March 13, 2017

Staff Comments on NEI 16-16 [Draft 1], "Guidance for Addressing Digital Common Cause Failure"

The staff has reviewed Nuclear Energy Institute (NEI) 16-16 [Draft 1] "Guidance for Addressing Digital Common Cause Failure (CCF)" which was submitted in December 2016 and made public in February 2017 [Agencywide Document Access and Management System (ADAMS) Accession Number ML17033B139]. The staff understands that this draft is considered a "work in progress" by NEI and that it will be submitted with a request for endorsement in the future. The enclosed comments are provided solely on the contents of the as-written document. Staff feedback on this draft is intended to clarify what the staff needs to review and determine if the final NEI 16-16 can be fully or partially endorsed.

In general, the approach and process presented in this preliminary draft guidance is acceptable for addressing digital system CCF concerns with methods that extend beyond diversity and 100% testing. In its current form, NEI 16-16 does not provide sufficient technical basis (i.e., justifications) or the technical basis is not explicitly identified for key concepts and methods to determine if this guidance will provide reasonable assurance of safety for digital upgrades. Further interactions are needed between NEI and the staff to develop the concepts presented into durable guidance for consideration of digital CCF for digital upgrades or new plant designs. The staff recommends that NEI engage the staff in developing a detailed action plan that specially tackles each of the technical areas and expeditiously reach agreeable resolutions.

Separate from the staff's review of NEI 16-16, additional guidance is being developed by the staff on the continued use of NEI 01-01 with qualitative assessment methodology, to support near-term industry upgrade needs in nuclear power plants. For NEI 16-16, NRC will separately review the new proposed approach to determine whether CCF is "not credible" and whether it is within design basis for all types of digital systems. Relevant technical insights that are derived from the development of the interim guidance will be appropriately considered.

No.	Text Location	NRC Comments	Proposed Action (i.e., addition, deletion or modification)
1	Section 1	This section, as well as elsewhere in the document, considers the occurrence of CCF, which does not fully align with the NRC definition and interpretation of CCF. During the December 2016 meeting NEI and NRC, staff identified the differences on definition of CCF. The meeting summary report summarizes this as: "The NRC staff uses the term to identify an error in software regardless of the consequences of that error. NEI uses the term to identify an error in software that has been triggered to affect multiple instances of the software, and it then focuses attention on the plant effect rather than on the software error itself."	NRC and NEI should discuss and resolve this difference during the upcoming interactions.
2	Section 1.1	This section states "there are only two design attributes that may be credited to eliminate the need for further consideration of CCF: diversity within the digital I&C system, or "testability' based on device simplicity." Will diversity and 100% testing be listed or discussed in Appendix A as "defensive measures" to be considered to address concerns that a CCF may occur? The staff understands that the guidance in this document seeks to expand the use of design attributes and methods beyond diversity and 100% testing.	Consider mentioning that 100% testing and diversity remain viable options for eliminating concerns related to further consideration of CCF in the document.
3	Section 1.1	The introduction states that "This document does not contain risk insights, as risk insights are not credited when addressing these deterministic licensing criteria." Does this statement mean that the process of digital CCF determination is not informed by the plant probabilistic risk analysis (PRA) model? This statement appears to be inconsistent with the concepts presented within the document, which for example states that risk insights are derived by investigating in a systematic manner: 1) what can go wrong, 2) how likely it is, and 3) what the consequences are. This document seems to consider these three questions. Specifically, the document considers how likely it is that a CCF will occur with consideration of sources that lead to a CCF and "defensive measures" that are in place to prevent or limit a CCF.	The staff recommends clarification on how the qualitative assessments proposed in the document can address deterministic licensing criteria. Consistent with Agency policy, the staff is willing to consider the use of risk insights in this document or future revisions.
4	Section 1.2	This section discusses using the likelihood of the CCF to determine the methods and acceptance criteria for addressing CCF. However, this section does not provide a reference to a technical analysis method or deterministic criteria for characterizing and determining the likelihood of a CCF occurring. It is not clear if the likelihood assessment is meant to use the same techniques as a credibility assessment.	Clarify what the methodology or deterministic criteria are for determining the likelihood that a CCF can occur.
5	Section 1.2 Flowchart	The flowchart refers to sections in the document. However, the sections referenced do not seem to correlate to the question or subject identified in the flow chart. For example, in Part 2, question "is a CCF credible" refers to Section 4.1.2.2.1, which discusses Preventive Measures. Section 4.1.2.2.1 does not provide a description/technical analysis of what constitutes "credible."	References should accurately correlate to the correct sections.
6	Section 1.2 Flowchart	The question "Is a CCF Credible?" in the Flowchart of the document is written to be answered in absolute "Yes" or "No" terms.	NRC and NEI should have additional discussions on the question "Is a CCF

No.	Text Location	NRC Comments	Proposed Action (i.e., addition, deletion or modification)
		The process advocated for determining an answer to "Is a CCF Credible?" is not sufficiently articulated for the staff to make an absolute determination.	Credible?" and proposed engineering method to answer the question. The staff recommends that the discussion focus on the level of uncertainty remaining in a digital system to a CCF vulnerability and that independent parties can reach the same conclusion after the proposed engineering method is applied.
7	Section 1.2 Flowchart	During the December 2016 meeting, the staff provided a comment about the question in Part 2 to determine if CCF is beyond design basis. At the time, the staff understood that this document was intended to only address software CCF due to software errors – which is currently considered beyond design basis in SRM-SECY-93-087. During the February 2017 meeting, NEI clarified that NEI 16-16 considers all type of CCF, not only software, and therefore this question was necessary to address CCF resulting from single failures or AOOs (design basis).	The staff recommends that the document be revised to clarify why the question "Is the CCF Beyond Design Basis" is relevant with examples.
8	Section 1.2 Flowchart	Expansion of the process diagram or an additional diagram that specifically outlines how technical results of the CCF analysis support specific sections of the Draft Appendix D to NEI 96-07, with respect to CCF issues, would be helpful. The staff needs this information to determine if endorsement or partial endorsement of the guidance as an acceptable methodology to address CCF concerns for use in Appendix D is possible.	Consider expanding the flow chart to outline how the results support Draft Appendix D to NEI 96-07.
9	Section 2	The definitions provided in these sections are more descriptions and/or approaches than formal definitions of the terms. Some definitions are not consistent with how the terms have been used in regulations and regulatory guidance. Endorsement or partial endorsement would be facilitated if the terms are defined consistently with other regulatory guidance documents or that the terms are consistently used in this document and in any documents that may later refer to it.	Recommend that formal definitions, similar to those recommended by the staff for use with NEI 96-07 Appendix D, be used. See comments 10-14 below for concerns relevant to specific definitions in the draft provided.
10	Section 2.1	The definition for best estimate method in this section implies that relaxed criteria can be used for this method. Rather, best estimate methods use the same acceptance criteria, but apply realistic plant conditions and parameters.	The staff recommends clarification of the definition.
11	Section 2.4	The definition for "CCF Beyond Design Basis" is not clear – the content does not come across as a definition.	SRM-SECY-93-087 states that since CCF is a low likelihood event, it may be considered "beyond design basis" and any analyses of the consequences of the CCF may use "best estimate" methods.
12	Section 2.5	The term "CCF Not Credible" is described as a determination that "the CCF is sufficiently unlikely." It is not clear what "sufficiently unlikely" means.	The staff recommends more detailed discussions between NEI and NRC on the subject, including the proposed graded approach to eliminating the need for further consideration of CCF in safety support systems (such as chillers as have been presented by NEI).

No.	Text Location	NRC Comments	Proposed Action (i.e., addition, deletion or modification)
13	Section 2.8	It is not clear why this guidance needs to define the role of the Digital Engineer.	Consider eliminating the definition of "Digital Engineer."
14	Section 2.9	This section states that a deterministic analysis refers to analyses that do not employ probabilistic or risk informed methods.	Consider the definition provided in NUREG-2122 which states "A characteristic of decision-making in which results from engineering analyses, not involving probabilistic considerations, are used to support a decision." or another definition provided in an NRC document.
15	Section 3.1	This section paraphrases the information in the SRM-SECY-93-087 which may lead to confusion.	The staff recommends that NEI use the exact text from SRM-SECY-93-087 to the extent practical.
16	Section 3.1	This section acknowledges the unique hazards and concerns with digital I&C technology and the reasons for a systematic assessment of CCF. The staff appreciates this discussion as a preface to the discussion of addressing CCF.	The staff believes it may also be beneficial to acknowledge the potential benefits of digital technologies to increase plant reliability and reduce risks associated with the maintenance of obsolete analog systems.
17	Section 3.3	Examples of support systems that result in a "YES" to the question "is the digital equipment an initiator, or credited for event mitigation?" in the flowchart, Part 1 are provided in this section. The staff finds that these examples are useful for clarifying which types of systems result in a "YES" answer.	Consider adding examples that result in a NO answer. Examples would clarify what types of systems result in a "NO" answer.
18	Section 3.4	It appears that this draft guidance is treating 3 possible conditions: (1) "CCF is not credible;" (2) CCF is credible but beyond design basis; or (3) CCF is credible and is within design basis.	The NRC and NEI should further discuss the appropriate characterization of CCF in terms of credibility, design basis, and beyond design basis. Review of the document would be aided by specific examples of digital modifications that could fall with the three categories proposed in the document. The staff's review will be aided by a practical understanding on the implications and use of this methodology.
19	Section 4.1.1	This section states that the digital engineer confirms the applicability of at least one P measure, L measure, or LR measure from Appendix A. If an alternate P, L, or LR measure is credited, the digital engineer is responsible for providing documented justification for each alternate measure. The section, in part, later states that a CCF that is not credible requires no further assessment.	The technical basis provided should be strengthened by additional information that includes design rationale, analyses, data, or operational experience to justify a "credibility" determination.
20	Section 4.1.2.2.2	What is a "preferred malfunction state?"	Define "preferred malfunction state."
21	Section 4.1.2.2.3	The document partially describes the use of "Conservative Methods" and "Best Estimate Methods." The staff's review would be facilitated by incorporating and referencing NRC guidance on acceptable implementation of these methods.	The staff recommends that NEI incorporate or reference NRC guidance on acceptable implementation of conservative and best estimate methods. Otherwise, provide justification for using alternate methods.

No.	Text Location	NRC Comments	Proposed Action (i.e., addition, deletion or modification)
22	Section 4.1.2.2.4	This section states that a "graded approach to defensive measures does not employ risk insights, because regulators have not permitted risk insights to be credited when addressing deterministic licensing criteria."	Consistent with Agency policy, the staff is willing to consider the use of risk insight in this document or future revisions.
23	Section 4.2	This section does not describe how to perform an analysis of the CCF malfunction.	The staff recommends adding a description on what constitutes an analysis of the CCF malfunction, methods, and acceptance criteria.