Industry Recommended Areas for Improvement in BTP 7-19

Public Meeting to Discuss the U.S. Nuclear Regulatory Commission (NRC) Staff Effort to Re-Evaluate its Position and Guidance on Digital Instrumentation and Controls Common Cause Failure

August 22, 2016

BTP 7-19 Areas for Improvement

- Discussion Points
  - Scope
  - Diversity
  - Four-Point Position
  - Bounding/Coping
  - Design Attributes to Eliminate CCF
  - Information for Review
  - Acceptance Criteria
  - Single Failure and CCF

Scope

Section A – *"In summary, while the NRC considers (software) CCF in digital systems to be beyond design basis, NPPs should be protected against the effects of anticipated operational occurrences (AOOs) and postulated accidents with a concurrent CCF in the digital protection system."*

Industry comment: The limited scope stated in this paragraph conflicts with the much broader scope (safety systems) identified in Section 3. This should be clarified.

Diversity

Section A(3):

- *Verify that adequate diversity has been provided in a design to meet the criteria established by NRC guidance.*
- *Verify that the displays and manual controls for (plant) critical safety functions initiated by operator action are diverse*

Industry Comment: Diversity is not the only answer. It should be acceptable to verify adequate plant protection for CCF, either by preventing CCF or coping with CCF

Four-Point Position

Section B (1.4):

Point 1 - "*The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.*"

Industry Comment: Clarify that if vulnerability to CCF has been adequately addressed (i.e., CCF not credible), then Points 2 and 3 are not applicable.

Point 4 - "*A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.*"

Industry Comment: Clarify that this means that any new CCF vulnerability does not affect these displays and controls; if it does then backup diverse displays and controls are needed. Independence between manual and automatic controls is not required.

Bounding/Coping

Section B (1.4)

Concerning Point 2 – "*Thus, in performing the assessment, the vendor or applicant should analyze each postulated CCF for each event that is evaluated in the SAR section analyzing power operation accidents at the plant conditions corresponding to the event. This analysis may use realistic assumptions to analyze the plant response to DBEs, or the conservative assumptions on which the Chapter 15 SAR analysis is based*"

Industry Comment: Clarify as follows:

- That best estimate may be used for beyond design basis CCF sources; conservative methods must be used for CCF sources that are within the design basis.
- The difference between bounding and coping
- For the Point 2 analysis a CCF that affects a mitigation function is considered coincident with each AOO or PA, including a Loss of Offsite Power (LOOP). Since a LOOP is a CCF, a digital CCF does not need to be considered coincident with an AOO/PA
- That for a CCF in a transient initiator (eg. feedwater control system or ESF spurious actuation), the transient is considered with no other concurrent AOO, PA or LOOP.

Design Attributes to Eliminate CCF

Section B (1.9) - Diversity or Testability

Industry Comment:

Alternate approaches need to be considered for flexibility. In NEI 16-xx, the industry will describe additional defensive measures that can be credited to eliminate consideration of CCF; the industry has referred to these as preventive measures. The industry will also describe defensive measures that cannot eliminate consideration of CCF, but can limit the effects of a CCF to make the CCF coping analysis described in Point 2 more manageable; these are referred to as limiting measures.

Information to be Reviewed

Section B (2) and B (3.1):

- *"The information to be reviewed is the D3 assessment conducted by the applicant".*
- *"The D3 assessment submitted by the applicant should demonstrate compliance with the NRC position on D3 described above"*.

Industry Comment: Add clarification to allow "inspection" of assessments rather than limiting information to "review" or submittal by the applicant.

Acceptance Criteria

Section 3.0 – Acceptance Criteria

Industry Comment: This section is only applicable, when consideration of CCF cannot be eliminated as discussed in Section 1.9 above.

Section 3.1 – Specific Acceptance Criteria

Industry Comment: Add Item 10, which explains what it means to be bounded for 50.59 Question 6 (i.e., same margin to critical safety limits, same method of mitigation). For design basis CCF sources, the bounding assessment considers only AOOs. For beyond design basis CCF sources the bounding assessment can also consider PAs

Single Failure and CCF

Section B (3.3)

"Since CCF is not classified as a single failure (as defined in RG 1.53), a postulated CCF need not be assumed to be a single failure in design basis evaluations. Consequently, realistic assumptions can be employed in performing analyses to evaluate the effect of CCF coincident with DBEs."

Industry Comment:

Clarify that a single failure of a digital resource that is shared by multiple SSCs can result in a CCF of those SSCs, and these CCFs are within the design basis. If these CCFs are not prevented conservative analysis methods apply.