April 06, 2011

Ms. Sandra Sloan
AREVA NP Inc.
3315 Old Forest Road
P.O. Box 10935
Lynchburg, VA 24506-0935

SUBJECT: AUDIT REPORT FOR DECEMBER 8-10, 14 AND 20, 2010: AN AUDIT TO REVIEW THE U.S. EPR FINAL SAFETY ANALYSIS REPORT CHAPTER 7 DESIGN CHANGE DEVELOPMENT

Dear Ms. Sloan:

On May 13, 2010, the staff communicated to AREVA NP (AREVA) that it had completed its review of digital instrumentation and control design with respect to communication independence and diversity and defense in depth. On June 25, 2010, the staff met with AREVA for further discussion of these matters. AREVA presented a mix of proposed design changes intended to reduce design complexity and amplified its bases in other areas of concern for Nuclear Regulatory Commission (NRC) consideration. These concerns are delineated in the June 25, 2010, Meeting Summary Enclosure Agencywide Documents Access and Management System (ADAMS) Accession No. ML102300568. On November 23, 2010, AREVA issued Revision 4 of its integrated closure plan to address the independence issues ADAMS Accession No. ML103280047.

This audit was performed to examine and evaluate non-docketed technical and in-process documents related to AREVA's proposed changes in order to gain common understanding that would support the staff technical decisions regarding the Instrumentation and Controls (Chapter 7) of the AREVA design certification application, for the U.S. EPR under Part 52 of Title 10 of the *Code of Federal Regulations* (10 CFR) Part 52.

The audit report is contained in the enclosure to this letter. AREVA's Closure Plan requested this preliminary audit to support the subsequent development of the associated licensing documentation.

Pursuant to 10 CFR Section 2.390, we have determined that the enclosed audit report does not contain proprietary information. However, we will delay placing the audit report in the public document room for a period of ten working days from the date of this letter to provide you with the opportunity to comment on the proprietary aspects. If you believe that any information in the attachments are proprietary, please identify such information line-by-line and define the basis pursuant to the criteria of 10 CFR 2.390. If no proprietary issues are identified, after ten working days, the audit report will be made publicly available. If proprietary issues are identified, the final audit report will be made publicly available after the staff makes the necessary changes to the document.

If you have any questions regarding this matter, I may be reached at 301-415-3361or at Getachew.Tesfaye@nrc.gov.

Sincerely,

/RA/

Getachew Tesfaye, Senior Project Manager
EPR Projects Branch
Division of New Reactor Licensing
Office of New Reactors

Docket No. 52-020

Attachments: 1) Audit Report, 2) Audit Plan
cc: DC AREVA – EPR Mailing List

If you have any questions regarding this matter, I may be reached at 301-415-3361or at Getachew.Tesfaye@nrc.gov.

Sincerely,

/RA/

Getachew Tesfaye, Senior Project Manager
EPR Projects Branch
Division of New Reactor Licensing
Office of New Reactors

Docket No. 52-020

Attachments: 1) Audit Report, 2) Audit Plan

cc: DC AREVA – EPR Mailing List

DISTRIBUTION:
PUBLIC
NARP R/F
TJackson, NRO
JColaccino, NRO
GTesfaye, NRO
MCanova, NRO
DSpauling-Yeoman, NRO
JZhao, NRO
RidsNroDnrlNarpResource

ADAMS Accession Number: ML110900368 **NRO-002**

OFFICE	DNRL/NARP: PM	DNRL/NARP: LA	DE/ICE1: BC	DNRL/NARP: PM
NAME	MCanova	JMcLellan	TJackson	GTesfaye
DATE	03/31/2011	04/05/2011	04/05/2011	04/06/2011

OFFICIAL RECORD COPY

Audit Report

For

U.S. EPR Design Certification Final Safety Analysis Report Chapter 7

Instrumentation and Controls

Date and Location:	12/8-10/2010	AREVA NP, 7207 IBM Drive, Charlotte, NC 28262
	12/14/2010	AREVA NP Satellite Location: 1700 Rockville Pike, Suite 400, Rockville, MD 20852
	12/20/2010	Exit via Telephone Conference

I. Purpose

The purpose of the regulatory audit (see Attachment 2 for the Audit Plan) by the U.S. Nuclear Regulatory Commission (NRC) was to examine and evaluate non-docketed technical and in-process document development, with respect to the subjects discussed below in Section II, "Regulatory Audit Scope," and to discuss the materials with AREVA NP subject matter experts. The intent is to gain understanding to support the basis for licensing and regulatory decisions regarding the U.S. Evolutionary Power Reactor (U.S. EPR).

II. Regulatory Audit Scope

1. December 8-10, 2010: The NRC reviewed the in-process and lower tier documentation in support of changes developed for the safety automation system (SAS) as described by AREVA NP in its presentation on June 25, 2010. These changes were proposed to address the staff's concerns regarding interdivisional communications.

   AREVA NP systems design personnel were present to aid in identifying materials and information intended to address the following audit topics.

   a. The NRC requested that information pertaining to the following issues be available for this audit:

      i. Information to support the specific reliability and safety enhancement provided by interdivisional communication of process variables using the 2nd Min/2nd Max function.

      ii. Design documentation related to the SAS human system interface (HSI) functions, and how interdivisional communication is necessary for an adequate HSI design.

      iii. Reduction in SAS complexity as described by AREVA NP in its presentation on June 25, 2010.

ATTACHMENT 1

iv. Revised design documentation related to the changes to the safety information and control system (SICS) interface with the safety divisions.

v. Revised design documentation related to the changes to communications between the plant information and control system (PICS) and the safety divisions.

vi. Revised design documentation related to data communication between protection system (PS) divisions.

2. December 14, 2010: The NRC reviewed the in-process and lower tier documentation in support of AREVA NP's proposed changes developed to address:

   a. Conceptual design information related to service unit (SU) interface hardware and administrative control protocols proposed to address bidirectional communications issues.

III. Summary of Observations

1. The audit team reviewed AREVA NP Document Number 80-7009322-000, "Design Review Board Minutes and Action Items – I&C Architecture Changes," issued on November 19, 2010, and AREVA NP Document Number 113-7007471-000, "DCS Architecture Changes – Design Certification," issued on November 15, 2010, which were provided to the audit team by AREVA NP. AREVA NP Document Number 113-7007471-000 states that all the changes are results of NRC concerns with the current design. The concerns mentioned in Document Number 113-7007471-000 refer to regulatory concerns that were previously raised by the NRC staff at a public meeting that was held on June 25, 2010. However, in the audit team's review of the AREVA NP documents, the audit team did not find sufficient technical bases describing how the changes met regulatory requirements. In AREVA NP Document Number 113-7007471-000, many of the evaluations mentioned that they needed to be completed in order to address the proposed changes. However, AREVA NP had not started to update the design documents to include these evaluations. AREVA NP explained that they had not started the updates because the internal review (which is also referred to as "Part B") of the design change request (DCR) had not been completed. AREVA NP Document Number 80-7009322-000 also includes action and observation items from their design review board (DRB), of which several were not completed. For the diverse actuation system (DAS), the audit team also found some differences between the design changes included in the above two documents and those presented to the NRC on June 25, 2010. In summary, the audit team was not provided in-process or completed licensing or design documents covering Items iii-vi in the audit plan. Since no in-process or completed design documents were available, Items iii-vi should be audited at a later date.

2. AREVA NP identified several hundred cases of interdivisional communications involving automatic control, manual control, and indications for the SAS system (excluding 2-out-of-4 voting logic among divisions, which are allowable per NRC Digital Instrumentation and Control (DI&C) Interim Staff Guidance 4 (ISG-04)). AREVA NP provided the audit team a report, AREVA NP Document Number 51-7009531-000, "Comparison of EFW

Level Control Reliability with Four Divisions of Sensor Input vs. Single Sensor Input," issued on October 18, 2010, to address the issue of 2nd Min/2nd Max and its impact on safety control system reliability and failure probability. This report compared the emergency feedwater (EFW) level control reliability with each division having four redundant sensor inputs versus each division having only one sensor input. Although this report shows that the EFW system reliability improves with the current design, the audit team found that the plant core damage frequency (CDF) did not have any appreciable improvement. The audit team evaluated AREVA NP Document Number 51-7009525-000, "Human Factors – U.S. EPR Display Methodology Study Report," issued on October 18, 2010, to address the issue of train video display units (VDUs) versus multidivisional/train VDUs. The audit team did not find sufficient safety justification and technical basis for SAS interdivisional communications. Except for the two reports noted above, AREVA NP did not provide justification for other interdivisional communications cases. The audit team recommends that the NRC staff assess the safety justifications for those interdivisional communication cases in a future audit.

3. AREVA NP presented the audit team with several system design documents in draft form (such as piping and instrumentation diagrams (PI&D), system design requirements, typical logic diagrams, and functional diagrams) for the component cooling water system (CCWS) to address the DI&C system interdivisional communications related to the CCWS system. The current design of the CCWS is a four-train system that functions to cool and transfer heat load from safety users to the heat sink. The common loads cooled by the CCWS consist of two separate sets, referred to as Common-1 and Common-2. The Common-1 header is supplied by either CCWS Train One or Train Two while the Common-3 header is supplied by either CCWS Train Three or Train Four. Each CCWS train is provided with four switchover valves to perform the required train separation. The audit team found that interlock functions were needed to prevent two redundant CCWS trains from connecting to the same common header at the same time. The interlock functions maintaining separation between redundant CCWS trains are performed by the SAS. Each switchover valve is assigned to a SAS division based on the CCWS train which it belongs to. In any SAS division, information about the position of valves in other trains is needed to control a switchover valve and is provided via data network connection by the SAS division which acquires the information. The audit team also found that similar interlock functions needed as well for controlling the containment isolation valves on the reactor coolant pump (RCP) thermal barriers cooling paths. The audit team found that it is the interlock functions for the switchover valves that require interdivisional communications for the CCWS. The audit team found that AREVA NP provided the plant system reasons for using the interlock function and its associated interdivisional communications. However, the audit team found that AREVA NP did not provide a sufficient safety justification to support the interdivisional communications for the CCWS.

4. In AREVA NP Document Number 113-7007471-000, "DCS Architecture Changes – Design Certification", issued on November 15, 2010, the audit team found that AREVA NP completed Part A of the review process and the DRB, but had not completed Part B of the review process. According to AREVA NP Document Number EPR-EN-PR-1003, "Design Change Control Process", Part A and Part B should be completed before the DRB is finished. To justify its review process, AREVA NP provided AREVA NP Document Number 0405-22, "Design Review Boards," issued on October 27, 2010. However, the audit team found that the criteria in Document 0405-22 were specifically applicable to the DRB process and not the design change control process. Hence, the

audit team still considers that AREVA NP did not follow the design change control process, for all changes contained in AREVA NP Document Number 80-7009322-000, “Design Review Board Minutes and Action Items – I&C Architecture Changes,” issued on November 19, 2010. To track this deviation (that the Part B assessments of the I&C architecture DCR were not completed before going to the DRB), AREVA NP entered WebCAP Number 2010-9122 on December 14, 2010, and will update the staff on its disposition.

5. The audit team found that AREVA NP did not provide sufficient in-process or completed licensing or design documents for auditing the conceptual design related to the SU changes. Therefore, the audit of conceptual design information related to the SU interface hardware and administrative controls to address bidirectional communication issues should be part of a future audit.

The audit team also made the specific observations discussed below on topics contained in Section II of this audit report.

IV. Discussion

Safety Automation System

In a presentation, AREVA NP discussed the following:

1. AREVA NP has an informal list of the mechanical systems that uses interdivisional communications in the SAS.

2. The mechanical systems design and their associated instruments require power from different electrical power supply divisions and therefore it is necessary for instrumentation and control systems to exchange information among divisions for functions such as interlocks.

3. The designer has only one set of typical logic diagrams to choose from. AREVA NP indicated that this is a bounding list in the SPACE design.

4. AREVA NP is only considering the safety-related portions of HSI. AREVA NP stated that, if it determined that a function provided no benefit, it would remove it and retain only those functions that provide safety enhancement. These analyses will discuss why a decision was made to share information.

AREVA NP intends to develop a bounding list of typical functional diagrams. To clarify the design of the SAS and justify the SAS design’s safety case, AREVA NP prepared the four-tier proposal given below containing a list of significant design aspects of SAS. It is intended to provide the staff with the information it needs to fully evaluate the SAS design against available guidance and regulations. This is a working list which is subject to change:

1. SAS systems with interdivisional communications requirements

    a. AREVA NP plans to provide mechanical reasons for interdivisional communications.

    i. AREVA NP plans to demonstrate the plant system reasons to perform or support a safety function (three to four sentences explaining a generic safety reason).

    ii. AREVA NP plans to demonstrate the reliability, probabilistic risk assessment (PRA), and importance to safety for each function to ensure that the level of detail is appropriate.

    iii. AREAV NP plans to demonstrate a reduction in the probability of unsafe conditions.

  b. Regarding HSI (one reason is for indication and the other reason is for control). AREVA NP plans to demonstrate:

    i. Operator workload (reduce it or keep it lower), and

    ii. Situational awareness (integrated displays, which are a potential issue, since they would require some form of interdivisional communication from the SAS).

  c. Regarding voting logic for engineered safety features (ESF) actions, the SAS has some safety-related controls for certain ESF actuations.

2. SAS allocation

  a. AREVA NP plans to update the FSAR with specific details on SAS closed-loop control, and will provide its other safety/non-safety auxiliary control functions.

  b. AREAV NP plans to clarify the relationship among the SAS, PS, and SICS.

  c. AREVA NP plans to provide closed-loop control (PS to SAS) information, such as the type of communication connection and whether it is hard wired.

3. SAS implementation

  a. AREVA NP plans to provide bounding logic diagram configurations (the various types of interdivisional communications will be categorized as standard types of logics that the staff can review).

    i. AREVA NP will use inspections, tests, analysis, and acceptance criteria (ITAAC) to reconcile any deviation from bounding logic diagram configurations.

4. SAS data communication

  a. AREVA NP plans to describe the various methods of SAS communication.

  b. AREVA NP plans to demonstrate that the SAS will only pass the exact or limiting information necessary to perform the safety function.

c. AREVA NP plans to demonstrate how it treats failures (e.g., in data communications, and signal conditioning details).

AREVA NP identified three plant system examples that use SAS interdivisional communications. AREVA NP also provided a working list of all systems that would utilize SAS interdivisional communication. However, AREVA NP did not provide a safety case for the SAS interdivisional communication examples. According to AREVA NP, the design of SAS is incomplete and the full range of instances of SAS interdivisional communications is not fully known.

SAS Failure Analysis

Currently, AREVA NP does not have an SAS FMEA in the way that it has for the PS overall FMEA. AREVA NP states that SAS failure analysis would be performed under the ITAAC. From what the staff observed during the audit, the SAS, which is as complex as the PS with a far greater amount of interdivisional communications, interacts not only with the PS, but many mechanical systems as well. The staff requested a stand-alone failure analysis of the SAS comparable to the PS failure analysis in U.S. EPR Tier 2, FSAR Section 7.3. The audit team did not consider the SAS ITAAC as an appropriate way to determine failure analysis in this regard. AREVA NP plans to create an SAS FMEA.

AREVA NP indicated that the SAS is always active and that AREVA NP will provide a clarification in U.S. EPR Tier 2, FSAR Section 7.1. AREVA NP plans to include more details in the U.S. EPR FSAR regarding how the SAS would detect a failure such as a valve misposition, and alarm the operator. It would also state how the SAS reacts if it detected the failure of a control valve to move to the right position - not just a failure of full open or full close, but an intermediate failure. AREVA NP also intends to include this information in the SAS FMEA. The staff pointed out that aspects of the FMEA should be part of the path forward and be adequately described in the FSAR.

According to AREVA NP, there is no failure type or mode of the PS or SAS that can worsen an event analyzed in U.S. EPR Tier 2, FSAR Chapter 15. AREVA NP stated that it would include information regarding its FMEA in U.S. EPR Tier 2, FSAR Section 7.3. Based on the statement above, the audit team questioned the need for 2nd Min/2nd Max if there is no impact to a single sensor failure.

SAS Reliability

The staff noted in AREVA NP Document Number 51-7009531-000, “Comparison of EFW Level Control Reliability with Four Divisions of Sensor Input vs. Single Sensor Input,” issued on October 18, 2010, that the probability of common-cause failure of the communications network is zero. The staff asked AREVA NP to discuss how this value is justified. During the discussion, AREVA NP stated that based on the TELEPERM XS (TXS) system design, it is not credible to have a common-cause failure in both the communications module and the function processor; therefore having a design-basis event that would result in failed outputs from the safety processor and propagation of the failed outputs to other divisions is not possible. The staff finds that this discussion does not provide sufficient justification for the assumed probability of common-cause failure for the communications module since the same software is used in both the communication module and function module. However, given the low probability of occurrence, any assumed value would have little significance in the overall probability of failure. Therefore, the staff considers the assumed probability of failure to be sufficiently accurate to the degree necessary to support the overall conclusion that using four divisions of sensors has lower probability of failure than single sensor input.

The staff also noted that this AREVA NP Document Number 51-7009531-000 did not provide an analysis of how the probability of failure relates to CDF. The use of 2nd Min/2nd Max improves the reliability of the steam generator level sensing since each division now has four signals available for control versus one sensor input. This design provides accommodation for single sensor failures. However, in the consideration of the overall plant reliability, with four trains of EFW, a single failure (including sensor failure) will not adversely impact the plant's ability to achieve the safety function. The staff informed AREVA NP that without an improvement in CDF, use of interdivisional communications to implement 2nd Min/2nd Max functions is not sufficiently justified to warrant the increase in complexity and possibility of unknown failure modes that may affect multiple divisions.

If AREVA continues to pursue the current design of shared sensor inputs, the staff asked AREVA NP to provide an analysis to demonstrate 1) an improvement in the CDF if AREVA NP finds that the use of shared sensor inputs provides for sufficient change in the plant's overall reliability, or 2) potential impacts on safety as analyzed in the Chapter 15 safety analysis if only a single sensor input is used.

AREVA NP also provided the staff with a list of manual, automatic, indication, and interlock functions that use interdivisional communications among the PS, SICS, and SAS divisions to achieve the function. In addition, AREVA NP provided a walk-through of the P&IDs for several examples of systems that used interdivisional communications. This included the CCWS interlocks, residual heat removal/safety injection (RHR/SI) functions, and main steam relief control valves (MSRCV). During the discussion of these examples, the staff informed AREVA NP that for systems such as the RHR/SI that uses interdivisional communication for voting, the staff does not need a justification for the voting feature, but rather a discussion on how the communication for voting addresses DI&C ISG-04. In other cases, AREVA NP should discuss the safety reason for the interdivisional communication, as well as demonstrate how the interdivisional communications address staff guidance in DI&C ISG-04.

SAS Human System Interface Functions

The staff observed that AREVA NP Document Number 51-7009525-000, "Human Factors-U.S. EPR Display Methodology Study Report," issued on October 18, 2010, considered two scenarios for the human factors study. The first scenario allows for multidivisional control and display of safety equipment from each safety display station. The second scenario permits control and display of safety equipment only from the safety display station belonging to the same division. This study was conducted to support the justification that interdivisional communication is required to support human factors considerations in designing the display and control stations. The staff informed AREVA NP that the scenarios considered are insufficient to justify interdivisional communications to support control and indication functions on the safety displays. Specially, the staff discussed with AREVA NP the need to include other scenarios and conditions in addition to these two test scenarios to provide sufficient justification for interdivisional communications. This includes accounting for failure conditions within the study in which the display may be indicating incorrect information from other divisions. This also includes providing different scenarios, such as those that include multidivisional display but not multidivisional control, in order to fully justify why human factors considerations require both multidivisional control and display functions.

As an extension of the discussion on multidivisional control, the staff also asked AREVA NP to discuss the purpose of including multidivisional display and control functions in the SICS when such functions are available from the non-safety PICS, and the PICS is normally used during all plant conditions. AREVA NP staff explained that a human factors study with previous plant operators showed that the operators preferred the inclusion of these functions in SICS to ensure that if the PICS were to fail in an accident condition, they would be able to retain situational awareness in the safety displays given the stressful nature of the situation.

Self Powered Neutron Detectors

The self powered neutron detectors (SNPDs) are safety-related neutron detectors located inside the reactor core. The SPNDs continuously measure the neutron flux at given positions in the core to provide information about the three-dimensional flux distribution. The SNPDs are used in the U.S. EPR design to calculate variables that cannot be directly measured, such as linear power density (LPD) and departure from nucleate boiling ratio (DNBR). The PS system provides automatic reactor trip functions utilizing LPD and DNBR calculations. There are 72 SPNDs used in the U.S. EPR design. In the AREVA NP's proposed design change for the SPND measurement system, each SPND signal is split on its conditioning unit to be sent to the four PS divisions. Therefore, the staff is concerned about the single failure of the SPND signal conditioning unit.

During the audit, AREVA NP discussed information regarding the SPND signal conditioning and transmission circuitry, which consists of a SCV1P module (signal amplifier and current-to-voltage converter), SPAM1 module (potentiometer), and SNV1 module (signal multiplier). The SPNDs are calibrated every 15 days to adjust setpoints and gain based on fuel burn and changes and core reactivity. The SPAM1 module used for the SPND signal conditioning is a multifunctional circuit card that includes a digital potentiometer. According to AREVA NP, the SPAM1 module as a digital potentiometer provides "fine gain control" at the SCV1P card, which receives signals directly from the SPND sensors. The SPAM1 module requires a computer to adjust the onboard potentiometer. The requirement for a computer to modify the potentiometer setting suggests the SPAM1 module has some software or firmware on it. The audit team noted that the approved TXS platform did not include the SPAM1. AREVA NP stated that the chance of a failure for an SPND component occurring in the meantime is not credible. This is a point that will require follow-up discussion either during a future audit or in a future licensing document submittal. The staff is concerned that the SPAM1 module could have in-range static failures that are not detectable by inherent self-testing on the module or the TXS.

The staff has follow-up items to be addressed in a future audit or future submission of licensing documents by AREVA NP:

1. Provide design information on the computer used to calibrate the SPAM1 module potentiometer.

2. Can the SU perform this potentiometer adjustment?

3. Provide the technical basis and necessity for the function that the SPAM1 module provides.

4. If there is a separate computer for the fine adjustment, does the SU have to be plugged in during this activity as well?

During the audit, the staff reviewed the technical literature for the three components used for SPND measurement signal conditioning, including the SCV1P, SPAM1, and SNV1. The staff also reviewed the SNV1 FMEA and the SPAM1 FMEA.

AREVA NP discussed the SPNDs with respect to the SPAM1 module. Regarding what happens if there is a failure in a static way, AREVA NP stated that the FMEA indicated that there are no undetected failures of the PS which includes any components comprising the SPNDs such as the SPAM1 module. Also, according to AREVA NP, the FMEA was not written for any specific hardware and this was out of the scope for that FMEA. The SPNDs are cobalt-59-based. The SPNDs will be calibrated every 15 days. AREVA NP stated that there is no need to look at individual cards. AREVA NP stated that they are looking at very accurate calibration factors, which are precisely approximated out to six decimal places. The staff asked what kind of failures would not be found, that is, how a latent failure can be found if it is upstream. According to AREVA NP, this question pertained to failures that are non-self-announcing failures.

AREVA NP stated that 15 days is the longest number of days that a failure could exist without its knowledge. AREVA NP further indicated that there is a 10^{-15} probability of SPND card module failure in 15 days. AREVA NP further indicated that the only concern about this scenario is if SPNDs are needed to address an event. AREVA NP provided a 14-page white paper, “Credible Failures of SPNDs,” issued on December 12, 2010. AREVA NP said that it is still true that the U.S. EPR design has no failures that are identifiable but non-detectable.

The staff is concerned about the occurrence of non-self-announcing failures, specifically, how AREVA NP addresses non-self-announcing failures. AREVA NP indicated that by using the FMEA data, it determined the probability of non-detected failure. AREVA NP stated there are options to monitor for those particular failures; this could be performed by the gateways or something in plant analysis could be done. AREVA NP asked the staff to consider the acceptability of the following statement: if there is such a small probability of failure, can you then say that there is no possibility of failure? The staff currently considers that all possible failure mechanisms should be considered for the SPNDs and their signal conditioning circuitry. Use of reliability data can support deterministic arguments but should not be the sole basis for addressing failures.

Regarding the implications for the application software addressing aspects of SPNDs (i.e. software-related error checking as a backup to what the hardware is doing), the staff sees that there are layers of error checking (i.e., card based error checking, in which there needs to be a distinction in the error checking).

SPND Self-Monitoring and FMEA

According to the product documentation for all the SPND modules, each component card that makes up an SPND channel has onboard self-monitoring independent of the TXS inherent features, such as the SNV1 signal multiplier module. They operate independently as well according to AREVA NP.

In the product materials for each card, the staff identified a few instances of "cross-channel comparison" that the cards perform to determine a failure. Follow-up items to be raised in a future audit and addressed in future licensing document submittals include, but are not limited to, the following:

1. How is this "cross-channel comparison" made, or what does this data sharing mean?

2. Does this involve some level of interdivisional communications that AREAV NP has not accounted for?

According to the FMEA for each SPND module, non-self-announcing failures are defined as failures that the individual card's self-monitoring cannot detect, nor the downstream receivers of the information being provided by the failed card. The staff's concern is whether the TXS inherent self-testing features can detect these types of failures. According to AREVA NP, the TXS can for the most part, detect failures that the onboard mechanisms cannot detect. AREVA NP also stated that non-self-announcing failures can be detected through periodic testing. The staff also learned about another design aspect of the TXS called "live-zero monitoring". Live-zero monitoring provides an alarm if a signal falls below 4 milliamps (mA). According to AREVA NP, live-zero monitoring is an engineered monitoring feature built into the application software of TXS and is not part of any hardware. Overall, these staff concerns will need to be resolved. The ability and reliability of the TXS platform's self-testing features to detect failures has not been analyzed. Also, the exact types of self-testing available are not yet fully known.

AREVA NP also proposed that the POWERTRAX system could be used to provide continuous monitoring since it pulls information from the SPNDs and can run comparisons to determine if an individual SPND reading has not moved over a given period of time. POWERTRAX used in conjunction with the Aeroball system, looks at the signal coming from the SPNDs that goes through the gateway. AREVA NP stated that this provides an accurate core map, and, since this occurs every 50 milliseconds (which in essence is continuous measuring), a failure would be known. AREVA NP said that an SPND failure is very noticeable and readily detectable, since the SPND either works or it does not. The staff noted that some aspects of the previously discussed information would be helpful with respect to the concerns associated with self-testing. This is only a conceptual design change alternative and has not been formally submitted to the staff for consideration at this time. AREVA NP stated that this would be a way of ensuring against non-self-announcing in-range failures.

Safety Information and Control System

The staff discussed the proposed design changes regarding removal of interdivisional communications in the SICS by using interdivisional communications within the SAS and PS to support the multidivisional display and control functions. The staff informed AREVA NP that, for the purposes of multidivisional display, it may be easier to demonstrate independence for a design that allowed sharing of information on a separate network from the reactor trip and ESF actuation path since failures of the multidivisional display functions can be isolated from the automatic safety functions. Therefore, the original SICS design may offer more independence than the proposed design. The staff also informed AREVA NP that demonstrating a case for multidivisional control requires significantly more information and justification than providing a case for multidivisional display. AREVA NP said it would consider the staff's remarks in proceeding with the SICS design change.

Plant Information and Control System

During the audit, AREVA NP did not provide in-process or completed design or licensing documents to the audit team to review. The audit for this topic should be considered incomplete.

Service Unit and Its Connection to PS/SAS

The audit team found that AREVA NP did not provide sufficient in-process or completed licensing or design documents for the audit. Therefore, the NRC could not complete the audit for the conceptual design information related to SU interface hardware and administrative control protocols proposed to address bidirectional communication issues as indicated in the audit plan. The staff recommended that this item be audited after AREVA NP makes available in-process or completed licensing or design documents.

During the discussion, AREVA NP stated that the SU is used to conduct maintenance; therefore, someone would be present the entire time and would see the light change from green to red, which is an indication that the mode has been changed. The mode key is hardwired to a binary sensor card. AREVA NP stated that it would provide information in the U.S. EPR design certification document (DCD) with respect to a description of the function block and also how the operator will be aware that the mode has been changed. AREVA NP proposed that the SU will only be plugged in for a maximum of 6 hours to perform maintenance and/or surveillance activities. The 6-hour time frame is based on the AREVA NP TS bases allowance of placing a PS/SAS division in bypass for up to 6 hours to do work. AREVA NP did not provide other technical reason for the 6-hour time frame.

During the 6 hours, the SU will be continuously connected with bidirectional communications to the PS/SAS. AREVA NP has proposed four individual hardwired disconnects (one per division of PS/SAS) to the SU. Besides the 15-day SPND calibrations, there are numerous other surveillances that can only be performed with a connected SU. Therefore, this could potentially lead to the SU being plugged in for a far greater extent than the staff would expect if the SU is not going to be plugged in permanently. The TS does not directly mention the SU. AREVA NP is using the TS allowance of 6 hours as a means to justify plugging in the SU. But because the SU is not reflected in the TS bases, there is nothing truly regulating the length of time during which the SU will be plugged in or restricting its amount of use per day, per week, or per shift. Essentially, AREVA NP is treating the SU as maintenance and test equipment (M&TE). This way the SU is connected to everything in a PS/SAS division, which could potentially introduce failures.

During the Rockville portion of the audit, the staff reviewed the drafted SU design change request document for the SU connection. The staff noted that the SU connection to each of the PS and SAS divisions is proposed to have dedicated links with features that allow for hardwired physical disconnects until connection is needed. A proposed 6-hour time limit is set for the connection between the SU and any one division; during this time, the system is operating normally, and this is also when the switch is turned to the operable mode. The staff noted that there seemed to be a connection available for local connections to the PS and SAS divisions. AREVA NP explained that the local connection may be used to connect a local SU to each division and that a combined operating license (COL) action item will need to address administrative controls to prevent modification to multiple divisions at once. AREVA NP stated its intention to have a COL item that addresses the administrative controls to prevent the SU from being connected to more than one division. The staff informed AREVA NP that this may challenge the guidance in DI&C ISG-04; however, the COL action item may be a path for resolving this issue. Additionally, the staff learned that there is a potential SU-initiated failure that can result in a safety system actuation or partial actuation, depending on the case, during what AREVA NP termed a “Go, No-Go” test. AREVA NP stated that normally, the SU cannot initiate a control function of any type. The staff will need more information on this issue.

Online Parameterization Changes

AREVA NP sought the staff’s opinion regarding the ability of the SU to perform parameter changes while the plant is on line. The only case where it can be determined that AREVA NP would need to make a change online is the 15-day SPND calibration (taking into consideration only normal maintenance activities). This would be consistent with current industry practices concerning treatment of nuclear instrumentation. System startup testing may also require online design changes. AREVA NP did not distinguish among the various instances where it would like to perform online changes. AREVA NP will need to provide a comprehensive list of activities that would require online design changes to the application software.

The audit team and AREVA NP discussed the concept of “inoperable but available versus inoperable but not-available.” If it is in parameter or operate mode, then the system is still available; according to AREVA NP, Point 10 in DI&C ISG-04 specifically allows this. AREVA NP asked whether, in parameter mode, a processor being worked on by the SU should be declared operable or inoperable; this will have to be reviewed in the TS. The staff indicated that it would be helpful if, in the U.S. EPR DCD, AREVA NP clarified what is operable and inoperable, especially when inspectors in the field need to determine this. AREVA NP stated that the PS/SAS division that is plugged into the SU will still perform its design safety function if required. Inoperability declarations concerning the SU are another staff concern. The staff believes this should be done on a case-by-case basis. This topic will require further discussion with AREVA NP.

AREVA NP also discussed the possibility of not declaring the processor inoperable while changing parameters (e.g., setpoints) in the parameterization mode. Specifically, AREVA NP asked the staff to provide input on whether online changes to setpoints in one division at a time meet Point 10 of DI&C ISG-04. The audit team informed AREVA NP that, according to the guidance in DI&C ISG-04, Section 1, Point 10, online changes to setpoints to one division at a time is acceptable, provided that technical specification (TS) requirements are met. During the audit, the staff also asked AREVA NP whether the SU can control components. AREVA NP stated that the SU does not have the capability to control components (except for the no-go surveillance test in which it sends a blocking signal to the priority actuation and control system module). The staff notified AREVA NP that there needs to be a commitment to keep the SU from controlling components to prevent future changes to the design that may allow this, and that this commitment may need to reside in Tier 2* portion of the U.S. EPR FSAR.

Potential SU Failure that Can Initiate a Safety Function

AREVA NP indicated that a single division is connected to a single SU, the hardwire disconnect is key controlled, and the operators have control over when an SU is taken to a state when it is disconnected; the status of the connection will be alarmed and seen in the control room. AREVA NP indicated that there will be some additional sections, not reflected in its current closure plan, that pertain to the SU. The staff asked if U.S. EPR Tier 2, FSAR Section 7.5 would reflect the information that the status of the connection will be alarmed and seen in the control room. AREVA NP indicated that it would make that change and include the information in Section 7.5, which pertains to information systems and displays. The staff further asked if AREVA NP would need to make changes to the closure plan and was told that SU changes are not in the current closure plan. However, the staff believes that the changes to the SU should be included in the closure plan.

Additional Information Identified by the Staff

1. According to AREVA NP, the TXS platform has multiple forms of inherent self-testing or self-checking capabilities. Within the TXS platform, the PS and SAS have their own self-testing features, which run independently of one another; the self-testing for both PS and SAS is divisional. The SPND circuit cards have onboard self-testing. In addition, a designer can build engineered monitoring features into the application software. For example, POWERTRAX can be configured to monitor SPND values. The staff will use RAIs to obtain more information on all of these TXS design aspects.

2. AREVA NP will not consider any potential design changes to mechanical or electrical systems that, by avoiding the use of interdivisional communications, could meet the independence requirements. However, the staff commented that AREVA NP should provide safety justifications for each system using interdivisional communications for logic control.

V. <u>Exit Meeting</u>

The staff communicated the following to AREVA NP at the audit exit meeting.

AREVA NP will need to add interactions to its closure plan to achieve the stated results. AREVA NP appears to be running behind the current closure plan schedule, and it remains to be seen if it can provide all deliverables in draft form in a timely manner, so as to achieve the final delivery in accordance with that schedule.

Furthermore, the following specific information was communicated to AREVA NP, using the format delineated in the attached audit plan.

1.a.i Information to support the reliability and enhancement provided for the SAS automatic functions

- The staff needs sufficient justification for the use of interdivisional communications.

- Regarding examples of systems provided by AREVA NP that use interdivisional communication, AREVA NP needs to demonstrate how these systems use interdivisional communications to enhance the safety function, as specified in DI&C ISG-04.

1.a.ii Design documentation related to the SAS HSI functions

- AREVA NP needs to provide sufficient justification for interdivisional communications used for the SAS HSI.

1.a.iv Revised design documentation related to the changes to the SICS interface with the safety divisions

- The staff and AREVA NP discussed the fact that demonstrating a case for multidivisional control requires significantly more information and justification than providing a case for multidivisional display.

1.a.vi Revised design documentation related to data communication between PS divisions

- To demonstrate reliability and independence for sharing the SPND measurements between PS divisions, AREVA NP needs to demonstrate that all failures (i.e., fail-high, fail-low, and in-range failures) can be accommodated by the Chapter 15 analysis, or can be detected and mitigated.

2.a Evaluation of the conceptual design information related to SU interface hardware and administrative control protocols proposed to address bidirectional communications issues

- The staff observed that there seemed to be a connection available for local connections to the PS and SAS divisions. How this local connection may challenge DI&C ISG-04 will be a follow-up topic for a future audit.

- While AREVA NP stated that it will not provide information on the SU through a technical report, the staff and AREVA NP discussed the need for AREVA NP to provide information in the U.S. EPR DCD that states that the SU will not be configured to have control functions. This information will be designated as Tier 2* in the U.S. EPR DCD.

Action Items

1. The staff found that AREVA NP addressed its questions and that the interface with the applicant's personnel was very well coordinated. The staff believes that next steps will include a meeting in February 2011 and possible additional audits.

2. AREVA NP plans to submit additional licensing documentation. As a result of further review of the SAS system, the staff may issue RAIs to ensure that AREVA NP's detailed design addresses the staff's concerns, as delineated in the closure plan.

3. Follow-on interactions are required regarding self-testing, in combination with an audit about two weeks after AREVA NP submits the technical report.

4. Live-zero monitoring was verbally identified as an engineered monitoring feature built into the application software of TXS and not part of any hardware. If a signal falls below 4 mA, an alarm is generated. This topic will be addressed in a follow-up audit.

VI. List of Documents Reviewed

1. 113-7007471-000, “DCS Architecture Changes – Design Certification”, November 15, 2010.
2. 80-7009322-000, “Design Review Board Minutes and Action Items – I&C Architecture Changes”, November 19, 2010.
3. 15-9039599-003, “Safety Automation System-SAS”, U.S. EPR System Description Document, Rev. 3, October 18, 2010.
4. 15-9025647-003, “Protection System (PS)”, U.S. EPR System Description Document, Rev. 3, October 18, 2010.
5. 0405-22, “Design Review Boards”, October 27, 2010, Rev. 023.
6. 51-7009531-000, “Comparison of EFW Level Control Reliability with Four Divisions of Sensor Input vs. Single Sensor Input”, Rev. 000, October 18, 2010.
7. 51-7009525-000, “Human Factors-U.S. EPR Display Methodology Study Report”, October 18, 2010.
8. TXS-2801-76-V.2.0, “TELEPERM XS SCV1P Current-to-Voltage Converter”, Product Brochure, August 2006 Version.
9. Report NLTC-G/2008/0043 (Document No. 0620148878), “SNV1 Failure Modes and Effects Analysis”, Rev D, March 29, 2010.
10. Document No. 062018173, “TELEPERM XS SPAM1 Failure Modes and Effects Analysis (FMEA),” Rev. A.
11. Design Change Request (DCR) 113-7009368-000, “Changes to the PS and SAS Service Unit Connection.” (Draft), No Date.
12. 02-EPR00-NPD-RSI-3XXX Series of PIDs for SI/RHR. (See next page)
13. 15-9085470-001, “SI and RHR System Description Document (SDD).” Section 5.11 Excerpt (I&C only), undated.
14. 15-9098204-000, “CCWS System Description Document (SDD).” October 18, 2010
15. TXS-2631-76-V2.0, “SNV1-2.5 and SNV1-10 Standard Signal Multipliers.” October, 2006 Version.
16. TXS-2601-76-V1.1, “SPAM1 Programmable Analog Signal Processing Module.” July 2008 Version.
17. NLTC-G/2008/en/0072 (Document I.D. No. 0620171050), Revision A, “Neutron Flux Measurement Failure Modes and Effects Analysis” (draft). November, 23, 2010.
18. 51-9060041-003, “Protection System Failure Modes and Effects Analysis for U.S. EPR DCD” (draft). October 18, 2010
19. EPR-EN-PR-1003, “Design Change Control Process.” (Not at Reading Room)
20. 02-EPR00-MPD-RCC-3XXX Series of PIDs for CCWS. (See pages 2)
21. Preliminary Functional Logic Diagrams for CCWS. (See next page 3)
22. EPR-EN-IN-6010, “Distributed Control System Functional Allocation Instruction.” May 28, 2010.
23. EPR-EN-IN-6012, “U.S. EPR Human System Interface (HSI) Design Work Instruction.” (Draft) December 21, 2009.
24. EPR-EN-IN-6015, “U.S. EPR Task Analysis Work Instruction.” (Draft) June 11, 2010
25. 115-907602-003, “U.S. EPR I&C Architecture Design Requirements.” September 5, 2006.
26. White Paper, “Credible Failures of SPNDs,” December 2010.

02-EPR00-NPD-RSI-3XXX Series of PIDs for SI/RHR:

1. EPR00-002-M6-RSI-3001, Revision 001, “Safety Injection System IRWST,” June 17, 2010 (Preliminary).
2. EPR00-002-M6-RSI-3101, Revision 001, “Safety Injection System Residual Heat Removal System, Safeguards Building, Train 1,” June 17, 2010 (Preliminary).
3. EPR00-002-M6-RSI-3102, Revision 001, “Safety Injection System Residual Heat Removal System, Reactor Building, Train 1,” June 17, 2010 (Preliminary).
4. EPR00-002-M6-RSI-3103, Revision 001, “Safety Injection System Accumulator, Train 1,” June 17, 2010 (Preliminary).
5. EPR00-002-M6-RSI-3201, Revision 001, “Safety Injection System Residual Heat Removal System, Safeguards Building, Train 2, “June 17, 2010 (Preliminary).
6. EPR00-002-M6-RSI-3202, Revision 001, “Safety Injection System Residual Heat Removal System, Reactor Building, Train 2,” June 17, 2010 (Preliminary).
7. EPR00-002-M6-RSI-3203, Revision 001, “Safety Injection System Accumulator, Train 2,” June 17, 2010 (Preliminary).
8. EPR00-002-M6-RSI-3301, Revision 001, “Safety Injection System Residual Heat Removal System, Safeguards Building, Train 3, “June 17, 2010 (Preliminary).
9. EPR00-002-M6-RSI-3302, Revision 001, “Safety Injection System Residual Heat Removal System, Reactor Building, Train 3,” June 17, 2010 (Preliminary).
10. EPR00-002-M6-RSI-3303, Revision 001, “Safety Injection System Accumulator, Train31,” June 17, 2010 (Preliminary).
11. EPR00-002-M6-RSI-3401, Revision 001, “Safety Injection System Residual Heat Removal System, Safeguards Building, Train 4, “June 17, 2010 (Preliminary).
12. EPR00-002-M6-RSI-3402, Revision 001, “Safety Injection System Residual Heat Removal System, Reactor Building, Train 4,” June 17, 2010 (Preliminary).
13. EPR00-002-M6-RSI-3403, Revision 001, “Safety Injection System Accumulator, Train 4,” June 17, 2010 (Preliminary).

02-EPR00-MPD-RCC-3XXX Series of PIDs for CCWS:

1. EPR-002-M6J-M222-0001, Revision 00A, “Piping and Instrumentation Diagram Symbols and Legends,” March 18, 2010.
2. EPR-002-M6J-M222-0002, Revision 00A, “Piping and Instrumentation Diagram Symbols and Legends,” March 18, 2010.
3. EPR-002-M6J-M222-0003, Revision 00A, “Piping and Instrumentation Diagram Symbols and Legends,” March 18, 2010.
4. EPR00-002-M6-RCC-3010, Revision 001, “US EPR Component Cooling Water System, Train, 1 Water Supply,” DRAFT – No DATE.
5. EPR00-002-M6-RCC-3011, Revision 001, “US EPR Component Cooling Water System, Train 1, Heat Exchanger,” DRAFT – No DATE.
6. EPR00-002-M6-RCC-3012, Revision 001, “US EPR Component Cooling Water System, Safeguard Building 1 Users,” DRAFT – No DATE.
7. EPR00-002-M6-RCC-3013, Revision 001, “US EPR Component Cooling Water System, Train 1 Pump Detail,” No DATE.
8. EPR00-002-M6-RCC-3014, Revision 001, “US EPR Component Cooling Water System, Train 1 Hydraulically Actuated Valve Details,” No DATE.
9. EPR00-002-M6-RCC-3012, Revision 001, “US EPR Component Cooling Water System, Train, 2 Water Supply,” DRAFT – No DATE.
10. EPR00-002-M6-RCC-3021, Revision 001, “US EPR Component Cooling Water System, Train 2, Heat Exchanger,” DRAFT – No DATE.
11. EPR00-002-M6-RCC-3022, Revision 001, “US EPR Component Cooling Water System, Safeguard Building 2 Users,” No DATE.
12. EPR00-002-M6-RCC-3023, Revision 001, “US EPR Component Cooling Water System, Train 2 Pump Detail,” No DATE.
13. EPR00-002-M6-RCC-3024, Revision 001, “US EPR Component Cooling Water System, Train 2 Hydraulically Actuated Valve Details,” No DATE.
14. EPR00-002-M6-RCC-3050, Revision 001, “US EPR Component Cooling Water System, Common 1B Header,” No DATE.
15. EPR00-002-M6-RCC-3051, Revision 001, “US EPR Component Cooling Water System, Reactor Building, Common 1 Users,” No DATE.
16. EPR00-002-M6-RCC-3052, Revision 001, “US EPR Component Cooling Water System, Common 1 Fuel Building Users,” No DATE.
17. EPR00-002-M6-RCC-3053, Revision 001, “US EPR Component Cooling Water System, Common 1A Header,” No DATE.
18. EPR00-002-M6-RCC-3054, Revision 001, “US EPR Component Cooling Water System, Common OCWS Users,” No DATE.
19. EPR00-002-M6-RCC-3055, Revision 001, “US EPR Component Cooling Water System, Common 1 Containment Penetration Detail,” No DATE.
20. EPR00-002-M6-RCC-3056, Revision 001, “US EPR Component Cooling Water System, Common 1 Hydraulically Actuated Valve Details,” No DATE.
21. EPR00-002-M6-RCC-3065, Revision 001, “US EPR Component Cooling Water System, Common 2 Containment Penetration Details,” No DATE.

Preliminary Functional Logic Diagrams for CCWS:

1. EPR00-002-J3-J500-0001, Revision 00A, “Digital Logic and Functional Block Diagram Symbol and Legend, Sheet 1 of 4,” NO DATE.
2. EPR00-002-J3-J500-0002, Revision 00A, “Digital Logic and Functional Block Diagram Symbol and Legend, Sheet 2 of 4,” NO DATE.
3. EPR00-002-J3-J500-0003, Revision 00A, “Digital Logic and Functional Block Diagram Symbol and Legend, Sheet 3 of 4,” NO DATE.
4. EPR00-002-J3-J500-0004, Revision 00A, “Digital Logic and Functional Block Diagram Symbol and Legend, Sheet 4 of 4,” NO DATE.
5. EPR-00-002-J3-RCS-5034, Revision 00A, “SAS Typical Interdivisional Signal Discrete Logic,” NO DATE.
6. EPR-00-002-J3-RVA-5000*, Revision 00A, “CCWS Train 1 & 2 Common 1.b Supply & Return Switchover Hydraulic Valves and Pumps,” NO DATE.
7. EPR-00-002-J3-RVA-5000*, Revision 00A, “CCWS Train 1 Common 1.B Supply & Return Switchover Valves 5210VN- & 5220VN- Division 1, 2,3, &4,” NO DATE.
8. EPR-00-002-J3-RVA-5000*, Revision 00A, “CCWS Train 1 Common 1.B Supply & Return Switchover Valves 5201VN- & 5217VN- Division 1, 2,3, &4,” NO DATE.
9. EPR-00-002-J3-RCS-5034(EPR00-ILD-RCS-2012), Revision 00A, “CCWS Containment Isolation Valves Interlock,” No DATE.
10. EPR-00-002-J3-RVA-5000*, Revision 00A, “CCWS Train 1-4 Heat Exchanger Flow,” NO DATE.
11. EPR-00-002-J3-RCS-5034, Revision 00A, “CCWS Train 1 Switchover Valves Interlock, Train 1&2 Common 1.b Valve Positions, Divisions 1&2,” No DATE.
12. EPR-00-002-J3-RVA-5000*, Revision 00A, “CCWS Train 1 & 2 Surge Tank Levels,” NO DATE.
13. EPR-00-002-J3-RVA-5000*, Revision 00A, “CCWS Pumps 1-4 Discharge Pressure,” NO DATE.
14. EPR-00-002-J3-RCS-5084, Revision 00A , “Train 1 Common 1.B Supply Switchover, Hydraulic Valve RCC90102VH-, 90104VH-, 90106VH-, 90108VH-, Division 1,2, 3, and 4,” No DATE.
15. EPR-00-002-J3-RCS-5084, Revision 00A , “Train 1 Common 1.B Supply Switchover, Hydraulic Valve RCC9114VH-, 9116VH-, 9118VH-, 9112VH-, Division 1,2, 3, and 4,” No DATE.
16. EPR-00-002-J3-RCS-5084, Revision 00A , “Train 2 Common 1.B Supply Switchover, Hydraulic Valve RCC9202VH-, 9204VH-, 9206VH-, 9208VH-, Division 1,2, 3, and 4,” No DATE.
17. EPR-00-002-J3-RCS-5084, Revision 00A , “Train 2 Common 1.B Supply Switchover, Hydraulic Valve RCC9212VH-, 9214VH-, 9216VH-, 9218VH-, Division 1,2, 3, and 4,” No DATE.

Appendix A

Table 1: NRC Staff Members

Name	Affiliation
Deirdre Spaulding-Yeoman	NRO/DE/ICE1
Jack Zhao	NRO/DE/ICE1
Deanna Zhang	NRO/DE/ICE1
Wendell Morton	NRO/DE/ICE1
Michael Canova	NRO/DNRL/NARP

Table 2: Applicant's Staff Members

Name	Affiliation
Chris Doyel	AREVA NP
Marty Bryan	AREVA NP
Brian McIntire	AREVA NP
Sandra Sloan	AREVA NP
Shelby Small	AREVA NP
George Pannell	AREVA NP
Christian Hessler	AREVA NP
Dennis Budzik	AREVA NP
Thad Wingo	AREVA NP
Tim Stack	AREVA NP
James Tyson	AREVA NP
Jeremy Shook	AREVA NP
Ed Sim	AREVA NP
Mike Gibson	AREVA NP
Rob Weiss	AREVA NP
Ken Coffey	AREVA NP
Doug Brownson	AREVA NP
Sid Scoggins	AREVA NP
Chad Bryant	AREVA NP
Adam Jones	AREVA NP
Nissia Sabri	AREVA NP
George Ifebuzo	AREVA NP
Shaun Brixey	AREVA NP
Mark Royal	AREVA NP

Audit Plan for December 8, 9, 10, and 14, 2010

U.S. EPR Design Certification Final Safety Analysis Report (FSAR) Chapter 7

Instrumentation and Controls (I&C)

Location:

- December 8-10, 2010, AREVA NP, 7207 IBM Drive, Charlotte, NC 28262.
- December 14, 2010, AREVA NP Satellite Location, 1700 Rockville Pike, Suite 400, Rockville, MD.

AGENDA:

The agenda is provided as an attachment to this audit plan.

Purpose:

The Office of New Reactors, Division of Engineering, I&C Branch 1 staff will perform a regulatory audit to examine and evaluate non-docketed technical and in-process documents with respect to the scope of the audit, as described below in the section titled, “Regulatory Audit Scope.” The intent is to gain understanding to support the basis of staff technical decisions, as well as licensing and regulatory decisions. As the applicant’s document processes are draft documents, review of them as un-docketed material is reasonable. All materials will be confirmed once formal docketing occurs.

Regulatory Audit Basis:

An audit is required to evaluate and identify detailed information related to the applicant’s submittals in direct support of the safety conclusions that need to be made regarding Chapter 7 of the AREVA NP design certification application, for the U.S. Evolutionary Power Reactor (EPR) under Part 52 of Title 10 of the *Code of Federal Regulations* (10 CFR Part 52).

10 CFR 52.47(a)(2) requires the design certification final safety analysis report (FSAR) description to be “sufficient to permit understanding of the system designs and their relationship to the safety evaluations” for [10CFR Part 52.47(c)(1)] “an essentially complete design except for site-specific elements...”

A clear level of understanding is necessary to ensure that the required level of information is properly represented in the NRC staff’s forthcoming safety evaluation report (SER) with clearly resolvable open items. The open items are to be addressed in Phase 4 of the subject design certification review.

Regulatory Audit Scope:

2. December 8-10, 2010: A review of the in–process and lower tier documentation in support of changes developed for the Safety Automation System (SAS) as described by AREVA NP in their presentation on June 25, 2010, to address the staff's concerns

   regarding system complexity as it specifically relates to interdivisional communications.

   AREVA NP systems design personnel are requested to be available to support this audit.

   a. Information pertaining to the following issues is requested to be available for this audit:

      i. Information to support the specific reliability and enhancement provided for the SAS Automatic functions.

      ii. Design documentation related to the SAS Human System Interface (HSI) functions.

      iii. Reduction in system complexity as described by AREVA NP in their presentation on June 25, 2010.

      iv. Revised design documentation related to the changes to the Safety Information and Control System (SICS) interface with the safety divisions.

      v. Revised design documentation related to the changes to communications between the Plant Information and Control System (PICS) and the safety divisions.

      vi. Revised design documentation related to data communication between Protection System (PS) divisions.

3. December 14, 2010: A review of the in-process and lower tier documentation in support of AREVA NP proposed changes developed to address:

   a. Conceptual design information related to Service Unit (SU) interface hardware and administrative control protocols proposed to address bidirectional communications issues.

Information and Other Material Necessary for the Regulatory Audit:

Via email dated November 19, 2010, AREVA NP indicated that they will provide the following documents, shown in the following table under the column heading, “AREVA NP Document Identification,” for the portion of the audit that is scheduled for December 8-10, 2010.

Table 1 – Documents AREVA NP to Provide on December 8-9, 2010 for SAS audit

AREVA NP Document Identification	Description
02-EPR00-MPD-RCC-3XXX Series of PIDs for CCWS	Series of Piping and Instrumentation Diagrams (P&IDs) for Component Cooling Water System (CCWS)
02-EPR00-NPD-RSI-3XXX Series of PIDs for SI/RHR	Series of P&IDs for Safety Injection (SI) and Residual Heat Removal (RHR)
15-9085470-001 SI/RHR SDD	SI and RHR system description document (SDD)
15-9098204-000 CCWS SDD	CCWS SDD
15-9091680-001 EBS SDD	Extra Borating System SDD
115-9075067-001 CCWS SDRD	CCWS system design requirements document (SDRD)
115-9091465-001 SI/RHR SDRD	SI and RHR SDRD
CCWS Functional Logic Diagrams	CCWS functional logic diagrams
EPR-EN-IN-6010	Distributed Control System Functional Allocation Instruction
EPR-EN-IN-6012	U.S. EPR Human System Interface (HSI) Design Work Instruction
EPR-EN-IN-6015	U.S. EPR Task Analysis Work Instruction
White paper on 2nd min/max reliability/probability argument for SAS	White paper on 2nd min/max reliability/probability argument for Safety Automation System (SAS)
White paper on human factors task analysis justification for multi-divisional HSI using SAS	White paper on human factors task analysis justification for multi-divisional human-system interface using SAS

Via email dated November 23, 2010, AREVA NP indicated that they will provide the following documents, shown in the following table under the column heading, “AREVA NP Document Identification,” for the portion of the audit that is scheduled for December 10, 2010.

Table 2 – Documents AREVA NP to Provide on December 10, 2010

AREVA NP Document Identification	Description
TXS-2801-76-V2.0	SCV1P Current-to-Voltage Converter
TXS-2631-76-V2.0	SNV1-2.5 and SNV1-10 Standard Signal Multipliers
TXS-2601-76-V1.1	SPAM1 Programmable Analog Signal Processing Module
NLTC-G/2008/en/0043	SNV1 Failure Modes and Effects Analysis
NLTC-G/2008/en/0071	SPAM1 Failure Modes and Effects Analysis
DRAFT NLTC-G/2008/en/0072	Neutron Flux Measurement Failure Modes and Effects Analysis
DRAFT 51-9060041-003	Protection System Failure Modes and Effects Analysis for U.S. EPR DCD

The staff requests that AREVA NP provide documentation which addresses all of the audit areas delineated in the above section of this audit plan titled, “Regulatory Audit Scope.” Examples of the expected documentation include, but are not limited to:

- All of the existing documentation including in-process documentation which supports the changes for the Safety Automation System (SAS) as described by AREVA NP in their presentation on June 25, 2010.

Additionally, the staff requests that AREVA NP provide the following documentation:

- Series of P&IDs for Emergency Feedwater (EFW) system, and Main Steam System.
- Complete set of functional logic diagrams.
- Design change packages for all proposed changes.
- Analysis and study reports to support proposed changes
- Technical design guidelines and standards used for proposed changes
- Impacted licensing documents as described in Table A-1 of the AREVA NP letter NRC:10:089, “Closure Plan for U.S. EPR Instrumentation and Control Communications Independence Issues, Revision 3,” ADAMS Accession No. ML102790100.

Furthermore, the staff requests that AREVA NP provide documentation for review, or identify the information in previously submitted documentation, which addresses the following:

- Clarification of the functional units within the figures in Section 7.3 of the U.S. EPR Tier 2 FSAR, to clearly distinguish the different sub-components of the SAS.
- Functional diagrams for CCWS interlocks and other similar interlocks that demonstrate the need for interdivisional communication between SAS divisions.
- Description of the information that is provided by the PICS in the Technical Support Center (TSC) for display. Describe the pathway for providing information to the TSC.

The staff requests that AREVA NP provide the following audit support documents, to facilitate an efficient and effective audit process, as indicated in the table below.

Table 3: Documents Requested by NRC Staff to Support Audit

Document	Description
Code of Federal Regulations	Chapter 10 Energy – Parts 1-199
IEEE Standard 603-1998	**IEEE Standard** Criteria for Safety Systems for Nuclear Power Generating Stations
DI&C-ISG – 04	Interim Staff Guidance on Highly Integrated Control Rooms – Communications Issues
AREVA NP Closure Plan	10/1/10 letter, Closure Plan for EPR I&C Communications Independence
AREVA NP Updated Closure Plan	Most recent draft Closure Plan for EPR I&C Communications Independence
AREVA NP Tech Reports	Supporting technical reports for AREVA EPR DCD Chapter 7; Digital Protection System,
Approved TXS Topical Report	Approved TELEPERM XS Report
All RAI Responses	All responses to requests for additional information (RAIs)

<u>Audit Team and Support Team - Assignments:</u>

The audit team will review the documents related to the proposed design changes which are available at the time of the audit. Team members are to bring their identified issues for their area of review, to facilitate their review of the AREVA NP proposed design. Additionally, team members are to provide a daily status to the team lead. The team lead will provide a daily briefing to AREVA NP.

<u>Audit Team:</u>

Deirdre Spaulding-Yeoman, Electronics Engineer and Audit Team Lead; will provide team support, will facilitate entrance meeting, daily summary meeting, and exit meeting, and review AREVA NP proposed design changes as related to SRP Sections 7.1, 7.4, 7.5, and 7.6.

Wendell Morton, Electronics Engineer; will review AREVA NP proposed design changes as related to SRP Section 7.3.

Deanna Zhang, Electronics Engineer; will review AREVA NP proposed design changes as related to SRP Sections 7.1, and 7.9.

Jack Zhao, Senior Electronics Engineer, will review AREVA NP proposed design changes as related to SRP Sections 7.2, and 7.8

Support Staff:

Terry Jackson, Branch Chief; will provide management support.
Michael Canova, Project Manager; will provide project management and licensing support.
Daniel Santos, Senior Level Advisor; will attend on December 14, 2010, only.

No quality assurance support from the Division of Construction, Inspection, and Operational Programs is required for this audit. Any materials deemed to be suitable for submittal or citation will be identified for future quality assurance program audit activities.

Room Requirements:

The NRC staff requests the use of a well-lit climate controlled room of sufficient size to accommodate six (6) NRC personnel, and the review of documentation; this room shall be for the exclusive use of the NRC staff. Additionally, the NRC staff requests a separate meeting room where the AREVA NP and NRC staff may interface, in order to allow sufficient privacy to the audit team.

Deliverables:

A technical staff audit report shall be submitted to the project branch addressing the areas of concern and any possible follow-on areas of concern. If necessary, the staff will submit requests for additional information. Information contained in the staff's audit report can be referenced in the draft SER.

Agenda
NRC Audit - U.S. EPR FSAR Chapter 7 I&C
December 8-10, 2010
AREVA NP Office
7207 IBM Drive, Charlotte, NC 28262

Wednesday, December 8, 2010

Time	Topic	Participants
8:30 A.M.	Entrance Meeting	NRC and AREVA NP
9:00 A.M	NRC Audit of Available Documentation	NRC
12:00 P.M.	Lunch	
1:00 P.M.	NRC Audit of Available Documentation	NRC
4:15 P.M.	NRC Audit Team Discussion	NRC
5:00 P.M.	NRC Summary of the Day	NRC and AREVA NP
5:30 P.M.	Adjourn	

Thursday, December 9, 2010

Time	Topic	Participants
8:30 A.M.	NRC Audit of Available Documentation	NRC
12:00 P.M.	Lunch	
1:00 P.M.	NRC Audit of Available Documentation	NRC
3:30 P.M.	NRC Audit Team Discussion	NRC
4:30 P.M.	Summary of the Day	NRC and AREVA NP
5:30 P.M.	Adjourn	

Friday, December 10, 2010

Time	Topic	Participants
8:30 A.M.	NRC Audit of Available Documentation	NRC
12:00 P.M.	Lunch	
1:00 P.M.	NRC Audit of Available Documentation	NRC
3:30 P.M.	NRC Audit Team Discussion	NRC
4:30 P.M.	Exit Meeting	NRC and AREVA NP
5:30 P.M.	Adjourn	

Agenda
NRC Audit - U.S. EPR FSAR Chapter 7 I&C
December 14, 2010
AREVA NP Satellite Location
1700 Rockville Pike, Suite 400, Rockville, MD 28262

Time	Topic	Participants
8:30 A.M.	Entrance Meeting	NRC and AREVA NP
9:00 A.M.	NRC Audit of Available Documentation	NRC
12:00 Noon	Lunch	
1:00 P.M.	NRC Audit of Available Documentation	NRC
3:30 P.M.	Exit Meeting	NRC and AREVA NP
5:00 P.M.	Adjourn	