From: VAUGHN, Stephen
To: Morton, Wendell; Govan, Tekia
Subject: [External_Sender] NEI Proposed Guidance for Section 1.8 of BTP 7-19
Date: Thursday, August 01, 2019 3:34:28 PM
Attachments: Revision to Section 1.8 of BTP 7-19 - Spurious Actuations - Revision 5.docx

---

Wendell and Tekia,

Based on the technical discussion during the public meeting today, the NEI Digital I&C working group made some edits to the draft we provided via email on 7/25. Please find the updated version attached to this email for your consideration as the staff continues the BTP 7-19 revision process.

We look forward to reviewing the draft revision of BTP 7-19 in mid-August and the subsequent public discussion at the end of August.

Regards,

Steve

STEPHEN J. VAUGHN | *SENIOR PROJECT MANAGER, ENGINEERING AND RISK*
1201 F Street, NW, Suite 1100 | Washington, DC 20004
P: 202.739.8163 M: 202.256.5393
sjv@nei.org

1.8 CCF and Consideration of Spurious Actuations

Guidance for addressing software common cause failures in safety-related systems is provided in IEEE Standard 379, Clause 5.5. Clause 4 of IEEE Standard 379 provides guidance on addressing spurious system actuations that cause, or are caused by, a design basis event which the safety function is required to mitigate.

Failure of software to perform as intended is a result of a deficiency in the software design. Clause 5.5 of IEEE Standard 379 states that common cause failures resulting from design deficiencies are not subject to the single failure criteria. As a result, software common cause failures are not subject to the single failure criteria.

Although software common cause failures are not subject to the single failure criteria, it is important to eliminate, to the extent practicable, software design deficiencies. Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-based I&C Systems", states that software quality "is an important element in preventing the propagation of common-cause failures." The first barrier of defense against software design deficiencies is a high-quality design process and specifically, a high-quality software development process. The second barrier is the nuclear quality assurance program which ensures the high-quality software development process was properly implemented.

For A1 systems, the reviewer should compare the applicant's software design and development process to the review guidance in BTP 7-14 to reach the conclusion that the software design and development process is of sufficient quality. In addition, the reviewer should assess the defensive design measures that were relied upon to reach a conclusion that the likelihood of a spurious actuation caused by a CCF is sufficiently low. Examples of defensive design measures that could significantly reduce the potential for spurious actuation are:

1. 2 out of 4 (2oo4) coincidence logic of four divisions before issuing an ESFAS or Reactor Trip system level initiation
2. 2oo2 coincidence logic within a single division for ESFAS actuations
3. Energize to actuate design for ESFAS to avoid spurious actuation versus a deactivate design for Reactor Trip
4. Use of only safety displays for manual soft control of A1 components with onerous spurious actuation consequences.

For B1, A2, and B2 systems, as part of the applicant's qualitative assessment[1] for the system, the reviewer should evaluate that the qualitative assessment supports a conclusion that a proposed digital I&C modification has a sufficiently low[2] likelihood of a spurious actuation.

[1] For guidance on a qualitative assessment see Regulatory Issue Summary, "CLARIFICATION ON ENDORSEMENT OF NUCLEAR ENERGY INSTITUTE GUIDANCE IN DESIGNING DIGITAL UPGRADES IN INSTRUMENTATION AND CONTROL SYSTEMS", ML18143B633)

[2] "Sufficiently low" means much lower than the likelihood of failures that are considered in the updated final safety analysis report (UFSAR) (e.g., single failures) and comparable to other CCFs that are not considered in the UFSAR (e.g., design flaws, maintenance errors, calibration errors)."