## ArevaEPRDCPEm Resource

**From:** Tesfaye, Getachew
**Sent:** Tuesday, August 30, 2011 1:23 PM
**To:** 'usepr@areva.com'
**Cc:** Zhang, Deanna; Morton, Wendell; Spaulding, Deirdre; Mott, Kenneth; Truong, Tung; Zhao, Jack; Mills, Daniel; Jackson, Terry; Canova, Michael; Colaccino, Joseph; ArevaEPRDCPEm Resource
**Subject:** U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7
**Attachments:** RAI_505_ICE1_5902_5735_5869_5754_5803_5950_5744.doc

Attached please find the subject requests for additional information (RAI). A draft of the RAI was provided to you on August 12, 2011, and discussed with your staff on August 22 and 25, 2011. No change is made to the draft RAI as a result of those discussions. 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:** 3366

**Mail Envelope Properties** (0A64B42AAA8FD4418CE1EB5240A6FED1471D38F71A)

**Subject:** U.S. EPR Design Certification Application RAI No. 505 (5902,5735,5869,5754,5803,5950,5744), FSAR Ch. 7
**Sent Date:** 8/30/2011 1:23:29 PM
**Received Date:** 8/30/2011 1:23:31 PM
**From:** Tesfaye, Getachew

**Created By:** Getachew.Tesfaye@nrc.gov

**Recipients:**
"Zhang, Deanna" <Deanna.Zhang@nrc.gov>
Tracking Status: None
"Morton, Wendell" <Wendell.Morton@nrc.gov>
Tracking Status: None
"Spaulding, Deirdre" <Deirdre.Spaulding@nrc.gov>
Tracking Status: None
"Mott, Kenneth" <Kenneth.Mott@nrc.gov>
Tracking Status: None
"Truong, Tung" <Tung.Truong@nrc.gov>
Tracking Status: None
"Zhao, Jack" <Jack.Zhao@nrc.gov>
Tracking Status: None
"Mills, Daniel" <Daniel.Mills@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 | 769 | 8/30/2011 1:23:31 PM |
| RAI_505_ICE1_5902_5735_5869_5754_5803_5950_5744.doc | 137722 | |

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

Request for Additional Information No. 505 (5902,5735,5869,5754,5803,5950,5744), Revision 0

8/30/2011

U. S. EPR Standard Design Certification
AREVA NP Inc.
Docket No. 52-020
SRP Section: 07.01 - Instrumentation and Controls - Introduction
SRP Section: 07.03 - Engineered Safety Features Systems
SRP Section: 07.04 - Safe Shutdown Systems
SRP Section: 07.05 - Information Systems Important to Safety
SRP Section: 07.07 - Control Systems
SRP Section: 07.08 - Diverse Instrumentation and Control Systems
SRP Section: 07.09 - Data Communication Systems

Application Section: FSAR Chapter 7

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

07.01-33

OPEN ITEM

Provide an evaluation of the most limiting location of the undetected single failure of a self-powered neutron detector (SPND). In addition, identify any changes to the Inspections, Tests, Analyses, and Acceptance Criteria (ITAAC) and Combined License (COL) action items associated with the new setpoint method.

In Attachment 2 of the letter dated, May 24, 2011, the applicant proposed to revise the Topical Report ANP-10287P, “Incore Trip Setpoint and Transient Methodology For U.S. EPR,” Revision 0, to add the method for including the undetected SPND failure and perform necessary Chapter 15 transient analyses taking credit of this SPND-based incore low departure from nucleate boiling ration (LDNBR) and high linear power density (HLPD) trips. In these two new submittals, the staff requests the applicant to (1) include the uncertainty analysis and method taking into account the possible undetected single failure of SPND at the most limiting location; (2) provide an evaluation of the most limiting location of the undetected single failure of SPND; (3) evaluate the impact on the DNBR undershoot due to this new SPND undetected single failure; and (4) identify any changes to the ITAAC and COL action items associated with the new setpoint method.

07.01-34

OPEN ITEM

The staff requests the applicant to provide additional information on diagnostic tools and testing machines (excluding the Service Unit) utilized in the U.S. EPR. In particular, the staff requests the applicant to provide more details on the "maintenance laptop" and "test machine", as documented in Technical Report ANP-10315P, Revision 1.

Clause 5.6 of IEEE Std. 603-1991 requires, in part, that safety system design be such that credible failures in and consequential actions by other systems of the design basis,

shall not prevent the safety systems from meeting the requirements of this standard. Both the maintenance laptop and portable test machine perform functions based on information provided by the applicant in Technical Report ANP-10315P. In Technical Report ANP-10315P, the applicant provides limited information concerning the maintenance laptop. The applicant also provides limited information on the portable test machine. The staff requests the applicant provide information regarding the following clarifying questions:

a. Summarize the types of maintenance activities, equipment issues, etc., that would require a local connection to a function processor by the maintenance laptop or portable test machine.

b. Justify why there is no form of isolation (data, electrical, etc.) between the maintenance laptop and test machines when a local connection is made at the serial port of a given function processor, similar to what has been implemented with the SU.

c. Do the test machines have the same software and access controls placed on them similar to the maintenance laptop, described in Section 2.2.6.1.2 of ANP-10315?

d. Are the test machines utilized in testing that involves bi-directional communications, such as with the SU? If so, is an MSI incorporated?

e. According to Section 2.2.6.1.3 of Technical Report ANP-10315P, the maintenance laptop is prevented from being able to change the operating mode of a function processor. If the a failure of a function processor occurs, such that the processor is no longer running within the runtime environment and the maintenance laptop can only retrieve information in the diagnosis state, then how is an individual function processor returned to normal operation (cyclic processing)? According to the applicant, the SU cannot establish communications with a processor that is not running within the runtime environment.

07.01-35

OPEN ITEM

Provide failure modes and effects analysis (FMEA) and ITAAC to perform the FMEA for the Safety Automation System (SAS) to verify design commitments made in U.S. EPR FSAR, Tier 2, Section 7.1.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. As part of an alternative request, the applicant proposes to use IEEE Std. 603-1998. Clause 5.1 of IEEE Std. 603-1998 require, in part, that safety systems perform all safety functions in the presence of any single detectable failure, all failures caused by a single failure, and all failures or spurious actuations caused by a design basis event. In Tier 2, Section 7.1.2.6.12, the applicant states that an FMEA was performed for the PS and described in ANP-10309P, as a means of meeting the requirements of IEEE Std. 603-1998, Clause 5.1. An FMEA is a typical method of analysis used to demonstrate compliance with single failure criteria of IEEE Std. 603-1998, Clause 5.1. The staff review of the PS FMEA determined that the SAS functionality, as it pertains to ESF functionality, is not addressed in the analysis. The applicant did not state in Section 7.1.2.6.12 that an FMEA was performed for SAS. SAS provides safety-related functions relating to safe

shutdown support as well as providing safety-related interlocks for numerous other safety systems. The staff review of Tier 1, Section 2.4.4, determined that there was no ITAAC item verifying the performance of a SAS FMEA, similar to that of the PS ITAAC item provided in Section 2.4.1.

Due to the safety significance of SAS, the staff requests the applicant provide an FMEA, or similar single failure analysis, for SAS that demonstrates SAS failure modes have been accounted for in the U.S. EPR design. The staff also requests the applicant provide an ITAAC item verifying the performance of the SAS FMEA.

07.01-36

OPEN ITEM

Clarify the new voting scheme for Safety Automation System (SAS) voting logic and how the voting logic is modified in the presence of a single failure.

10 CFR 50.55a(h) incorporates by reference IEEE Std. 603-1991. As part of an alternative request, the applicant proposes to use IEEE Std. 603-1998. Clause 5.1 of IEEE Std. 603-1998 require, in part, that safety systems perform all safety functions in the presence of any single detectable failure, all failures caused by a single failure, and all failures or spurious actuations caused by a design basis event.

Upon receiving a start signal from the PS, SAS provides closed-loop controls for specified engineered safety features (ESF) systems to allow the plant reach and maintain safe shutdown conditions. Initially, the design of SAS incorporated a 2nd min / 2nd max selection scheme as part of its divisional logic scheme, which can be seen in U.S. EPR FSAR, Tier 2, Section 7.3, Revision 2. In response to RAI 442, Question 07.03-32, the applicant provided Interim Revision 3 mark-ups of Tier 2, Section 7.3. As shown in Tier 2, Figure 7.3-12, Interim Revision 3 mark-ups, a single sensor voting scheme has replaced the 2nd min / 2nd max function. Given this change to a more conventional voting scheme, the applicant did not provide any design information on the new voting scheme in the FSAR. The applicant also did not provide any information on how SAS voting logic is modified in the presence of a single failure, similar to information provided for the PS in Technical Report ANP-10309P. This information is critical to the staff's evaluation of SAS compliance with IEEE Std. 603-1998, Clause 5.1. The staff requests the applicant provide information in the FSAR concerning the new SAS voting scheme and to also provide information on how SAS voting logic is modified in the presence of single failures, faulty signals and messages, etc.

07.01-37

OPEN ITEM

Provide an ITAAC Item in U.S. EPR FSAR, Tier 1, Section 2.4.4, that ties together satisfactory completion of the SAS ITAAC to completion of referenced ITAAC provided by the applicant in response to RAI 78, Questions 14.03.05-3&4 (Supplement 2).

IEEE Std. 603-1998, Clause 5.2, requires, in part, that the safety system design provide features to ensure that system-level actions go to completion. 10 CFR 52.47(b)(1) requires, in part, that ITAAC are necessary and sufficient to provide reasonable assurance that if the ITAAC are performed and the acceptance criteria met, a facility that

incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. For the staff's review of compliance for SAS, the staff did not find an ITAAC item in Tier 1, Section 2.4.4, that verified SAS system design incorporates features that ensure completion of protective action. The SAS performs safety-related closed loop controls to help the plant achieve and maintain safe shutdown conditions as well as providing safety-related interlocks. In the applicant's response to RAI 78, Questions 14.03.05-3&4 (Supplement 2), the applicant states the following:

> *"Completion of protective action is verified by several ITAAC. ITAAC Item 4.2 in Section 2.4.1 verifies that an ESF actuation signal remains as long as conditions that represent the completion of the function do not exist and requires deliberate operator action to be returned to normal. ITAAC Item 4.4 in Section 2.4.5 verifies proper connections from the other I&C systems to the PACS. Various mechanical system PACS ITAAC is provided that verifies that the actuator responds to the state requested by the test signal sent to the PACS. Examples of this ITAAC can be found in Tier 1, Sections 2.2.1, 2.2.3, 2.2.4, 2.2.7, 2.6.1, 2.6.6, 2.7.1, 2.7.2, 2.7.11. All ITAAC items mentioned above provide verification that completion of protective action requirement is satisfied."*

The staff understood the applicant's rationale in this excerpt. However, the staff requests the applicant provide an ITAAC Item in Tier 1, Section 2.4.4, that ties these commitments together into the SAS ITAAC to ensure that the ITAAC for SAS will not be completed until satisfactory completion of the above-mentioned sections are satisfactory.

07.01-38

OPEN ITEM

Describe how the Safety Automation System (SAS), Safety Information and Control System (SICS), Incore Instrumentation System (IIS), Excore Instrumentation System (EIS), Boron Concentration Measurement System (BCMS), Signal Conditioning and Distribution System (SCDS), Rod Position Measurement System (RPMS) and Radiation Monitoring System (RMS) recover from a 'loss of power condition' and whether these systems have a fail-safe design incorporated.

IEEE Std. 603-1998, Clause 5.5 requires, in part, that the safety systems shall perform all design functions in the presence of conditions described in the design basis. SRP Appendix 7.1-C provides, in part, that for Clause 5.5, the safety system should fail into a predefined safe state upon a loss of power condition and actuated components should fail 'as-is'. U.S. EPR FSAR, Tier 2, Section 7.1.2.6.16, states that the PS implements a fail-safe design, for which a loss of power results in a fail as-is condition. The applicant did not address the failure behavior of SAS, SICS, IIS, EIS, BCMS, SCDS, RPMS and RMS upon a loss of power condition occurring. The staff requests the applicant provide information in the FSAR describing how a fail-safe design is incorporated into these systems and how these systems performs after a loss-of-power occurs.

07.01-39

OPEN ITEM

Discuss how the self-test features in the U.S. EPR design are fully tested and verified on a periodic basis. This RAI question is part of a series of follow-up questions to RAI 285, Question 07.03-21.

IEEE Std. 603-1998, Clause 5.7 requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Appendices 7.1-C and 7.1-D provide guidance on meeting the requirements of Clause 5.7. SRP-BTP 7-17 was also used as guidance. In its response to RAI 285, Question 07.03-21, the applicant provided Technical Report ANP-10315, which provides the overall surveillance and self-testing philosophy for the U.S. EPR design. The technical report was provided in order to provide the staff information regarding the design implementation of the self-testing features. In Section 3.6 of Technical Report ANP-10315, the applicant provided four technical points intended to address guidance provided in BTP 7-17, which states, in part, that automatic self-diagnostic features should be verified during periodic tests.

The staff's review yielded the following points:

- Overall, the four points do not appear to adequately verify the full design functionality of the self-testing features as enumerated in Section 2.2.6 of Technical Report ANP-10315.
- The applicant did not link the four points, or any other verification method, to the overall surveillance philosophy provided in Technical Report ANP-10315. Technical Report ANP-10315 provides methods for how tests such as response time tests are performed, as illustrated in Figure 2-4. The staff did not find specific information on how self-test verification would be performed as part of a surveillance test.
- If there is a failure of self-tests, whether system-wide, or isolated to an individual function processor, there is no mention of how operability is affected.

In particular, the staff's concern lies with hardware portions of the self-test features that may degrade and fail. To these points, the staff requests the applicant to provide the following:

a. Address verification of self-test features during the life of the system; particularly hardware self-test components that can degrade over time (e.g., hardware watchdog timer and other such hardware components).

b. For the method of self-test verification determined by the applicant, describe how the verification is performed during surveillance testing of all the applicable TXS safety systems.

c. How does the applicant address operability for a processor that has a failed self-test feature?

07.01-40

OPEN ITEM

Provide information on what operator actions are taken on a failure of the self-tests to perform a full system scan within one hour. Also, provide more information on the acceptability of allowing a function processor or division or TXS safety system to continue to operate normally, with a failed self-test run. This RAI question is part of a series of follow-up questions to RAI 285 Question 07.03-21.

IEEE Std. 603-1998, Clause 5.7 requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Appendices 7.1-C and 7.1-D provide guidance on meeting the requirements of Clause 5.7. SRP-BTP 7-17 was also used as guidance. In terms of a failure of the self-testing features, Section 2.2.6.1 of Technical Report ANP-10315, states that,

> "*If the continuous self-test is not complete after one hour, the runtime environment issues an error message to the SU. This error message is also transferred to the application software for inclusion in engineered alarms to the operator."*

Section 2.2.6.6 of Technical Report ANP-10315 states,

> *"The runtime environment monitors the operation of the cyclic self-test. If the cyclic self-test does not complete one self-test cycle within one hour, the runtime environment issues an error message. This does not disrupt runtime environment operation. In particular, the processing of the application software functions is not affected."*

The applicant is crediting the self-test features of the U.S. EPR design to meet the requirements of Clause 5.7. The staff did not identify why the failure of a self test did not yield a more significant operator response. As Section 2.2.6.6 is currently written, a TXS function processor, and potentially, a TXS safety system, could continue running indefinitely without any continuous self-tests being performed because no interruption of operations occurs. Failure of the continuous monitoring self-tests indicates a potentially more significant issue with the system if it was originally designed to perform the tests on a regular periodicity. The staff requests the applicant address the following concerns:

a. If a self-test failure to run fully within one hour occurs, what is the operability state of the function processor or system?

b. How long does the applicant believe the function processor or TXS system can be credited to safely run without cyclic self-testing being active?

c. What operator actions would be required if a self-testing failure is alarmed in the main control room?

07.01-41

OPEN ITEM

Define the terms such as 'halted', 'disabled' and 'out of service', when used in the U.S. EPR FSAR and associated technical reports. This RAI question is part of a series of follow-up questions to RAI 285, Question 07.03-21.

10 CFR 52.47(a)(2) requires, in part, that design description of SSCs in the application shall be sufficient to permit understanding of system designs and their relationships to safety evaluations. The staff requests the applicant clarify what it means in terms of design functionality, when the FSAR and associated technical reports use terms such as 'halted', 'out of service', 'disabled' and other such terms, when applied to components such as APUs, ALUs, CPUs, etc. In addition, outline what these terms mean for the operations of these components in the FSAR and/or Technical Reports ANP -10309 and ANP-10315.

07.01-42

OPEN ITEM

Clarify whether the SAS is now covered by the scope of ANP-10315, with the addition of the SAS technical specification. Also clarify whether surveillance testing as documented by ANP-10315 applies to all other TXS safety systems that have an associated technical specification. This RAI question is part of a series of follow-up questions to RAI 285, Question 07.03-21.

IEEE Std. 603-1998, Clause 5.7, requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Appendix 7.1-C was used as guidance in the review. In response to RAI 442, Question 07.01-30, the applicant provided Interim Revision 3 mark-ups of U.S. EPR FSAR, Tier 2, Chapter 16, Section 3.3, which incorporated a Technical Specification for SAS. As such, the staff has the following questions for the applicant that require clarification:

a. With the inclusion of a SAS Technical Specification, does the applicant intend on expanding the scope of surveillances, as stated in Section 1.2 of Technical Report ANP-10315 to include SAS?

b. Does the scope of surveillance testing, described in Technical Report ANP-10315 (excluding Section 2.2.6) apply to all other safety-related TXS systems? If not, where is this information documented?

07.01-43

OPEN ITEM

Provide a design description and ITAAC testing item in U.S. EPR FSAR, Tier 1, to address self-test functionality for the Safety Information and Control System (SICS) and clarify the classification of qualified display system (QDS).

IEEE Std. 603-1998, Clause 5.7 requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. 10 CFR 52.47(b)(1) requires, in part, that ITAAC are necessary and sufficient to provide reasonable assurance that if the ITAAC are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be

operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. SRP Section 14.3.5 provides guidance to meet the requirements of 10 CFR 52.47(b)(1).

The applicant states the following in U.S. EPR FSAR, Tier 2, Section 7.5.2.2.8:

> *"The safety-related QDS within the SICS has the capability to perform automatic self-testing to verify its ability to perform the intended functions. This self-testing feature includes, but is not limited to, the availability of components such as processors, communication and link modules, power supplies, and input/output modules. These self-testing features are included to provide a mechanism for detecting all detectable failures, which are not compromised by the additional complexity added to the system design. The self-test features of the SICS do not affect the ability of the system to perform its safety functions."*

U.S. EPR FSAR, Tier 1, Section 2.4.2, does not provide any design information for self-test features in the SICS design. ITAAC Table 2.4.2-2 does not contain an item that verifies the self-testing aspect of the SICS design. The staff requests that the applicant provide Tier 1 information regarding SICS self-test functionality as well as verification of SICS self-test functionality. In addition, the staff requests the applicant to clarify whether the QDS is still safety-related.

07.01-44

OPEN ITEM

Provide design information in the U.S. EPR FSAR concerning self-testing functionality incorporated into the Incore Instrumentation System (IIS), Excore Instrumentation System (EIS), Boron Concentration Measurement System (BCMS), Signal Conditioning and Distribution System (SCDS), Rod Position Measurement System (RPMS), Radiation Monitoring System (RMS) and Safety Information and Control System (SICS).

IEEE Std. 603-1998, Clause 5.7, requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Section 7.1-C provides guidance for meeting the requirements of Clause 5.7.

U.S. EPR FSAR, Tier 2, Section 7.1.2.6.18, states that the safety-related systems meet the requirements of IEEE Std. 603-1998, Clause 5.7. The staff does not have a clear understanding of what other safety-related systems credit self-testing features. Tier 2, Section 7.1.2.6.18, refers only to Tier 2, Sections 7.2 and 7.3, which are the reactor trip system and engineered safety features systems, respectively. These Tier 2 sections do not necessarily contain design information reflective of the other safety-related TXS I&C systems. Technical Report ANP-10315 does not provide the staff a clear understanding of other safety-related I&C systems (besides PS and SAS) that implement credited self-test features.

a. The staff requests the applicant discuss self-testing features incorporated into the above-mentioned safety systems.

b. The staff also requests the applicant clarify whether self-testing design information presented in Technical Report ANP-10315 applies to all other TXS

safety systems, and if so, to state that in the next revision of Technical Report ANP-10315.

c. Identify if any of the self-testing features will be credited for Technical Specification surveillances.

07.01-45

OPEN ITEM

Discuss self-testing features implemented in the Priority Actuator and Control System (PACS) and clarify whether design information on self-testing features described in Technical Report ANP-10315 applies to PACS. This RAI question is part of a series of follow-up questions to RAI 285 Question 07.03-21.

IEEE Std. 603-1998, Clause 5.7, requires, in part, that the capability for testing and calibration of safety system equipment shall be provided while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. SRP Appendix 7.1-C provides guidance for meeting the requirements of Clause 5.5 and 5.7.

The applicant takes credit for the TXS self-testing features to meet the requirements of Clause 5.7. This includes any self-monitoring features associated with the PACS. Technical Report ANP-10310P, Revision 1, states, in part, that the infrastructure signals of the PACS are processed by self-monitoring features on the programmable logic device (PLD). The PLD is the safety-related priority module and would fall under the same IEEE 603 requirements as the rest of the U.S. EPR design. As such, these self-monitoring features fall under the requirements of Clause 5.5 and Clause 5.7. Technical Report ANP-10315P does not address the self-monitoring features of the PACS. U.S. EPR FSAR, Tier 1, Section 2.4.5, Interim Revision 3 mark-ups, of the applicant's response to RAI 452, Question 07.03-36, does not verify PACS self-testing functionality. Information on the PACS self-monitoring is not discussed in Tier 2 information. SRP Appendix 7.1-C provides, in part, that for Clause 5.5, the safety system should fail into a predefined safe state upon a loss of power condition and actuated components should fail 'as-is'. According to Technical Report ANP-10310, infrastructure signals are used to set the output of the priority module to a predefined value. Therefore the PLD, by means of self-testing features, is responsible for this action. It would appear that the self-testing features are the mechanism that allows the PACS, and subsequently, the actuated equipment to fail into a predefined safe state and to fail as-is.

a. The staff requests the applicant describe the full set of self-test functionality implemented into the PACS.

b. The staff also requests the applicant clarify if self-testing design information presented in Technical Report ANP-10315 applies to PACS as well.

07.01-46

OPEN ITEM

Provide more design information in the US EPR FSAR concerning the Operation I&C Disable Switch.

Clause 5.1 of IEEE Std. 603-1991 requires, in part, that safety systems shall perform all safety functions required for a design basis event in the presence of any single detectable failure, all failures caused by the single failure, and all failures and spurious actions that cause or are caused by the design basis event. SRP Appendices 7.1-C and 7.1-D and SRP BTP 7-17 were used as guidance in the review. The applicant states the following in U.S. EPR FSAR, Tier 2, Section 7.1, Interim Revision 3 mark-ups:

> *"During normal operation, the* **operational I&C disable switch** *on the SICS is set so that the PAS can send commands to the PACS. In this configuration, automatic commands from the PAS override manual commands from the SICS because of the nature of the manual control logic in the PACS. If the operational I&C disable switch is set to DISABLE by the operator, the PAS input will be disabled (i.e., the input signals from the PAS to the communications module will be blocked from being sent to the priority module), providing the priority of the SICS manual commands. The operational I&C disable switch disables PAS inputs, all other PACS inputs remain operational."*

The staff requests the applicant address the following follow-up items:

a. What is the safety-qualification of the Operation I&C Disable Switch?

b. Describe how the operational I&C disable switch addresses single failures.

c. Is the Operational I&C Disable Switch necessary for performance of credited manual operator actions to mitigate the Steam Generator Tube Rupture event, as described in Chapter 15 safety analyses?

d. Is an ITAAC necessary to verify the operation and design of the operational I&C disable switch?

07.01-47

OPEN ITEM

Clarify design discrepancy in FSAR information concerning the PACS in response time testing.

Clause 6.1 of IEEE Std. 603-1991 requires that means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4.e of IEEE Std. 603-1998. The guidance of SRP Appendix 7.1-C for Clause 6.1 indicates that the applicant's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met, and that 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.

ITAAC Item 4.24 from U.S. EPR FSAR, Tier 1, Table 2.4.1-7, performs the verification of PS response times. The acceptance criteria for Item 4.24 state the following:

> *"A report exists and identifies the required response time from sensor to ALU output which supports the safety analysis response time assumptions for RT signals listed in Table 2.4.1-2 and ESF signals listed in Table 2.4.1-3."*

Table 15.0-8, "Engineered Safety Features Actuation System (ESFAS) Functions Used in the Accident Analysis", Note 4 regarding Time Delay (response times) states the following:

*"Represent the total time for completion of the function. Includes sensor delay, I&C delay (includes PS computerized portion, and PACS delays), and other delays as noted until the function is completed."*

The individual PACS modules are all downstream of the ALUs in all four PS divisions, as represented by Tier 2, Figure 7.3-1. As it is currently worded, ITAAC Item 4.24 would not adequately verify the response time requirement of the accident analyses because the test does not incorporate all timing delays if the test measurement ends at the output of the individual ALUs. The staff requests the applicant revise the acceptance criteria of ITAAC Item 4.24 to ensure it includes the PACS.

07.01-48

OPEN ITEM

Provide more design on SAS compliance with the requirements of IEEE Std. 603-1998, Clause 6.1. Also provide an ITAAC that verifies SAS control and display location in the main control room (MCR) to verify the requirements of Clause 6.2 are incorporated into the SAS design.

For Automatic Controls

Clause 6.1 of IEEE Std. 603-1991 requires that means shall be provided to automatically initiate and control all protective actions except as justified in Clause 4.e of IEEE Std. 603-1998. The guidance of SRP Appendix 7.1-C for Clause 6.1 indicates that the applicant's analysis should confirm that the safety system has been qualified to demonstrate that the performance requirements are met, and that 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.

The applicant provides the following design elements into the protection system design to meet the requirements of Clauses 6.1:

- An approved setpoint methodology for the U.S. EPR FSAR.
- Operating margins for process variables monitored for reactor trip (RT) and engineered safety features (ESF) systems presented in U.S. EPR FSAR, Tier 2, Sections 7.2 and 7.3.
- Setpoints and corresponding system response times (time delays) for each RT and ESF function documented in Tier 2, Table 15.0-7 and Table 15.0-8, respectively.
- ITAAC Item 4.1 and 4.2 from Tier 1, Table 2.4.1-7, which verifies the completion of protective action for automatic ESF actuation signals.

The SAS Tier 1 ITAAC is documented in Tier 1, Section 2.4.4. The applicant does not provide an ITAAC item that provides a direct verification of the SAS design meeting the requirements of Clauses 6.1 and 7.1. The staff is not aware of any setpoint analysis or response time requirements for SAS. Per the guidance provided in SRP Appendix 7.1-C, the staff requests the applicant to provide information such as the above four items for SAS. In particular, does SAS have any response time requirements, considering that SAS functionality in terms of ESF support, may have timing requirements for helping the plant achieve safe shutdown conditions?

For Manual Controls

Clause 6.2 of IEEE Std. 603-1991 requires, in part, that means be provided to manually initiate protective system actuation at the division level with minimal number of discrete operator manipulations. There is also no information on the SAS manual controls in Tier 1, Section 2.4.4. Tier 1, Table 2.4.4-6, does not have an ITAAC item that verifies SAS manual controls design function. There is also no ITAAC item in Table 2.4.4-6 verifying where SAS controls and displays are located and verifying if they're in the main control room (MCR), specifically on the SICS. Tier 2, Table 7.1-4, Interim Revision 3 mark-ups, states that the SICS has a hardwired connection to the SAS for manual grouped commands so this is also a potential discrepancy in the Tier 1 information. The staff requests the applicant add information to Tier 1 concerning SAS manual grouped controls. The staff also requests the applicant add ITAAC Items to Table 2.4.4-6 to verify the manual control design function, as well as display and controls location in the MCR.

07.01-49

OPEN ITEM

Provide information on how the Safety Automation System (SAS) meets the requirements of IEEE Std. 603-1998, Clauses 6.6 and 6.7.

Clause 6.6 of IEEE Std. 603-1991 requires, in part, that whenever the applicable permissive conditions are not met, a safety system shall automatically prevent the activation of an operating bypass or initiate the appropriate safety function(s). The operator may take action to prevent the unnecessary initiation of a protective action. Clause 6.7 of IEEE Std. 603-1991 requires, in part, that a safety system be able to retain the capability to accomplish its safety function while sense and command features equipment is in maintenance bypass. SRP Appendix 7.1-C provides guidance on meeting the requirements of Clause 6.6 and 6.7 of IEEE Std. 603-1991.

In response to RAI 78, RAI 78, Questions 14.03.05-3&4 (Supplement 2), operating bypass functionality for SAS is verified by ITAAC Item 4.3 in U.S. EPR FSAR, Tier 1, Table 2.4.1-7. The PS is a standby system, with limited interaction with SAS. SAS contains a significant number of continuous functions that are outside the bounds of system interaction with the PS, which would not be verified by ITAAC Item 4.3. The staff requests the applicant provide more information on how the applicant intends to verify how SAS meets the requirements of IEEE Std. 603-1998, Clause 6.6. Similarly, in the response to RAI 78, RAI 78, Questions 14.03.05-3&4 (Supplement 2), the applicant states the maintenance bypass functionality is verified by ITAAC Item 4.18 in Tier 1, Table 2.4.4-6. However, this ITAAC addresses performance of automatic functions, but does not identify maintenance bypasses. The staff requests the applicant to describe how the maintenance bypasses are addressed with SAS.

07.01-50

OPEN ITEM

Identify the approved version of Topical Report ANP-10272 in the U.S. EPR FSAR and address the application-specific action items within the report.

Clause 5.3 of IEEE Std. 603-1991 requires, in part, that safety systems shall be designed, manufactured, inspected, installed, tested, operated, and maintained in accordance with a prescribed quality assurance program. Section 4, Limitations and Conditions, of the Safety Evaluation for AREVA NP Topical ANP-10272, states, in part, that an application may reference the approved AREVA NP Topical Report ANP-10272 provided the application satisfies the listed conditions and limitations. The conditions and limitations are intended to ensure that all aspects of digital safety system are properly designed and implemented. U.S. EPR FSAR, Tier 2, Section 7.1.1.2.2 references Topical Report ANP-10272, "Software Program Manual for TELEPERM XS Safety Systems," which describes the lifecycle processes for application software development used in safety-related applications of the TXS platforms. The staff requests the applicant to address the limitations and conditions identified in Section 4 of the Safety Evaluation for Topical Report ANP-10272 and to incorporate the approved version of the report into the U.S. EPR FSAR.

07.01-51

OPEN ITEM

Address staff concerns related to use of multiple TXS processor operating states and the operability considerations, status of TXS processor outputs while in the parameterization and function test states, potential to remove priority logic from response time testing, and the basis for replacing traditional surveillance tests with self-tests features.

IEEE Std. 603-1998, Clause 5.7 requires the capability for testing and calibration of safety system equipment while retaining the capability of the safety systems to accomplish their safety functions. The capability for testing and calibration of safety system equipment shall be provided during power operation and shall duplicate, as closely as practicable, performance of the safety function. The capability should be provided to permit testing during power operation. SRP Section 7.1-C provides staff guidance for this requirement. The staff requests the applicant to address the following issues:

a. The response to RAI 485, Question 07.09-70, was not considered complete by the staff as it does not address surveillance tests that require more than one operating state to be performed. The staff understands that certain surveillance tests, such as the No-Go Actuating Device Operational Test, are required to be performed in both cyclic processing and parameterization TXS processor operating states. In RAI 485, Question 07.09-70, the staff requested the applicant to identify each surveillance test and the TXS function processor operating state for which the surveillance would be performed. Multi-state surveillance information was not included as part of the applicant's response. Therefore, the staff requests the applicant re-submit the response to address surveillance tests where there are multiple TXS function processor states utilized.

b. In RAI 485, Question 07.09.70, the staff requested clarification on how operability is addressed for TXS function processor operational states. The applicant considers a TXS function processor operable when it is in the cyclic processing state and inoperable for all other states. For those surveillance tests and maintenance activities where multiple processor operating states are used, the staff requests the applicant to clarify what is the overall operability of a TXS

function processor while the surveillance test or maintenance activity is performed.

c. The response to RAI 485, Question 07.09-70, indicates that TXS function processor outputs remain active in the parameterization operating state. For the functional test state, hardwired outputs are set to zero, but data messages are still actively transmitted and processed by receiving CPUs that are also in functional test state. For both operating states, the staff requests the applicant provide the basis on why active outputs are allowed while the device is considered inoperable. Also, for the functional test state, do receiving CPUs that are not in the functional test state, evaluate data messages from a function processor that is in the functional test state?

d. The applicant states the following in Section 2.5 of Technical Report ANP-10315 that “A COL applicant referencing the U.S. EPR standard design may propose to exclude the priority logic from periodic response time testing. This would require the applicant to submit a topical report justifying that approach.” The statement should be removed from the technical report for the following reasons. The applicant included the priority logic (PACS) timing delays into the overall response times for the safety analyses in FSAR Chapter 15, and notes this specifically in FSAR Table 15.0-8, Interim Revision 3 mark-up, as provided in response to RAI 452, Question 07.03-36. Portions of the staff's evaluation and final approval of system performance is contingent upon priority logic being included in the response time testing per the guidance in Regulatory Guide 1.118. At this time, the staff does not have a basis to approve currently, or in the future, the removal of the priority logic from response time testing.

e. Section 2.1 of Technical Report ANP-10315P, Revision 1, states that "...self-test features replace the traditional channel check and channel functional test surveillances." The applicant does not provide a basis on how the self-tests accomplish this, as this sentence is not elaborated on in the remainder of the technical report. The staff requests the applicant to discuss the types of failures found in traditional channel checks and functional tests and how the design functionality of the self-test features envelopes those traditional forms of testing. Specifically, point out what aspects of the self-test features provide justification for this statement and what failures of the safety instrumentation and control systems are not covered by the self-test features.

07.03-37

OPEN ITEM

Provide clarification on various changes made to U.S. EPR FSAR, Tier 2, Section 7.3, under the response to RAI 442, Question 07.03-32.

The applicant provided Interim Revision 3 mark-ups of Tier 2, Section 7.3, in response to RAI 442, Question 07.03-32. After a review of the changes made to Table 7.3-1, the staff has three observations:

a. The Turbine Trip Function was deleted.

b. For the CVCS isolation for anti-dilution protective function, boron temperature was removed from the list of variables monitored for this function in Interim Revision 3 mark-

ups of the U.S. EPR FSAR. Tier 2, Figure 7.3-22, that depicts this function, does not show boron temperature being deleted as a change for Interim Revision 3 mark-ups. Interim Revision 3 mark-up of Tier 2, Section 7.3.1.2.11, does not describe boron temperature as an input variable and does not show any revision concerning this deletion. Revision 2 of Tier 2, Section 7.3, shows boron temperature as an input variable on Figure 7.3-22. Table 7.3-1 also shows boron temperature as a monitored variable.

c. For MFWS isolation protective function, reactor trip (RT) breaker position was deleted. Also, steam generator (SG) isolation signal was not included. Tier 2, Figure 7.3-16, depicts the MFWS isolation function. RT initiation is shown as an input variable while SG isolation signal is not shown. Interim Revision 3 mark-up of Tier 2, Section 7.3.1.2.8, describes both the initiation of RT and SG isolation signal as initiating conditions for MFWS isolation.

The staff requests that applicant provide clarification on why these changes were made.

07.03-38

OPEN ITEM

Provide information on how SAS and other TXS safety-related I&C systems comply with the requirements of IEEE Std. 603-1998, Clause 4, as shown on U.S. EPR FSAR, Tier 2, Table 7.1-2.

Section 4 of IEEE Std. 603-1991, requires, in part, the specific basis established for the design of each safety system. The staff reviewed the FSAR to determine how the applicant addressed design basis requirements of IEEE Std. 603-1998, Clause 4, and applicable general design criteria, for SAS and other safety-related systems. The staff was unable to determine that for SAS and other safety-related I&C systems, all design basis requirements have been incorporated. For example, in Tier 2, Section 7.1.2.6.10, Interim Revision 3 mark-ups, the applicant states that the U.S. EPR design does contain equipment protective features that may prevent a piece of safety-related equipment from performing its function and that a failure of this type would be bounded by the single failure analysis. The applicant goes on to state that failure modes and effects analysis (FMEA) have been performed for the safety-related process systems to demonstrate that no single failure can prevent performance of a safety function.

The staff accepted the applicant's rationale in its evaluation of the PS for compliance with Clause 4.k. However, the staff has not received an FMEA for SAS, or the other safety-related systems in the U.S. EPR design. The applicant has bounded compliance with Clause 4.k by the single failure criterion but without similar analysis for SAS and other safety-systems available to the staff for review, the staff cannot make a reasonable assurance finding. Table 7.1-2 matches individual requirements to the various TXS I&C systems. Table 7.1-2 does not demonstrate specifically how the requirements are met for each system that is applicable to IEEE Std. 603-1998, Clause 4.

The staff requests the applicant specifically address the requirements of Clause 4 for each TXS safety-related I&C system in US EPR FSAR Tier 2, Section 7.1. If particular sub-clauses to IEEE Std. 603-1998, Clause 4 are not applicable to a TXS safety-related I&C system then the staff requests the applicant state this and provide a justification for the exclusion.

07.04-15

OPEN ITEM

Clarify the display and control capability of the safety information and control system (SICS) in the remote shutdown station (RSS) and address inspection, tests, analyses, and acceptance criteria (ITAAC) for engineered safety feature (ESF) controls, including those associated with safety automation system (SAS).

10 CFR 52.47(a)(2) requires, in part, a description of structures, systems, and components sufficient to permit understanding of the system design. U.S. EPR Design Control Document, Tier 2, Section 7.4.1.3.4, Interim Revision 3 mark-ups, Page 7.4-7, states, in part:

*"… the HMI [PICS and the SICS] workstation both in the MCR and RSS will continue to display …"*

*"… The SICS and PICS provide the displays and controls in the RSS to allow the monitoring and control and control of the following safe shutdown …"*

Tier 2, Section 7.4.1.3.4, Interim Revision 3 mark-ups, Page 7.4-9, states "An indication on the PICS and SICS shows that RSS control has been established." During the review, the staff questioned whether SICS provides displays and the necessary manual controls in the RSS. Also, the staff questioned if any SAS manual controls were needed in the RSS. The staff did not identify any ITAAC in Tier 1, Section 2.4, addressing ESF manual actuations in the RSS. The applicant is requested to confirm the scope of displays and controls for SICS in the RSS and to provide ITAAC that verify the manual controls in RSS.

07.05-10

OPEN ITEM

Provide additional information which addresses conformance to Regulatory Guide (RG) 1.97, Revision 4, and address the completeness of the post accident monitoring (PAM) variable list.

10 CFR Part 50, Appendix A, General Design Criteria 13, "Instrumentation and Controls," requires, in part, instrumentation to be provided to monitor variables and systems over their anticipated ranges for normal operation, anticipated operational occurrences, and accident conditions. U.S. EPR FSAR Section 7.5, Interim Revision 3 mark-up, identifies a list of PAM variables and states that the design conforms to RG 1.97, Revision 4. The staff requests the applicant to address the following issues with regards to the PAM variables:

a. The applicant states conformance to RG 1.97, Revision 4, but acknowledges that emergency procedure guidelines, emergency operating procedures, and abnormal operating procedures for the U.S. EPR are not developed and used in developing the PAM variable list. It appears that some alternative methods were used to develop the PAM variable list. If that is the case, the applicant should clearly state how they conform with RG 1.97, Revision 4, and where they are proposing alternative methods to RG 1.97.

b. In U.S. EPR FSAR Section 7.5, Interim Revision 3 mark-up, the applicant provides some information for how the PAM instrument list was developed, including the use of Babcock and Wilcox emergency operating procedure technical basis. However, the staff requires a more comprehensive analysis as to how the applicant arrived at the

PAM instrument list. As one example, the applicant noted differences between Babcock and Wilcox plants and the U.S. EPR, but did not specify those differences.

c. The applicant states that the PAM instrument list is a bounding list. As review guidance, the staff considers RG 1.97, Revision 3, as a bounding PAM instrument list. Provide the basis for differences between the RG 1.97, Revision 3, and the U.S. EPR PAM instrument descriptions.

d. If the U.S. EPR PAM instrument list is considered bounding, revise wording in Tier 1 and Tier 2 of the application to indicate that the list is bounding and no further verification is necessary. In addition, if the U.S. EPR PAM instrument list is bounding, ITAAC Item 2.1 of Tier 1, Table 3.7-2, is not necessary and should be removed.

07.05-11

OPEN ITEM

Is a COL Information Item necessary for verification of the PAMS instrument list, and are there any site-specific PAMS instrumentation for the U.S. EPR?

10 CFR Part 50, Appendix A, General Design Criteria 13, "Instrumentation and Controls," requires, in part, that instrumentation be provided to monitor variables and systems over their anticipated ranges for normal operation, anticipated operational occurrences, and accident conditions. During the review of the U.S. EPR design certification and the Calvert Cliffs combined license (COL) application, the staff noted that the Calvert Cliffs COL application addressed a COL information item associated with updating the PAMS instrument list. Given the existence of ITAAC in Section 3.7 of the U.S. EPR FSAR, Tier 1, to verify the PAMS instrument list following completion of the emergency procedures, is there a need for a COL information item related to verification of the PAMS instrument list? Second, the staff did not see discussion in the U.S. EPR FSAR related to any site-specific PAMS instruments. For example, meteorological instruments and instruments associated with other site-specific structures, systems, and components may be PAMS instruments. The applicant is requested to address the need for a COL information item to address site-specific PAMS instruments.

07.07-23

OPEN ITEM

Clarify the design commitment related to process information and control system (PICS) environmental qualification.

10CFR52.47(a)(2) requires that a description and analysis of the structures, systems, and components of the facility shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. In the U.S. EPR FSAR, Tier 2, Section 7.1.1.3.2, Interim Revision 3 mark-ups, the applicant states that "equipment selected for PICS will be rated (or otherwise reasonably expected) to operate under the mild environmental conditions..." The staff finds the design description to be ambiguous and can be interpreted in multiple ways. The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. The staff requests the applicant to remove the statement "(or otherwise reasonably expected)," or provide sufficient justification for the statement, in order to provide a clear design commitment.

07.08-43

OPEN ITEM

The staff requests the applicant to provide clear and unambiguous design commitment descriptions for (1) the DAS and PS credited human diversity and (2) credited SICS indications.

10 CFR 52.47(a)(2) requires that a description and analysis of the structures, systems, and components (SSCs) of the facility shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. The staff requests the applicant to clarify the following design descriptions:

a. Section 3.2.1 of Technical Report ANP-10304 provides a diversity design commitment between the PS TXS platform and the DAS platform that the design organization, management, designers, programmers, and testing engineers will be different. However, Section 4.2 of the same report states that it is likely that different design organizations will be responsible for the design of the two systems and that this will not be determined until the detailed design of these systems is in progress. These two design statements for the DAS and PS credited human diversity are conflicting. The applicant is requested to clarify the commitment for human diversity.

b. Table 2-1 of Technical Report ANP-10304 states that the SICS indicators can include programmable electronic I&C technology, which, according to Tier 2, Section 7.1, Interim Revision 3 mark-ups, can be TXS microprocessor-based. By contrast, Section 4.2 of Technical Report ANP-10304, SICS design diversity, states that the indications provided in SICS are performed by hardwired, analog components. The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. The staff request the applicant to provide clear design descriptions about the type of SICS indicators that are credited in the Technical Report ANP-10304.

07.08-44

OPEN ITEM

The staff requests the applicant to provide, in accordance with Item II.Q of SECY-93-087 and the BTP-7-19 acceptance criteria, a manual reactor coolant pump (RCP) trip.

The requirements of 10 CFR Part 50, Appendix A, GDC 13, state that appropriate controls shall be provided to maintain variables and systems that can affect the fission process, the integrity of the reactor core, the reactor coolant pressure boundary, and the containment and its associated systems, within prescribed operating ranges. The requirements of GDC 22 state 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 guidance of SRP 7.8, states that: "The adequacy of the set of manual control and display functions is reviewed to confirm it is sufficient to monitor the plant states and to actuate systems required by the control room operators to place the nuclear plant in a hot-shutdown condition and to control the following critical safety functions: reactivity control, core heat removal, *reactor coolant inventory*, containment isolation, and containment integrity." The applicant used it's small-break loss of coolant accident (SBLOCA) sensitivity studies to determine the latest RCP manual trip time utilizing D3 best-estimate analysis assumptions, including the availability of all four trains of SIS, and has found that the maximum peak cladding temperature (PCT) for SBLOCA remains well within the 10 CFR 50.46 acceptance criteria even if the RCPs are not tripped, and concluded that the sensitivity studies also demonstrates that a RCP trip during an

SBLOCA event with an software common-cause failure (SWCCF) in the PS is not needed to mitigate the event. However, the staff finds that based on the applicant's "Small Break LOCA" event analysis of Section A.3.7.3.2 contained in the Technical Report ANP-10304 plant response event descriptions, which state:

- During an SBLOCA with RCPs running, a greater amount of inventory could be lost out the break than with RCPs tripped.
- The most limiting SBLOCA is in the cold leg pipe at the discharge side of the RCPs.
- With an SWCCF in the PS, the RCPs continue operating, with the opportunity to be tripped (manually) at a later time.

Since the DAS is not credited with an automatic RCP trip function, then a diverse D3 manual RCP trip is necessary to address the listed SRP 7.8 guidance and requirements. The diverse D3 manual RCP trip should be designed according to the defense-in-depth and diversity policy listed in Item II.Q of the SRM to SECY-93-087, the guidance of SRP 7.8 and the SRP BTP 7-19 acceptance criteria. The staff could not identify a credited diverse manual RCP trip within the manual controls as listed in the Technical Report ANP-10304.

07.08-45

OPEN ITEM

The staff requests the applicant to provide clear and unambiguous design descriptions for the claimed PS subsystem diversity descriptions for all applicable design documents.

10CFR52.47(a)(2) requires that a description and analysis of the structures, systems, and components (SSCs) of the facility shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. The staff reviewed the U.S. EPR design documents for PS subsystem diversity design. Technical Report ANP-10309, Revision 3, states in Section 1.0, last paragraph, that:

> *"The PS provides signal diversity, as described in Section 10.0, "Signal Diversity." The signal diversity design rules presented in Section 10 represent elements of diversity described in NUREG/CR-6303 (Reference 3). AREVA NP* **takes credit** *[emphasis added] for the signal diversity within the PS, as described in the U.S. EPR Diversity and Defense-in-Depth Assessment Technical Report, ANP-10304."*

However, Section 10.1 of Technical Report ANP-10309 states:

> *"Signal diversity, as applied to the PS, is the use of two diverse parameters to initiate RT to mitigate the effects of the same AOO or PA. This signal diversity* **is not credited** *[emphasis added] in the diversity and defense-in-depth plant response analysis to mitigate any AOO or PA."*

Furthermore, Section 4.2.4 of Technical Report ANP-10304 states:

> *"Each PS division is divided into two independent subsystems (i.e., A and B). Subsystem A in each division is redundant to Subsystem A of other divisions; the same is true of Subsystem B. The primary purpose of this arrangement* **is to provide** *[emphasis added] signal diversity for RT functions."*

In addition, it is not always stated within the design descriptions that the credited signal diversity is only applicable for RT functions. As stated in Section 2.2 of Technical Report ANP-10304:

*"Each division of the PS contains two independent subsystems to support signal diversity."*

The information provided for the design basis items, taken alone and in combination, should have one and only one interpretation. The staff request the applicant to provide clear, consistent, and unambiguous design descriptions about the functions that PS subsystem diversity is credited for and specify when the PS subsystem design diversity is credited for all applicable design documents.

07.08-46

OPEN ITEM

The staff request the applicant to update the U.S. EPR FSAR with the ITAAC commitment provided in the response to RAI 413 (4772), Revision 1, Supplement 8, Question 07.08-42.

IEEE-603-1998, Clause 4.l, requires that the design basis shall document as a minimum any other special design basis that may be imposed on the system design (e.g., diversity, interlocks, regulatory agency criteria). 10CFR52.47(b)(1) requires that he proposed inspections, tests, analyses, and acceptance criteria that are necessary and sufficient to provide reasonable assurance that, if the inspections, tests, and analyses are performed and the acceptance criteria met, a facility that incorporates the design certification has been constructed and will be operated in conformity with the design certification, the provisions of the Act, and the Commission's rules and regulations. The staff agreed with the applicant's response to RAI 413, Questions 07.08-42, to create an ITAAC commitment to confirm that, for each AOO, a primary and secondary RT function using different sensors as input are identified and assigned to different PS sub-systems. The applicant stated in its response that these markups to U.S. EPR FSAR Tier 1, Section 2.4, will be submitted with the response to RAI 452, Question 07.03-36. However, upon staff's review of the response to RAI 452, Question 07.03-36, the staff could not identify an ITAAC commitment that would "confirm that, for each AOO, a primary and secondary RT function using different sensors as input are identified and assigned to different PS sub-systems" as stated in the response to RAI 413, Question 07.08-42 (Supplement 8). Therefore, staff requests the applicant to provide the stated ITAAC.

07.08-47

OPEN ITEM

The staff requests the applicant to provide design descriptions demonstrating the diverse actuation system's (DAS's) ability to be tested at power.

10CFR50.62(c)(1) and (c)(6) requires that ATWS equipment must be designed to perform its function in a reliable manner. The guidance of SRP 7.8 states that the ATWS mitigation system should be testable at power. The staff could not identify design descriptions that would demonstrate how the DAS ATWS design addressed the stated guidance of SRP 7.8 for at power testing, or the stated requirements of 10CFR50.62.

07.08-48

OPEN ITEM

The staff requests the applicant to provide the credited quality assurance descriptions and commitments for the non-safety related portions of the signal conditioning and distribution system (SCDS) and the safety information and control system (SICS).

10CFR50.62(c)(1) state that anticipated transients without scram (ATWS) equipment must be designed to perform its function in a reliable manner. The guidance of SRP 7.8 states that Generic Letter 85-06, “Quality Assurance Guidance for ATWS Equipment That Is Not Safety-Related,” provides acceptable guidance for the quality assurance of diverse I&C systems and components. The staff reviewed the U.S. EPR FSAR, Tier 1, Table 2.4.25-3, and determined that the SCDS safety-related outputs do not consist of diverse actuation system (DAS) output connection(s). Therefore, DAS diverse connections are provided by the non-safety related portions of the SCDS. In addition, Figure 2-1 of Technical Report ANP-10304 demonstrate that credited DAS controls and indications are implemented on the non-safety related portions of the SICS. The staff was not able to identify quality assurance design commitments regarding the non-safety related portions of SCDS and SICS that are used for DAS/ATWS design implementation and mitigation.

07.08-49

OPEN ITEM

The staff request the applicant to identify or provide design descriptions that would define what the design characteristics are of the credited DAS “software structure” and to demonstrate the diversity achieved between the TXS software attributes and the credited software attributes of the DAS "software structure."

10CFR50.62(c)(1) and (c)(6) requires that ATWS equipment must be diverse from the reactor trip system. 10CFR52.47(a)(2) requires that a description and analysis of the structures, systems, and components (SSCs) of the facility shall be sufficient to permit understanding of the system designs and their relationship to the safety evaluations. The applicant states in Section 4.2 of Technical Report ANP-10304 that if the DAS uses programmable electronic technology that it will not be microprocessor based and that the *software structure* will be *fundamentally different*. The staff reviewed the U.S. EPR DAS design descriptions in the U.S. EPR, Tier 1 and 2, FSAR, Interim Revision 3 mark-ups, and Technical Report ANP-10309, Revision 4, and could not identify design descriptions that would demonstrate the design characteristics and credited diversity attributes of the DAS possible implementation using "structured software." Therefore, the staff requests the applicant to provide this design information.

07.09-71

OPEN ITEM

Explain how invalid signals are identified by safety automation system (SAS) processors and state whether the voting logic in the SAS is modified to accommodate the identified invalid signals to meet the requirements of IEEE Std. 603-1998, Clause 5.6.1.

IEEE Std. 603-1998, Clause 5.6.1, requires redundant portions of the safety system to be independent and physically separated from each other to the degree necessary to retain the capability to accomplish the safety function. The staff issued Digital Instrumentation and

Controls Interim Staff Guidance 4 (D I&C ISG-04) to provide criteria for implementing interdivisional data communications. Criterion 2 in Section 1 of D I&C ISG-04 states that "The safety channel should be protected from adverse influence from outside the division of which that channel is a member…" In addition, Criterion 12 in Section 1 of D I&C ISG-04 states that, "Communication faults should not adversely affect the performance of required functions in any way…" The staff evaluated the SAS interdivisional communication functions and determined that the SAS has not adequately addressed Criteria 2 and 12. Specifically, the staff finds that the applicant has not provided sufficient detail regarding provisions in the design that prevents SAS divisions from being adversely impacted by information originating from outside the division. As such, the staff requests the applicant explain how invalid signals are identified by SAS processors and state whether the voting logic in the SAS is modified to accommodate the identified invalid signals. Incorporate this description into the U.S. EPR FSAR, Tier 2, or in documents incorporated by reference.

07.09-72

OPEN ITEM

Clarify how the principle of key retention extends to the isolation switch that connects the dedicated Service Unit (SU) to the Rod Position Measurement System (RPMS), described in Section 7.1.1.6.4 and 7.1.1.5.14 of the U.S. EPR FSAR, Tier 2, Interim Revision 3, addresses Criterion 10 in Section 1 of Digital Instrumentation and Controls Interim Staff Guidance 4 (D I&C ISG-04) to meet the requirements of IEEE Std. 603-1998, Clause 5.6.3.

IEEE Std. 603-1998, Clause 5.6.3, requires safety system design to be such that credible failures in, and consequential actions by other systems, do not prevent the safety systems from meeting the requirements of this standard. The staff issued D I&C ISG-04 to provide criteria for implementing data communication between safety and non-safety systems. Criterion 10 of Section 1 to D I&C ISG-04 states that "On-line changes to safety system software should be prevented by hardwired interlocks or by physical disconnection of maintenance and monitoring equipment. A workstation (e.g. engineer or programmer station) may alter addressable constants setpoints, parameters, and other setting associated with a safety function only by way of the dual-processor/shared-memory scheme described in this guidance, or when the associated channel is inoperable. Such a workstation should be physically restricted from making changes in more than one division at a time…"

In the response to RAI 442, Question 7.1-26, the applicant provided FSAR markups to reflect changes in the U.S. EPR I&C systems design. Section 7.1.1.6.4 of the FSAR markups provided a description of an additional hardwired disconnect between the SU and the divisional MSIs for the Protection System (PS) and Safety Automation System (SAS). The hardwired disconnect isolates the PS and SAS from the SU until a temporary connection is established between the SU and the divisional Monitoring and Service Interface (MSI) of the PS or SAS. This is achieved with a key-operated isolation switch located in the Main Control Room (MCR). The isolation switches are keyed so that a single key operates the eight switches (four MCR and four local), and they are physically retained in the switch when positioned to allow the SU connection to the system to prevent connection of a SU to more than a single division. This switch is hardwired and physically prevents the connection of a SU to more than a single division of the PS or SAS at a time. Section 7.1.1.5.14 of the U.S. EPR FSAR, Tier 2, Interim Revision 3, states that a dedicated SU is also provided for testing and maintenance of the RPMS. This section states that each division of the RPMS has a MSI for testing and maintenance of the RPMS. Each MSI

connects to a dedicated SU for the RPMS, which resides in the I&C service center. The RPMS MSI does not have any other connections than to its dedicated SU. The SU connections to the MSI are implemented in the same manner as the PS and SAS. Clarify how the principle of key retention extends to the isolation switch that connects the dedicated SU to the RPMS, described in Section 7.1.1.6.4 and 7.1.1.5.14 of the U.S. EPR FSAR, Tier 2, Interim Revision 3, addresses Criterion 10 in Section 1 of D I&C ISG-04 to meet the requirements of IEEE Std. 603-1998, Clause 5.6.3. Specifically, if one division of the SAS/PS is connected to its SU, describe what method is employed to prevent the dedicated SU for the RPMS from being connected to a separate division of the RPMS. The staff requests the applicant to include this clarification in U.S. EPR FSAR, Tier 2.