SUMMARY OF THE NRC STAFF CONCLUSIONS REGARDING ANP-10284, "U.S. EPR INSTRUMENTATION AND CONTROL DIVERSITY AND DEFENSE-IN-DEPTH METHODOLOGY TOPICAL REPORT," REVISION 0

BACKGROUND

By letter (NRC:07:022) dated June 20, 2007 (ML071760187), AREVA NP Inc. (AREVA NP) submitted for U.S. Nuclear Regulatory Commission (NRC) staff review Topical Report (TR) ANP-10284, "U.S. EPR Instrumentation and Control Diversity and Defense-in-Depth Methodology Topical Report," Revision 0 (ML071760188). The TR describes AREVA NP's design approach to Defense-in-Depth and Diversity (D3) for I&C systems applied to its U.S. EPR nuclear power plant design. This approach includes design features and processes that minimize the potential for software common-cause failures (CCFs) in the digital safety systems and a diverse backup system to cope with a postulated CCF occurring simultaneously with an Anticipated Operational Occurrence (AOO) or a Postulated Accident (PA). This TR is intended to provide the D3 generic methodology, not the specific coping analysis for the U.S. EPR.

By letter dated August 20, 2007 (ML072150532), the NRC staff identified that it performed an acceptance review of the subject TR and determined that AREVA NP had not provided the level of detail that would normally be expected in a TR per NRC Office Instruction LIC-500. However, reviewing this document will help advance our efforts with industry to determine what requirements are necessary for digital instrumentation and controls (I&C) and related issues. Therefore, the staff agreed to begin the review and to advise AREVA NP that there will be multiple rounds of requests for additional information (RAIs).

By letter to AREVA NP dated November 1, 2007 (ML072830112), the NRC Staff issued an RAI, and AREVA NP responded to the RAI by Letter NRC:08:003, dated January 22, 2008 (ML080290163). The NRC staff issued a second RAI dated May 15, 2008 (ML081330180), and AREVA NP responded to the second RAI by Letter NRC:08:041, dated June 13, 2008 (ML081690512).

KEY FINDINGS

In a telephone call on December 12, 2008, the NRC stated that TR ANP-10284 could not be approved based on the lack of sufficient information provided to date. Specifically, the staff found that the TR did not address the majority of the criteria used by the staff to make a reasonable assurance finding.

KEY FINDING EVALUATION SUMMARY

During the process of reviewing TR ANP-10284, NRC staff noted the following areas where there was insufficient information regarding the D3 proposal:

- Diversity between Echelons of Defense:

  The TR does not specify the diverse actuation system (DAS) platform specifications or provide a NUREG/CR-6303 Guideline 2 diversity analysis between the DAS and the Protection System (PS).

- BTP 7-19 Points 2 & 3 of the NRC Four-point position on D3 for ALWRs:

  The TR did not provide the plant response calculated using best-estimate analyses for each anticipated operational occurrence (AOO) and each postulated accident (PA) in the design basis occurring in conjunction with each single postulated common-cause failure to demonstrate that adequate diversity and adequate protection exists.

- The TR did not describe how the DAS is designed such that its actuation signals and its initiation of protective functions do not interfere with the PS actuation process or actuation safety functions before the PS.

- The TR did not identify the selection of DAS automatic and manual actuated functions.

- The TR did not address the quality assurance aspects of the design and development process for DAS software and hardware.

- The TR did not establish or describe the applicant's commitment to test the DAS in accordance with the guidance provided in Generic Letter 85-06 and its enclosure titled "QA Guidance for Non-safety-related ATWS Equipment" to ensure availability.

- The TR did not describe the type of environment DAS equipment would be installed in or the requisite assurance commitments necessary to show that the DAS equipment is able to operate in the environment that would occur during normal plant operation, including AOOs.

- The TR does not directly address how the DAS actuation status of the systems and components actuated by DAS is confirmed

- The TR does not describe the architectural aspects of the DAS and how it interfaces with other parts of the U.S. EPR I&C system. Specifically, an adequate description of electrical isolation (isolation devices), communications independence, and physical separation between the DAS and the PS is needed.

- The TR did not provide an evaluation of design features to reduce the effects of spurious trips and actuations.

- The TR did not address assurance of DAS completion of protective actions.

- The TR did not provide an analysis of monitoring or display communication failures or faulty signals and commands that are transmitted to other systems or to the plant data network.

In addition to the items listed above, the information provided by AREVA NP indicated that manual initiation of diverse actuation is performed at the component level versus the system level. This concept is inconsistent with NRC staff guidance and position that indicates a need for system-level manual actuation. Therefore, the staff does not find the component-level manual actuation acceptable. Furthermore, the Priority Actuation and Control System Module (AV42) is a common element for both safety-related engineered safety features actuation and the DAS signals. AREVA NP proposed that the AV42 is not susceptible to a software CCF. However, the NRC staff did not find the AV42 as proposed in TR ANP-10273P acceptable. Therefore, AREVA NP would need to propose an acceptable design with regards to the AV42. Finally, TR ANP-10284 does not clearly indicate how 10 CFR 50.62, "Requirements for Reduction of Risk From Anticipated Transients Without Scram (ATWS) Events for Light-Water-Cooled Nuclear Power Plants," is met. While the NRC staff found some elements of the design may be used to address 10 CFR 50.62, the TR did not clearly address this requirement.

The NRC staff acknowledges that TR ANP-10284 was not intended to address each criterion for a D3 analysis. However, in reviewing Section 7.8 of the U.S. EPR Final Safety Analysis Report, the NRC Staff did not identify information that would adequately address the items listed above. Furthermore, the D3 methodology proposed by AREVA NP largely reflected the guidance in NUREG-6303, and therefore, NRC approval is not needed to use such methods.

OTHER FINDINGS

The NRC staff observed the following aspects of TR ANP-10284 for which no negative findings were identified. These aspects are observations only and should not be construed as approval of the D3 proposal or rule out the potential for negative findings if the TR were submitted in the future.

- Combining the reactor trip and engineered safety features (ESF) actuation as a single line of defense (this approach is also approved in Digital I&C Interim Staff Guidance No. 2, therefore, no explicit licensing approval is required for this approach)

- Failure of a shared sensor between the DAS and the PS would not impair the reactor trip (RT) or engineered safety feature actuation.

- Diversity of power supply between the DAS and the PS

- Diversity of reactor trip means

CONCLUSION

The NRC staff found the information provided in TR ANP-10284 to be insufficient for approval. Due to the lack of information provided in the TR, the NRC staff found little of the design that could be approved without a subsequent condition on the TR requiring additional information to be provided in the U.S. EPR design certification application. Currently, such missing Information is not in the design certification application. AREVA NP would need to address further address the Standard Review Plan acceptance criteria for D3 in a revision to the TR or the U.S. EPR design certification application.