NRC Staff Conclusions on Aspects of the U.S. EPR Digital Instrumentation and Control Systems Design

Background:

The U.S. EPR design certification application was submitted for NRC review in December 2007. The NRC staff has been reviewing this application since that time and has identified a number of issues that need to be addressed by AREVA NP. AREVA NP has made some progress in addressing some of the issues identified by the staff. For example, a public meeting was held on June 25, 2010, to address significant technical issues associated with I&C independence. In response, AREVA NP made a number of design changes to address some of the issues. However, AREVA NP's May 31 2013 response to the NRC staff's questions indicate that the current design continues to suffer from issues similar to those that had to be addressed in 2010.

Introduction

Software-based, control systems that are not safety-related and displays have the potential to fail in a manner that could challenge safety system performance, induce plant transients, and potentially result in plant behavior that is not bounded by the plant safety analyses. In order to ensure that such potential failures are adequately addressed by the U.S. EPR design, the NRC issued RAI 555, Question 07.01-53, in which the staff requested AREVA NP to address the potential for spurious operation of systems and components due to either software common cause failure (SWCCF) or single failures that could affect multiple control functions. Within RAI 555, Question 07.01-53, the staff identified the regulatory requirements for this issue, including IEEE 603-1991, Clause 5.6.3, "Independence Between Safety Systems and Other Systems." To date, AREVA NP has not adequately addressed this RAI. AREVA NP's response highlights a lack of available design information to address the concern at this stage, provides promises that future design work will ensure that such concerns are addressed, and includes assertions that the non-safety-related software in question would be designed to self detect such issues and protect itself from its own failure. This is inconsistent with agency positions and staff guidance, as outlined below, nor has AREVA NP's response otherwise justified its approach. Therefore AREVA NP's response is unacceptable.

Examples of Assertion that Non-Safety Related Software Will Address Common-Cause Failure

With a few exceptions, the applicant largely relies on affected non-safety-related software to function as a barrier to prevent the propagation of failures within the same software. In other words, if a fault were to occur within the software, the applicant would be relying on the faulted software to reliably and consistently prevent spurious operation of multiple trains of plant equipment. Agency guidance does not provide for such an approach for safety-related software, which has to meet higher standards. The NRC's position on the treatment of SWCCF in safety-related software is outlined in the Staff Requirements Memorandum (SRM) to SECY-93-087, Branch Technical Position(BTP) 7-19 "Guidance for Evaluation of Diversity and Defense-in-depth in Digital Computer-based Instrumentation and Control Systems," and NUREG/CR-6303 "Method for Performing Diversity and Defense-in-depth Analyses of Reactor Protection Systems." Consistent with this guidance, for safety-related software, means are to be taken outside the software affected by the SWCCF to either prevent or mitigate the SWCCF. Means within the software affected by the SWCCF are not to be credited for prevention or mitigation. For the same reasons NRC guidance does not provide for self-correction for safety-related software, the staff rejects the proposal that faulted non-safety-related software can rely on itself to mitigate such faults.

In addition, crediting software design features to mitigate a SWCCF assumes an in-depth and thorough understanding of how the software will operate at the detailed-design level, including an understanding of potential errors, failures, and failure modes. Such an understanding for complex, software-based systems is challenging to achieve. Therefore, the staff position calls for preventive and mitigative means for SWCCF outside the affected software both from a practical approach and to support an adequate level of defense-in-depth.

Example of Insufficient Software / Hardware Failure Analysis

Operating System - The staff finds that the assessment of software failures and failure modes provided in the response to RAI 555, Question 07.01-53 insufficient. For example, on Page 109 of the response, the applicant asserts, yet provides no information to substantiate, that the only way for the operating system to fail in such a way as to cause spurious operation of plant equipment would be through the malicious actions of a programmer. The response does not address functions performed by the operating system other than in regard to communication failures, nor does it provide sufficient design information on the operating system to justify the claims that the software could only fail as a result of malicious actions. AREVA has not provided information sufficient evidence to support this assertion, and accordingly the staff rejects this claim. Regulatory guidance on this topic is covered by BTP 7-19 and NUREG/CR-6303.

Seismic Qualification – The staff finds the analysis of seismically-induced failure of the non-safety-related systems inadequate. For example, one of the staff's concerns in regards to the Process Information and Control System (PICS) and the Process Automation System (PAS) is that failures of these systems as a result of seismic events were not adequately addressed. Per Interim Staff Guidance DI&C-ISG-04, "Digital Instrumentation and Controls", Section 5, "Malfunctions and Spurious Actuations", multi-divisional control and display stations should be qualified to withstand seismic conditions applicable to safety-related equipment at the same plant location. In addition, DI&C-ISG-04 states that non-safety-related stations should be shown to produce no spurious actuation and have no adverse effect upon any safety-related equipment or device as a result of a design basis condition, both during and after that condition. Lastly, Digital Instrumentation and Control (DI&C)-Interim Staff Guidance (ISG)-04 states that if spurious actuations are possible as a result of the design basis condition, then the safety analyses must envelope those spurious actuations. On page 110 of the response, the applicant stated that operator actions will mitigate failures resulting from seismic events. The applicant has provided no technical basis to justify the reliance on operator actions. Without a supporting technical basis, the staff does not consider operator actions a sufficient mitigation strategy. Since the applicant did not analyze for seismically-induced failure of PICS and PAS per the guidance it committed to follow, the staff finds that the applicant did not consider all the credible failure modes and did not demonstrate that these potential failure modes are enveloped by the safety analyses to address the guidance of DI&C-ISG-04. Therefore, the staff finds the applicant's approach unacceptable.

Examples of Insufficient Justification and Indications of Incomplete Design

The applicant introduced the use of NUREG/CR-7150, "Joint Assessment of Cable Damage and Quantification of Effects from Fire," to address the categorization of credible, implausible, and incredible events. This document has not been approved by the NRC for use in digital I&C-related reviews or guidance, especially in terms of evaluating the credibility of SWCCF or single failures that could lead to SWCCFs in software-based digital I&C systems. Furthermore, the application does not provide sufficient justification for applying this NUREG to digital I&C systems. The NRC has guidance that addresses SWCCF (e.g., BTP 7-19 and NUREG/CR-6303). The staff finds the applicant's has not justified its use of NUREG/CR-7150.

On Page 22 of the response, the applicant states, "SWCCFs that are triggered through plant parameters that are experienced during normal plant startup and power levels will be identified and resolved during the software verification, testing, and simulation phases." As stated in Branch Technical Position (BTP) 7-19, the staff does not agree that software defects, including those that potentially could lead to a SWCCF, can be completely removed during the software development process. Even with high-quality and high-integrity safety-related software development, the assumption is that latent defects will exist, and it is the responsibility of the applicant to demonstrate that the overall safety of the plant is ensured in the presence of failures caused by latent software errors. The staff finds the applicant's approach unacceptable.

On Pages 79 and 87 of the response to RAI 555, Question 07.01-53, the applicant provides a brief listing of software development activities for PAS and PICS. In both places, the applicant states that for PAS and PICS, verification and validation (V&V) of software and the "criticality analysis" are performed under accepted industry practice. However the applicant does not define those practices, leaving them open to broad interpretation. The staff finds this unacceptable.

The staff also had questions regarding potential failures of equipment protective functions, potential spurious actuations, and whether failures associated with these protective functions have been fully assessed by the applicant. In response, the applicant indicated a lack of complete design to allow for addressing the concern at this time and provided statements that the concerns will be addressed during detailed design. The staff finds this approach unacceptable because it does not provide the justification necessary to reach a safety conclusion. Examples of such language include, but are not limited to, the following:

> Non-safety-related I&C system failures that could impact multiple process systems were excluded from this analysis because the population of non-safety-related I&C functions will not be fully defined until detailed design is completed. [Page 4]
>
> There are non-safety-related functions that control multiple process systems in the plant, but these functions were not currently defined and were determined to be addressed as part of the software program lifecycle as the functions are developed (refer to Appendix F of this Response). [Page 12]
>
> Some examples of postulated credible and incredible failures are addressed in this Response. This Response is not meant to include an exhaustive list of credible and incredible failures. [Page 15]

Lack of Justification for Segmentation Approach and Insufficient Analysis

Control function segmentation is a process used in nuclear DI&C applications. Control functions are strategically dispersed (segmented) across divisions and organized differently within the divisions. The goal of segmentation is to introduce sufficient independence and diversity across segmented portions to allow credit for a level of diversity. Justification of segmentation involves presentation of information on important elements such as separation and independence, commonalities and differences in input signals, commonalities and differences in algorithms and execution of these algorithms, and an analysis of how common elements are evaluated in relation to their effects on segmentation.

The applicant proposed segmentation as a means to help address SWCCFs that could result in spurious actuation of multiple, redundant trains of plant equipment. The applicant proposed to disperse critical control functions systematically to a set of segments. The applicant also proposed to disperse non-critical control functions to segments so that no segment has the same combination of critical and non-critical control functions. However, the applicant did not provide a justification addressing the elements above to demonstrate the adequacy of this strategy.

For example, if the critical control functions have the same algorithm and sense the same inputs, the applicant would need to provide information to justify how the different combinations of non-critical and critical functions on each of the divisions introduce sufficient differences to justify successful segmentation. Alternatively, the critical control functions themselves could have different algorithms and/or sense different inputs to achieve effective segmentation.
In addition, a segmentation analysis would need to be presented on a scenario basis (e.g., feedwater heater isolation) to demonstrate effectiveness of the proposed design. The staff raised this concern with the applicant at a March 2013, public meeting. However, to date, the applicant has not been able to provide such information. The applicant has indicated that sufficient design detail is not yet available to allow submittal of such information. Based on this, the staff considers the segmentation analysis incomplete and unacceptable.