PUBLIC SUBMISSION

As of: 3/17/20 2:35 PM
Received: March 16, 2020
Status: Pending_Post
Tracking No. 1k4-9flf-rw9s
Comments Due: March 16, 2020
Submission Type: Web

Docket: NRC-2019-0253
Proposed Revisions to Standard Review Plan Branch Technical Position 7-19 "Guidance for Evaluation of Potential Common Cause Failure in Digital Instrumentation and Control Systems"

Comment On: NRC-2019-0253-0001
Proposed Revision to Standard Review Plan Branch Technical Position 7–19 Guidance for Evaluation of Potential Common Cause Failure Due to Latent Software Defects in Digital Instrumentation and Control Systems

Document: NRC-2019-0253-DRAFT-0007
Comment on FR Doc # 2020-00350

Submitter Information

Name: Ken Scarola
Address:
3672 Pine Tree Ln
Murrysville, 15668
Email: KenScarola@NuclearAutomation.com

General Comment

Nuclear Automation Engineering, LLC submits these comments for consideration by the Staff. The attachment addresses specific issues raised by other BTP 7-19 Revision 8 commenters.

Attachments

2020-03-16 NAE Response to Comments from Others

BTP 7-18 Revision 8 Draft - Comments from Nuclear Automation Engineering

Nuclear Automation Engineering, LLC submits these comments for consideration by the Staff. These address specific issues raised by other BTP 7-19 Revision 8 commenters.

Comment: *The guidance in SRP 7.7 is confusing because it suggests that postulated NSR failures that can cause spurious actuations must meet the acceptance criteria for anticipated operational occurrences (i.e., treated as design basis events). However, the actual practice for new plants reviews and the direction taken in Draft Revision 8 of BTP 7-19 is that certain postulated failures in NSR systems that affect spurious actuation of multiple components can be treated as beyond design basis events with other acceptance criteria.*

> NAE response: The words *"failure of any control system component"* is commonly understood to refer to a random hardware component failure, not a design defect. Since random hardware failures are expected to occur during the life of the plant, the SRP is correct in that the plant level results of a random hardware failure (i.e., any component) should be treated as an anticipated operational occurrence (AOO), which is a design basis event (DBE). On the other hand, spurious operations due to a design defect are not expected to occur during the life of the plant because (1) the rigorous design processes applied to the control systems covered by SRP Section 7.7 make design defects unlikely, and (2) while there is no claim for defect free designs, the unusual conditions needed to trigger a defect are not expected to occur during the life of the plant. Therefore, for new plants, erroneous operations due to a design defect have been treated as beyond design basis events (BDBE) with relaxed analysis methods (e.g., best-estimate) and relaxed plant level acceptance criteria (e.g., as required for postulated accidents, not AOOs). BTP 7-19 should clearly make these distinctions for NSR control systems as well as SR systems within the same safety division.

Comment: *The guidance in SRP 7.7 is also confusing regarding the statement "evaluation of multiple independent failures is not intended,"… That same statement has also been used to require additional features within an NSR system design to provide some other type of 'independence' (e.g., controller segmentation) that has no established regulatory definition.*

> NAE response: BTP 7-19 should clarify the distinction between inter-division independence and intra-division independence. In accordance with IEEE-603, RG 1.75 and IEEE-384, inter-division independence must accommodate single random hardware failures, as well as fire (within enclosures), flood and electrical faults. Traditionally, when considering intra-division independence, only random hardware failures have been evaluated. The difference is based on the expected likelihood of these events, as discussed above. BTP 7-19 should also clarify that common intra-division design features, such as segmentation, cannot prevent erroneous signals that may be generated by a random hardware failure or design defect in one segment from propagating to other segments; other defensive measures are also required. Equally important is that without adequate defensive measures, a random hardware failure or design defect in a shared resource, such as a communication network or visual display unit, can adversely affect multiple segments.

Comment: *The guidance in DI&C-ISG-04 provides acceptable defensive measures that eliminate spurious actuation concerns from operator interface stations.*

> NAE response: The guidance in ISG-04 is insufficient, because:

(1) There is no discussion of the effects of workstation failures or design defects on intra-division NSR or SR equipment. ISG-04 is limited to inter-division issues.
(2) The guidance for two operator actions is inadequate because it does not address independence for the processing and communication of those actions. Without adequate defensive measures, there are single random hardware failures and single design defects that can erroneously generate the signal (or signals) that would normally result from both actions.

Comment: *Remove the applicable guidance from BTP 7-19 Draft Revision 8… regarding the treatment of spurious actuation hazards.*

NAE response: Spurious operations are a serious threat to plant safety due to the ever-increasing extent of digital integration. Raising awareness to these issues in BTP 7-19, including the distinction in analysis methods for spurious operations due to random hardware failures and design defects, is guidance that industry needs in the short term. In the future, the Staff should provide additional more comprehensive guidance to address defensive measures that can be credited in preventing or limiting spurious operations from both of these sources.