9 April 2013

Subject: AREVA Concerns Regarding NRC Staff Position on Non-Safety Control System Failures for the U.S. EPR

Background: Based on a presentation provided by the NRC on 18 March 2013, titled "Expectations for Addressing U.S. EPR Non-Safety Control System Failure" by Deanna Zhang, Wendell Morton, and Kenneth Mott, AREVA has concerns that the NRC staff is applying a review standard for the U.S. EPR non-safety control system design that is beyond precedence and beyond the intent of D I&C-ISG-04. The implications of the staff's positions will establish a new industry precedent which would likely result in the dismantling of integrated non-safety I&C control systems leading to increased complexity and operator workload, materially reducing the benefits that integrated I&C systems provide for safely operating complex systems.

Action: AREVA requests a public meeting to seek clarifications on the following concerns regarding the NRC Staff interpretation of the Standard Review Plan Section 7.7 and D I&C-ISG-04 as follows:

1. Effects of control system failures - The review should confirm that the failure of any control system component or any auxiliary supporting system for control systems does not cause plant conditions more severe than those described in the analysis of anticipated operational occurrences in Chapter 15 of the SAR. This evaluation should address failure modes that can be associated with digital systems such as software design errors as well as random hardware failures. (The evaluation of multiple independent failures is not intended.)

    - Assessed NRC Position: The evaluation of postulated software errors should extend to all segments of a control system. If two segments have some common code (as would be the case in a segmented control system design) then a common cause failure must be assumed in each segment. It is reasonable to postulate that the software error is such that there is some common trigger that occurs during normal operation that will cause the spurious control actuation of multiple components. NRC Staff does not believe that segmentation of the control system hardware (i.e., processors and sensors) and the differences in the application software for each segment provide sufficient independence.
    - AREVA Concern: Position being communicated by the staff appears to go well beyond the precedent set by the NRC acceptance of a segmented plant control system design for Watts Bar Unit 2, without the required assumption of (or analysis of) spurious control actions across segments (with different processors, sensors, and inherently different software). AREVA has also observed that the NRC has inspected other operating plants that have installed highly integrated digital plant control systems for 10 CFR 50.59 compliance and found segmentation sufficient to demonstrate that the existing Chapter 15 transient analyses remained bounding. The standard being applied to the US EPR appears to exceed these precedents and AREVA is requesting NRC staff clarification to establish a clear understanding of the review standard for the U.S. EPR Design Certification.

2. Potential for inadvertent actuation - The control systems design should limit the potential for inadvertent actuation and challenges to safety systems.

- Assessed NRC Position: Any or all combinations of spurious manuals actions from the non-safety digital operator control station must be treated as a single credible failure that must be bounded by the plant transient analyses in Chapter 15 of the FSAR. No credit is granted for specific verification tasks that establish that unwanted ganged commands are not included in the design. Similarly, no credit is granted for design testing, component testing, pre-operational testing, or start-up testing to validate that design or software errors that lead to unintended multiple component actuations from a single control action can be eliminated from consideration in plant transient analyses.
- AREVA Concern: AREVA agrees with the industry position that this review criterion is insufficient to support the review of a highly integrated digital control room operator work station. AREVA believes that following the DI&C-ISG-04 guidance provides a basis for a reasonable assurance finding that credible spurious manual actuations from the non-safety digital operator control station is limited to a single component or intentionally designed ganged command. If any or all combinations of spurious manuals actions from the non-safety digital operator control station must be treated as a single credible failure, then no integrated plant control room operator work station can be shown to work in a practical sense. The position stated by the staff exceeds the intent of D I&C-ISG-04 and would effectively result in the redesign of the control room operator interface in a way that would have significant impacts on the human factors engineering conclusions by increasing the complexity of operator interfaces and ultimately operator workload. AREVA is requesting NRC staff clarification to establish a clear understanding of the review standard for the U.S. EPR Design Certification.