Comments from Nuclear Automation Engineering on NEI 20-07 Draft B “Guidance for Addressing Software CCF In High Safety-Significant Safety-Related Digital I&C Systems”

Comments Overview

- The focus on software CCF does not recognize the likelihood of a design defect in hardware aspects of digital designs.
- The case for using design process attributes exclusively to eliminate further consideration of CCF is inadequate.
- The "no CCF" operating history for systems complying with IEC 61508 is incorrectly correlated to nuclear applications.
- The bases that non-concurrent triggers, segmentation, preferred failure states or operating history can eliminate CCFs are technically insufficient.
- Attempting to eliminate all further consideration of CCF is not in the best interests of the nuclear industry.

Incorrect Distinction for CCFs due to Software

- The likelihood of a design defect is related to complexity.
- The complexity of most digital hardware requires that it be designed with software based development tools.
- Design defects in complex digital hardware are no less likely than defects in complex digital software.
- Even simple hardware and software can have complex interactions.
- Therefore, there is no technical basis for limiting consideration of CCF due to design defects in software only.
- BTP 7-19 Revision 8 Draft has eliminated the CCF distinction for software only.

Inadequate Crediting for Design Process

- The nuclear industry has been applying a rigorous design process to the development of digital safety systems since the 1970s.
- A rigorous design process, which supports the low likelihood of a design defect, was the primary basis for the NRC commissioners defining a digital CCF as a beyond design basis event in the SRM to SECY 93-087.
    - A rigorous design process was not a sufficient basis for the NRC commissioners to conclude that a design defect requires no further consideration.

Inadequate Crediting for Design Process (cont.)

- There is no evidence that a design process that complies with IEC 61508 vs. the IEEE standards currently applied by the US nuclear industry (and other US industries with mission critical applications) would yield a significant reduction in the likelihood of a design defect, thereby supporting a conclusion that a design defect requires no further consideration.
  - The same goals derived from IEC 61508 are derived from IEEE standards.
  - International nuclear regulatory bodies which invoke IEC 61508 also require explicit assessment of the consequences of postulated CCFs in digital I&C systems (IEC 61226, IEC 62340, MDEP DICWG-01). A diverse actuation system is required.
- Note that IEC 61508 also requires deterministic design attributes which are not required by NEI 20-07.

Incorrect Operating History Correlation

- IEC 61508 is applied to numerous process industries that do not have redundancy comparable to nuclear safety systems.
  - The lack of CCFs is more likely due to inherent diversity of applications, which leads to non-concurrent triggers and different application level defects, not due to no design defects.
  - Defects in systems that comply with IEC 61508 could result in CCFs of multiple redundancies if they resided in nuclear safety applications.
- Complex designs have defects.

Incorrect Crediting for Non-Concurrent Triggers

- Non-concurrent triggers cannot be credited to prevent all CCFs.
- Triggered design defects can cause process upsets or alarms (i.e., self-announcing), which are immediately detectable by plant operators. These defects can be corrected before the same defect is triggered in additional digital processors (i.e., before a CCF of multiple processors).
- Triggered design defects can erroneously close the non-automated suction/discharge valves of pumps that are normally in standby. These failures may be undetected between periodic surveillances; therefore, non-concurrent triggers (e.g., months apart) can result in CCF of multiple pumps.
- A triggered design defect that leads to failure-to-actuate may be undetected until there is a process demand for actuation. The same defect can be triggered months apart (i.e., non-concurrent) in multiple digital processors (i.e., a CCF).

Incorrect Crediting for Segmentation

- Distribution of functions to multiple processors (i.e., segmentation) is not sufficient to limit the effects of a design defect to only one processor.
- The segments must also be sufficiently diverse to prevent concurrent triggering of the same defect (e.g., differences in applications, I/O configurations, communication configurations).
- The triggered defect must be self-announcing to prompt corrective actions. Triggers that result in no process upset or no alarm remain hidden, allowing non-concurrent triggers to result in a CCF.

Incorrect Crediting for Preferred Failure States

- A preferred failure state cannot be guaranteed for a design defect, because the cause (or trigger) and effect of the defect cannot be determined.
  - If we knew the trigger condition, we would correct the defect to correctly respond to the trigger.
  - Since we don’t know what the defect is, we can’t trigger it.
  - Since we can’t trigger the defect, we can’t know its effect.
- Therefore, we cannot assure a preferred failure state when the defect is triggered.

Incorrect Crediting for Operating History

- Operating history tells us only that hidden defects have not been triggered by the historical applications.
  - Operating history does not tell us that defects don't exist or that defects will not be triggered in the future.
- Operating history is a component of commercial grade dedication, which demonstrates that a product is equivalent to a 10 CFR 50 Appendix B product.
  - This provides a basis to conclude that a design defect is sufficiently unlikely so that a CCF may be considered a beyond design basis event; it is not a basis to conclude that a CCF requires no further consideration.

Managing CCFs is in the Best Interests of the Nuclear Industry

- Efforts to conclude that design defects in complex digital systems require no further consideration, based solely on qualitative design process attributes, are not consistent with the defense-in-depth bases of the nuclear industry.
- Digital systems can be deployed with cost effective deterministic defensive measures that prevent or limit most CCFs.
- Where a CCF must be managed, very simple non-safety diverse digital backup equipment can be deployed cost effectively. The “best estimate” analyses to demonstrate the effectiveness of backup equipment is not complex or costly; high fidelity training simulators have also been used.
- Backup equipment provides an additional layer of defense to cope with breaches in secure development or operational environments (e.g., cyber attacks).
- Backup equipment can be credited to extend LCO completion times, when front-line equipment is inoperable.
- Backup equipment can facilitate cost effective Appendix R compliance for large scale digital modernizations.