Chiller Example Part 3
CCF Methodology Illustration Alternative

July 11 2016 • NRC CCF Workshop • Washington DC

Overview

- In Part 2, we explained that Level 2 could not be reached for an implementation design defect, so plant safety was demonstrated through a CCF Coping Analysis.
  - Level 2 - CCF not credible (i.e., as unlikely as other sources of CCF that are not considered in deterministic safety analysis)
- However, other Chiller applications have additional design attributes that were not considered at the time the EPRI report was written.
- Using the preventive (P) measures described in the EPRI report, these design attributes can be credited to reach Level 2.
- This alternative will be in NEI 16-XX.

CCF Prevention from a Design Defect

- A CCF requires both a defect and a concurrent trigger affecting multiple SSCs.
- A defect must be assumed due to the complexity of this digital application.
- NRC guidance, including NUREG/CR-6303, requires consideration of a defect in a single software block, not multiple different defects.
- A concurrent trigger of the defect in that software block in both trains is not credible for this chiller application.

Non-Concurrent Triggers

- The chiller in one train is in operation at all times; the other train is in standby. The operating chiller is continuously processing external inputs; the standby chiller is not.
  - The software execution trajectory in each chiller controller is different, making a concurrent internal trigger unlikely.
    - E.g., memory overload, memory allocation errors
- The operating chiller has external stimulation, the standby chiller has none.
    - No common external triggers.
- Neither chiller changes state for ESF actuation.
  - No triggers concurrent with plant accidents.

CCF Prevention

- Different configurations with different external stimulation makes a concurrent trigger in both trains unlikely.
- But to claim we have achieved Level 2, we must also ensure a triggered defect is detectable, so it can be corrected before non-concurrent triggers accumulate to become a CCF.
  - If a trigger occurs in the standby train there could be
    - Spurious actuation – Immediately self-announcing to plant operators
    - Inability to actuate – No effect because other train is running; detectable on next demand (periodic train switchover)
  - If a trigger occurs in the operating train there could be
    - Spurious de-energization – Immediately self-announcing to plant operators
    - Inability to de-energize – No effect because train continues to run; detectable on next demand (periodic train switchover).
    - **Inability to restart after a LOOP**

LOOP Consideration

- Inability to restart after a LOOP is bounded by the SBO analysis, which credits operator actions to restore cooling.
  - This case is less onerous than an SBO because the triggered defect affects only one train; the other train can be put into operation immediately.
- LOOP concurrent with an AOO/PA and a concurrent digital CCF is not considered.
  - LOOP is a CCF; NRC guidance does not require consideration of two concurrent (and independent) CCFs.
    - Licensing precedence for all ALWRS and Oconee RPS
      - But no clearly documented NRC guidance

Impact on Regulatory Guidance

- SRM to SECY 93-087 and BTP 7-19 start with a CCF vulnerability assessment.
  - Coping analysis is not required if there is no CCF vulnerability.
- But BTP 7-19 allows a CCF vulnerability to be precluded only through simplicity (100% testing) or internal diversity.
  - A revision is needed to permit demonstration of non-concurrent triggers and other P measures that will be presented in NEI 16-XX.
- This revision will not provide 100% assurance; no regulatory guidance does. But it can give the designer a very high level of assurance, which facilitates a conclusion of reasonable assurance for the regulator.

Questions?