct and complete responses to 1 of the remaining 14 questions, as committed.

The following table indicates the respective page in the response document, ““RAI 75 Supplement 2 Response US EPR DC.pdf,” that contains AREVA NP’s response to the subject question.

Question #	Start Page	End Page
RAI 75 — 07.02-25	2	2

The schedule for technically correct and complete responses to the remaining 13 questions is unchanged and provided below:

Question #	Response Date
RAI 75 — 07.02-7	March 31, 2009
RAI 75 — 07.02-10	March 31, 2009
RAI 75 — 07.02-11	March 31, 2009
RAI 75 — 07.02-15	March 31, 2009
RAI 75 — 07.02-17	March 31, 2009
RAI 75 — 07.02-18	March 31, 2009
RAI 75 — 07.02-20	March 31, 2009
RAI 75 — 07.02-21	March 31, 2009
RAI 75 — 07.02-22	March 31, 2009
RAI 75 — 07.02-27	March 31, 2009
RAI 75 — 07.08-4	March 31, 2009
RAI 75 — 07.02-5	March 31, 2009
RAI 75 — 07.02-6	March 31, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935

Phone: 434-832-3694
Cell: 434-841-8788

From: Pederson Ronda M (AREVA NP INC)
Sent: Wednesday, January 14, 2009 2:09 PM
To: 'Getachew Tesfaye'
Cc: PANNELL George L (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 75, Supplement 1

Getachew,

AREVA NP Inc. provided responses to 12 of the 31 questions of RAI No. 75 on November 3, 2008. The attached file, "RAI 75 Supplement 1 Response USEPRDC.pdf," provides technically correct and complete responses to 5 of the remaining 19 questions, as committed.

The following table indicates the respective page(s) in the response document, "RAI 75 Supplement 1 Response USEPRDC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 75 — 07.02-1	2	5
RAI 75 — 07.02-2	6	6
RAI 75 — 07.02-4	7	7
RAI 75 — 07.02-16	8	8
RAI 75 — 07.02-26	9	9

The schedule for technically correct and complete responses to the remaining 14 questions is unchanged and provided below:

Question #	Response Date
RAI 75 — 07.02-7	March 31, 2009
RAI 75 — 07.02-10	March 31, 2009
RAI 75 — 07.02-11	March 31, 2009
RAI 75 — 07.02-15	March 31, 2009
RAI 75 — 07.02-17	March 31, 2009
RAI 75 — 07.02-18	March 31, 2009
RAI 75 — 07.02-20	March 31, 2009
RAI 75 — 07.02-21	March 31, 2009
RAI 75 — 07.02-22	March 31, 2009
RAI 75 — 07.02-25	March 31, 2009
RAI 75 — 07.02-27	March 31, 2009
RAI 75 — 07.08-4	March 31, 2009
RAI 75 — 07.02-5	March 31, 2009
RAI 75 — 07.02-6	March 31, 2009

Sincerely,

Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
AREVA NP Inc.

An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: WELLS Russell D (AREVA NP INC)
Sent: Monday, November 03, 2008 8:15 PM
To: 'Getachew Tesfaye'
Cc: 'John Rycyna'; Pederson Ronda M (AREVA NP INC); BENNETT Kathy A (OFR) (AREVA NP INC); DELANO Karen V (AREVA NP INC)
Subject: Response to U.S. EPR Design Certification Application RAI No. 75, FSAR Ch 7

Getachew,

Attached please find AREVA NP Inc.'s response to the subject request for additional information (RAI). The attached file, "RAI 75 Response US EPR DC.pdf" provides technically correct and complete responses to 12 of the 31 questions.

Appended to this file are affected pages of the U.S. EPR Final Safety Analysis Report in redline-strikeout format which support the response to RAI 75 Questions 07.02-23, 07.02-24, and 07.02-28.

The following table indicates the respective pages in the response document, "RAI 75 Response US EPR DC.pdf," that contain AREVA NP's response to the subject questions.

Question #	Start Page	End Page
RAI 75 — 07.02-1	2	2
RAI 75 — 07.02-2	3	3
RAI 75 — 07.02-3	4	4
RAI 75 — 07.02-4	5	5
RAI 75 — 07.02-5	6	7
RAI 75 — 07.02-6	8	8
RAI 75 — 07.02-7	9	9
RAI 75 — 07.02-8	10	10
RAI 75 — 07.02-9	11	11
RAI 75 — 07.02-10	12	12
RAI 75 — 07.02-11	13	13
RAI 75 — 07.02-12	14	15
RAI 75 — 07.02-13	16	16
RAI 75 — 07.02-14	17	17
RAI 75 — 07.02-15	18	18
RAI 75 — 07.02-16	19	19
RAI 75 — 07.02-17	20	20
RAI 75 — 07.02-18	21	21
RAI 75 — 07.02-19	22	22
RAI 75 — 07.02-20	23	23
RAI 75 — 07.02-21	24	24
RAI 75 — 07.02-22	25	25
RAI 75 — 07.02-23	26	26
RAI 75 — 07.02-24	27	27
RAI 75 — 07.02-25	28	28
RAI 75 — 07.02-26	29	29

RAI 75 — 07.02-27	30	30
RAI 75 — 07.02-28	31	31
RAI 75 — 07.08-4	32	32
RAI 75 — 07.02-5	33	34
RAI 75 — 07.02-6	35	35

A complete answer is not provided for 19 of the 31 questions. The schedule for a technically correct and complete response to this question is provided below.

Question #	Response Date
RAI 75 — 07.02-1	January 15, 2009
RAI 75 — 07.02-2	January 15, 2009
RAI 75 — 07.02-4	January 15, 2009
RAI 75 — 07.02-7	March 31, 2009
RAI 75 — 07.02-10	March 31, 2009
RAI 75 — 07.02-11	March 31, 2009
RAI 75 — 07.02-15	March 31, 2009
RAI 75 — 07.02-16	January 15, 2009
RAI 75 — 07.02-17	March 31, 2009
RAI 75 — 07.02-18	March 31, 2009
RAI 75 — 07.02-20	March 31, 2009
RAI 75 — 07.02-21	March 31, 2009
RAI 75 — 07.02-22	March 31, 2009
RAI 75 — 07.02-25	March 31, 2009
RAI 75 — 07.02-26	January 15, 2009
RAI 75 — 07.02-27	March 31, 2009
RAI 75 — 07.08-4	March 31, 2009
RAI 75 — 07.02-5	March 31, 2009
RAI 75 — 07.02-6	March 31, 2009

Sincerely,

(Russ Wells on behalf of)
Ronda Pederson
ronda.pederson@areva.com
Licensing Manager, U.S. EPR Design Certification
New Plants Deployment
AREVA NP, Inc.
An AREVA and Siemens company
3315 Old Forest Road
Lynchburg, VA 24506-0935
Phone: 434-832-3694
Cell: 434-841-8788

From: Getachew Tesfaye [mailto:Getachew.Tesfaye@nrc.gov]
Sent: Thursday, October 02, 2008 8:36 PM
To: ZZ-DL-A-USEPR-DL
Cc: Tung Truong; Kenneth Mott; Michael Canova; Terry Jackson; Joseph Colaccino; John Rycyna
Subject: U.S. EPR Design Certification Application RAI No. 75 (570_1131),FSAR Ch 7

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on September 9, 2008, and on October 2, 2008, you informed us that the RAI is clear and no further clarification is needed. As a result, no change is made to the draft RAI. The schedule we have established for review of your application assumes technically correct and complete responses within 30 days of receipt of

RAIs. For any RAIs that cannot be answered within 30 days, it is expected that a date for receipt of this information will be provided to the staff within the 30 day period so that the staff can assess how this information will impact the published schedule.

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

Hearing Identifier: AREVA_EPR_DC_RAIs
Email Number: 357

Mail Envelope Properties (1F1CC1BBDC66B842A46CAC03D6B1CD41014D68B2)

Subject: Response to U.S. EPR Design Certification Application RAI No. 75, FSAR Ch 7, Supplement 3
Sent Date: 3/31/2009 2:33:06 PM
Received Date: 3/31/2009 2:33:08 PM
From: WELLS Russell D (AREVA NP INC)

Created By: Russell.Wells@areva.com

Recipients:
"Pederson Ronda M (AREVA NP INC)" <Ronda.Pederson@areva.com>
Tracking Status: None
"BENNETT Kathy A (OFR) (AREVA NP INC)" <Kathy.Bennett@areva.com>
Tracking Status: None
"DELANO Karen V (AREVA NP INC)" <Karen.Delano@areva.com>
Tracking Status: None
"Getachew Tesfaye" <Getachew.Tesfaye@nrc.gov>
Tracking Status: None

Post Office: AUSLYNCMX02.adom.ad.corp

Files	**Size**	**Date & Time**
MESSAGE	10445	3/31/2009 2:33:08 PM
RAI 75 Supplement 3 Response US EPR DC.pdf		110535

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

Response to

Request for Additional Information No. 75, Supplement 3

10/2/2008

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.02 - Reactor Trip System
SRP Section: 07.08 - Diverse Instrumentation and Control Systems
Application Section: FSAR Ch 7

Question 07.02-11:

When will the Equipment Qualification Data Packages (EQDP) and Seismic Qualification Data Packages (SQDP) be available for staff to review?

FSAR 7.2.2.3.6 states that reactor trip function is implemented using the NRC approved TELEPERM XS digital platform. FSAR 7.1.2.6.15 states that safety systems shall meet the requirements of Clause 5.4 of IEEE 603-1998 and equipment used shall be qualified using appropriate method described in FSAR 3.11. FSAR 3.11.3 states that summaries and results of qualification tests for electrical equipment and components are documented in the EQDP, and summaries and results of seismic qualification tests for electrical and mechanical equipment and components in the harsh environment areas are documented in the SQDP.

Response to Question 07.02-11:

AREVA NP notes that design certification is intended to support combined construction and operating licenses for several future power plants. Accordingly, the U.S. EPR design certification application is intended to support current and future versions of the TXS platform, and it is not appropriate to submit information for design certification representing a specific and limited time in the evolution of the TXS platform.

The equipment qualification data packages and seismic qualification data packages will not be submitted as part of design certification since this material would contain information regarding a specific version of equipment. When a plant-specific version of equipment is selected, the appropriate documentation will be available for audit. ITAAC is provided in Tier 1 to commit to equipment and seismic qualification.

This approach is consistent with the NRC’s review process described in the Standard Review Plan (SRP). Specifically, SRP 7.0 states:

> “Review of DC applications should normally extend to cover detailed design. However, for digital computer-based I&C systems, it may be premature to complete final design details at the DC stage. Waiting until the COL stage to complete the final design of such systems allows the COL applicant/licensee to use the most recent technology for each plant. Therefore, the review of DC applications for digital computer-based I&C systems may be limited to (1) a detailed review at the functional block diagram level, (2) a review of the applicant/licensee’s commitment to prescribed limits, parameters procedures, and attributes for the detailed design process, and (3) ITAAC adequate to demonstrate that the as-built facility conforms to these commitments.”

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.02-17:

What are the effects of possible hardware and software failures? What design features have been incorporated to prevent or limit these effects of these failures?

Hardware failure conditions to be considered should include failures of portions of the computer itself and failures of portions of communication systems. Hard failures, transient failures, sustained failures, and partial failures should be considered. Software failure conditions to be considered should include, as appropriate, software common-cause failures, cascading failures, and undetected failures.

Clause 5.15 of IEEE 603-1991 requires that the degree of redundancy, diversity, testability, and quality provided in the safety system design is adequate to achieve functional reliability commensurate with the safety functions to be performed. For computer systems, both hardware and software reliability should be analyzed. Standard Review Plan (SRP) Appendix 7.1-D describes the staff position on software reliability determination. SRP BTP 7-14 provides guidance for software development processes that are expected to produce reliable software.

DC FSAR, Tier 2, Section 7.1.2.6.26, states that safety systems meet the reliability requirements of IEEE 603-1998 and the additional guidance of IEEE 7-4.3.2-2003 to support overall plant availability. High reliability is provided through: highly redundant architecture, reliable equipment, independent subsystems, continuous online fault detection and accommodation abilities, high quality software design process, and strong operating experience of the TXS platform. However, the DC FSAR did not address hardware and software failures and how they are addressed.

Response to Question 07.02-17:

Worst-case single, credible hardware and software failures in an instrumentation and controls (I&C) safety system will not result in the loss of the safety function. Several design features have been incorporated to prevent the loss of a safety function due to the effects of hardware and software failures. One of these features is the highly redundant architecture design. Each safety I&C system has four redundant and independent divisions so that a single software or hardware failure does not result in the loss of a safety function. A detailed discussion on how independence is established in the safety I&C systems is described in U.S. EPR FSAR Tier 2, Section 7.1.1.6.4.

Another design feature to prevent or limit the effects of hardware and software failures is the use of a high quality software development process. The software development process is in accordance with SRP BTP 7-14 to increase the reliability of the software produced and therefore reduce the probability of hardware and software failures. This software development process is discussed in U.S. EPR FSAR Tier 2, Section 7.1.1.2.2.

Thirdly, the safety I&C systems are implemented using the TELEPERM XS (TXS) digital platform. TXS is a digital I&C system based on experience gained internationally from new nuclear plant designs and retrofits from existing plants with digital I&C equipment. The maturity of the TXS platform aids in the reliability of the safety I&C systems of the U.S. EPR. Features of the TXS platform that limit the effects of failures include the continuous online self testing and diagnostics that allow early detection of hardware and software failures. The TXS platform is discussed in U.S. EPR FSAR Tier 2, Section 7.1.1.1.

Lastly, AREVA NP recognizes the concern that despite the high quality of design and the use of defensive measures to combat hardware and software system failures, it is still possible that a software failure may defeat the safety functions in redundant safety divisions through a software common cause failure. The AREVA NP solution to a software common cause failure (SWCCF) of the safety I&C system is the use of a platform diverse from TXS that can be used to automatically initiate required safety functions, or allow manual execution of required safety functions by the operator in the event that a SWCCF occurs. This diverse system is the diverse actuation system (DAS) and is described in U.S. EPR FSAR Tier 2, Section 7.1.1.4.6. The functions of the DAS are described in U.S. EPR FSAR Tier 2, Section 7.8.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.02-18:

What analyses have been performed to demonstrate that the performance requirements of the safety systems are met regarding setpoints, margins, errors, and response time? What design practices are implemented to avoid timing problems?

IEEE 603-1991, Clause 6.1, states in part that the safety system should, with precision and reliability, automatically initiate and execute protective action for the range of conditions and performance except as justified in Clause 4.5 of IEEE Std. 603-1991. The applicant/licensee's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met. The evaluation of the precision of the safety system should be addressed to the extent that setpoints, margins, errors, and response times are factored into the analysis. Standard Review Plan (SRP) and Branch Technical Position (BTP) 7-12 discuss considerations for the review of the process for establishing instrument setpoints. SRP BTP 7-21 discusses, for digital computer-based systems, that the evaluation should confirm that the functional requirements have been appropriately allocated into hardware and software requirements. The evaluation should also confirm that the system's real-time performance is deterministic and known.

FSAR 7.1.2.6.28 states that safety systems meet the requirements of Clauses 6.1 and 7.1 of IEEE 603-1998, and that PS is designed to automatically initiate reactor trip and actuate the ESF systems necessary to mitigate the effects of DBEs. However, it does not provide sufficient information to address setpoints, margins, errors, and response-time.

Response to Question 07.02-18:

AREVA NP has submitted the following topical reports to address setpoints, margins and errors:

- ANP-10275PA, “U.S. EPR Setpoint Methodology Topical Report”.
- ANP-10287P, “Incore Trip Setpoint and Transient Methodology for U.S EPR Topical Report”.

The first report provides a methodology in accordance with RG 1.105, “Instrument Setpoints for Safety Related Instrumentation.” It covers setpoints for all protective system functions except those functions involving the incore instrumentation. The second report covers setpoints associated with functions that involve the incore instrumentation.

As part of ITAAC in U.S. EPR FSAR Tier 1, Section 2.4.1, an analysis will be performed to verify the protection system setpoints are determined using the methodologies listed above. The acceptance criteria for the ITAAC is the generation of a report that concludes that the setpoints were determined using the above methodologies.

To address BTP 7-21 on real time performance, part of the response to RAI 4 of the Protection System Topical Report, ANP-10281P, provides documentation detailing the allocation of time delays and demonstrates that the protection systems real time performance is deterministic. This information is attached to the letter, Ronnie L. Gardner (AREVA NP Inc.) to Document Control Desk (NRC), “Response to a Second Request for Additional Information Regarding ANP-10281P, ‘U.S. EPR Digital Protection System Topical Report’,” NRC:07:073, December 3, 2007.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.02-20:

What are the range, accuracy, resolution, response time, and sample rate for the instruments that produce the safety system inputs?

As stated in Clause 6.4 of IEEE Std. 603-1991, to the extent feasible and practical, sense and command feature inputs shall be derived from signals that are direct measures of the desired variables as specified in the design basis. Staff guidance in the Standard Review Plant states that a safety system that requires loss of flow protection would, for example, normally derive its signal from flow sensors. A design might use an indirect parameter such as a pressure signal or pump speed. However, the applicant/licensee should verify that any indirect parameter is a valid representation of the desired direct parameter for all events. For both direct and indirect parameters, the applicant/licensee should verify that the characteristics (e.g., range, accuracy, resolution, response time, sample rate) of the instruments that produce the safety system inputs are consistent with the analysis provided in Chapter 15 of the SAR.

DC FSAR, Tier 2, Section 7.1.2.6.31, states that safety systems meet the requirements of Clause 6.4 of IEEE 603-1998, and that signals used in the sense and command features are direct measures of the desired variable in the design basis. FSAR Table 7.2-1, "Reactor Trip Variables," list variables to be monitored and ranges.

Response to Question 07.02-20:

The information requested in this question depends on the specific instrumentation procured for each power plant that references the U.S. EPR Design Certification.

The as-procured instruments are not specified to support the design certification; instead, specific instrumentation will be selected as part of the detailed design of each power plant that references the U.S. EPR design certification. As such, information such as range, accuracy, resolution, response time and sample rate of the as-procured instrumentation will be available for NRC audit when instrumentation is procured on a project-specific basis.

To support design certification, these instrumentation characteristics are accounted for in the instrument setpoint methodology (ANP-10275PA) and response times assumed in the Chapter 15 safety analyses (U.S. EPR FSAR Tier 2, Table 15.0-7).

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.02-27:

How will the self-diagnostic feature of TXS, as identified below, be verified to function as-designed?

Clause 5.10 of IEEE 603-1991 requires that the safety systems be designed to facilitate timely recognition, location, replacement, repair, and adjustment of malfunctioning equipment.

DC FSAR, Tier 2, Section 7.1.2.6.21, states that safety systems meet the requirements of Clause 5.10 of IEEE 603-1998, and that safety systems built upon the TXS platform contain self-diagnostic test features to detect both hardware and software faults and assist in diagnostic and repair activities.

Response to Question 07.02-27:

The self-diagnostic features of the TXS platform are verified to function as-designed by application independent qualification. This is described in Sections 2.1.2 and 3.2 of Siemens Topical Report EMF-2110(NP), Revision 1, “TELEPERM XS: A Digital Reactor Protection System.

During plant operation, self-diagnostic functionality is performed during time intervals when no cyclic processing of the application software is active. It consists of a sequence of pre-defined monitoring tasks. If this sequence is not completed within a pre-defined amount of time, an error is generated.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.08-5:

Explain the selection process and analysis that were used to select the functions that are automatically actuated by the Diverse Actuation System (DAS).

DC-FSAR Tier 1 Table 2.4.9-2 list functions that are automatically actuated by the DAS. However, this list is not a complete list when making a comparison to the digital protection system's (i.e., TXS, PS) automatic protection functions provided in DC-FSAR Tier 1 Table 2.4.1-3 and Table 2.4.1-4 (both sheets 1 and 2).

DC-FSAR Section 7.8.1.1.3 credits the DAS as a subsystem of the PAS that is used for execution of automatic functions to mitigate an anticipated transient without scram or software common-cause failure (CCF) of the safety I&C systems. DC-FSAR Section 7.8.2.2.7 states that the DAS is provided as a diverse backup in the event of a software CCF that disables both the reactor trip and engineered safety features actuation functions of the Protection System.

Branch Technical Position 7-19 (BTP 7-19) provides guidance for evaluation of diversity and defense-in-depth (D3) in digital computer-based instrumentation and control systems. The NRC has established a four-point position on D3. Point 3 of the four-point D3 position states:

"If a postulated common-cause failure could disable a safety function, a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same common-cause failure, ***should be required to perform either the same function as the safety system function that is vulnerable to common-cause failure or a different function that provides adequate protection.*** The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions."

BTP 7-19 further provides acceptance criteria for plant response to a single, postulated CCF to be included within the D3 assessment submitted by the applicant/licensee and states that the D3 assessment should demonstrate compliance with the four-point position by confirming that anticipated operational occurrences and design basis accidents are mitigated in the presence of common-cause failure, by, among other things, showing that:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.
2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the

vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

The NRC staff has reviewed the applicant's D3 assessment, U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report, ANP-10284, Revision 0 [Adams Accession No. ML0717601881], and could not locate an analysis such as acceptance criteria items 1 and 2 above, which would demonstrate compliance with the NRC's four-point position on diversity. The staff could not locate the documented basis within the D3 assessment or the DC-FSAR which would demonstrate compliance with Point 3 of the NRC's four-point D3 position.

Response to Question 07.08-5:

The diverse actuation system (DAS) functions identified in the U.S. EPR FSAR are supported by a qualitative analysis that was performed in accordance with step 2 of the D3 methodology defined in ANP-10284, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report". This analysis will be submitted to the NRC by the end of May, 2009.

A D3 analysis will not result in a one-to-one correspondence between protection system functions and DAS functions. The diverse means can perform a different function that provides adequate protection. Adequate protection for beyond design basis events—such as software common cause failure (CCF) of the protection system (PS) in conjunction with a design basis event—is defined by a set of acceptance criteria that are less stringent than those used in design basis event analysis. Therefore, a smaller set of diverse protective functions can provide adequate protection for these less stringent acceptance criteria.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.

Question 07.08-6:

Describe the plant response using best-estimate analysis based on the Diverse Actuation System (DAS) setpoints and explain the process for selecting the DAS setpoints.

DC-FSAR Tier 2 Section 7.8.1.1.3 states that the DAS executes the automatic reactor trip and engineered safety feature actuation and that setpoints for these functions are set so that the Protection System will actuate prior to the DAS.

Branch Technical Position 7-19 (BTP 7-19) provides acceptance criteria for plant response to a single postulated common cause failure (CCF). This analysis should be included within the Defense-in-Depth and Diversity (D3) assessment submitted by the applicant/licensee. The D3 assessment should confirm that anticipated operational occurrences and design basis accidents are mitigated in the presence of a common-cause failure, by, among other things, showing that:

1. For each anticipated operational occurrence in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding 10 percent of the 10 CFR 100 guideline value or violation of the integrity of the primary coolant pressure boundary. The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.
2. For each postulated accident in the design basis occurring in conjunction with each single postulated common-cause failure, the plant response calculated using best-estimate (realistic assumptions) analyses should not result in radiation release exceeding the 10 CFR 100 guideline values, violation of the integrity of the primary coolant pressure boundary, or violation of the integrity of the containment (i.e., exceeding coolant system or containment design limits). The applicant/licensee should (1) demonstrate that sufficient diversity exists to achieve these goals, (2) identify the vulnerabilities discovered and the corrective actions taken, or (3) identify the vulnerabilities discovered and provide a documented basis that justifies taking no action.

The NRC staff has reviewed the applicant's D3 assessment, U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report, ANP-10284, Revision 0 [Adams Accession No. ML0717601881], and the DC-FSAR and could not locate an analysis of the plant response to a postulated common cause failure such as acceptance criteria items 1 and 2 above, which would demonstrate compliance with the NRC's four-point position on diversity. Specifically, the analysis should address the DAS setpoints and how they can meet the two items above and not interfere with the operation of the Protection System.

Response to Question 07.08-6:

The evaluations and analyses described in Section 4.0 of U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report, ANP-10284, Revision 0 will provide a description of the plant response in the event of a software common cause failure of the protection system (PS). Specifically, step two will provide the qualitative evaluation of anticipated operational occurrences (AOO) and postulated accidents (PA), and step four will provide the quantitative analyses of AOOs and PAs. The results of the quantitative analysis of

AOOs and PAs will be submitted to the NRC by the end of November, 2009. The analyses will utilize either conservative or best-estimate methods and include the evaluation of trip setpoints. As stated in U.S. EPR FSAR Tier 2, Section 7.8.1.1.3, the setpoints for the DAS functions will be set so that the PS will actuate prior to the DAS.

FSAR Impact:

The U.S. EPR FSAR will not be changed as a result of this question.