Preview – Appendix A of NEI 16-16

"Guidance for Addressing Digital Common Cause Failure"

Vic Fregonese

Nuclear Energy Institute

Meeting Between the U.S. Nuclear Regulatory Commission Staff and the Nuclear Energy Institute

April 11, 2017

Agenda

- Overview of NEI 16-16 Appendix A
- Preventive (P) Measures
- Limiting (L) Measures
- Likelihood Reduction (LR) Measures
- Questions/Comments

NEI 16-16 Appendix A

- Will use the Appendix A from EPRI Report 3002005326*

** Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems.*

EPRI, Palo Alto, CA: 2016. 3002005326.

NEI 16-16 Appendix A

- Defensive measures are provided for preventing or limiting a CCF of multiple controlled SSCs caused by an I&C failure in each of the following categories:
  - Single random hardware failure (9 types of equipment)
  - Single environmental disturbance (5 types of disturbances)
  - Single design defect (5 types of defects)
  - Single human error (1 type of error)
- A CCF Susceptibility Analysis uses preventive (P) measures in Appendix A to determine the applicability of each failure source and determine if a CCF from each applicable source is credible or not. If a CCF is credible, the CCF Susceptibility Analysis can use limiting (L) measures in Appendix A to identify the SSC malfunction result.

Navigation

- There are 45 tables of detailed P and L measures that will be provided in Appendix A, spread across 92 pages.
  - There are 67 P measures and 35 L measures
  - A PDF attachment is being considered to support printing a summary listing of all P and L measures on one sheet of paper, size C for readability
  - A preliminary version of this is available as a handout at the meeting today
- Do not read the subject line of a P or L measure and consider it the whole measure. The details matter.

Preventive Measure

- A preventive (P) measure is a set of defensive measures that when applied as a set, provide reasonable assurance that a CCF potentially caused by a specific I&C failure source is not credible.
  - When a CCF is not credible, no further consideration is required.
- NEI 16-16 Appendix A provides a series of preventive measures for each category of I&C failure source:
  - Single random hardware failure (e.g., redundancy, no shared resources)
  - Single environmental disturbance (e.g., equipment qualification, barriers)
  - Single design defect (e.g., quality, avoidance of concurrent triggers, self-announcing, testing, operating history)
  - Single human error (e.g., human performance, HFE)
- CCF credibility is determined for each applicable failure source using the preventive measure tables in Appendix A.

Limiting Measure

- A limiting (L) measure is a set of defensive measures that when applied as a set, provide a predictable component level malfunction for a credible CCF.
  - A credible CCF means the malfunction result must be analyzed. It may be bounded by a previous plant level analysis in the FSAR, or it may require an analysis to be added to the FSAR. Limiting measures generally make the analysis easier and help identify coping methods.

Limiting Measure (continued)

- NEI 16-16 Appendix A provides a series of limiting measures for each category of I&C failure source:
  - Single random hardware failure (e.g., limit the number of SSCs that share an I&C resource, force a preferred SSC malfunction)
  - Single environmental disturbance (e.g., limit the number of SSCs affected, barriers, force a preferred SSC malfunction)
  - Single design defect (e.g., limit the number of SSCs affected, quality, operating history, force a preferred SSC malfunction)
  - Single human error (no limiting measures)
- The SSC malfunction can be determined using the applicable limiting measure tables in Appendix A.

Likelihood Reduction Measure

- A likelihood reduction (LR) measure is a set of defensive measures that when applied as a set, reduce the likelihood of a credible CCF. For example, for a design defect:
  - A structured design process is applied, thereby supporting a much lower expectation of a design defect than the expectation of a random hardware failure, and
  - There is sufficient independence or segmentation to prevent a failure caused by the design defect from propagating to multiple plant components or functions, or occurring concurrently in multiple independent digital devices
- An LR measure allows the CCF to be considered beyond design basis, and thereby allows the use of best estimate analysis methods and acceptance criteria for the analysis of the CCF malfunction result.

Questions/Comments?