Industry Perspective on CCF Technical and Regulatory Positions

John Connelly

Engineering Manager-Capital Projects, Exelon

Chairman-NEI Technical Issues Focus Group

Public Meeting to Discuss the NRC Effort to Re-Evaluate its Position on SCCF

MARCH 21, 2016

NRC and Industry Technical Positions

NRC Position	Industry Position	Gap
CCF is a unique problem caused by software in digital systems	The CCF issue is about malfunctions of multiple controlled SSCs that can be caused by any one of four I&C failure categories, and the likelihood of CCF of multiple SSCs can be made very low for each category	NRC policy on software CCF does not recognize positive operating experience, and puts it out of the full context of malfunctions of controlled SSCs due to other I&C failure categories
Guidance states that 100% testing or equipment diversity are the only measures that can render a software CCF non-credible	100% testing can reduce the likelihood of software CCF in only the simplest devices	NRC policy on 100% testing is not a success path for many protection and control system projects
	Other measures are available that are as good as or better than equipment diversity.	NRC policy on equipment diversity is onerous and costly for many protection system projects, and is not a success path for control system projects
Unless 100% testing or equipment diversity are applied, a software CCF must be assumed and a coping analysis is required	Research and experience show that the likelihood of a malfunction of multiple controlled SSCs (i.e., a CCF) due to a software design defect can be made as low as other sources of CCF that are not considered in plant safety analyses (e.g., multiple hardware failures, human errors, errors in requirements)	NRC policy on assumption of software CCF predetermines the outcome of CCF susceptibility analysis regardless of design and quality attributes that are available for many protection and control system projects

Industry Concerns*

- Industry needs to reach agreement with NRC on deterministic defensive measures that facilitate reaching a CCF unlikely conclusion
  - NRC Position: For design defects in safety systems, 100% testing or equipment diversity. For control systems, there is no written policy.
  - Industry Position: For all systems there are other defensive measures that can reduce the likelihood of CCF due to a design defect to a level that can be considered beyond design basis. There are additional defensive measures that can further reduce the CCF likelihood to a level that precludes the need for consideration in deterministic safety analysis.
- Industry needs to reach agreement with NRC on efficient methods to demonstrate that CCFs are bounded by other previously analyzed accidents
  - NRC Position: No clear policy on how to demonstrate bounding in terms of a previously analyzed accident.
  - Industry Position: For all systems the plant level result of a CCF caused by a design defect is evaluated using best estimate methods; bounding is based on any previously analyzed AOO or PA.

*Reference: NEI Letter dated 2/26/16