UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

January 25, 2021

MEMORANDUM TO: Jeanne Johnston, Chief
Long Term Operations and Modernization Branch
Division of Engineering and External Hazards
Office of Nuclear Reactor Regulation

FROM: Tekia V. Govan, Project Manager **/RA/**
Reactor Assessment Branch
Division of Reactor Oversight
Office of Nuclear Reactor Regulation

SUBJECT: SUMMARY OF THE PUBLIC MEETING TO DISCUSS THE NUCLEAR ENERGY INSTITUTE'S PRE-SUBMITTAL OF NEI 20-07, DRAFT B, HELD ON JANUARY 12, 2021

On January 12, 2021, the U.S. Nuclear Regulatory Commission (NRC) staff held a meeting with the Nuclear Energy Institute (NEI) to discuss pre-submittal activities for NEI 20-07, Draft B, "Guidance for Addressing Software Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML20245E561). NEI has requested staff engagement on this guidance document prior to submitting a request for formal NRC endorsement.

Prior to this meeting, a member of the public submitted to the NRC staff written comment on the public version of draft NEI 20-07 (ADAMS Accession No. ML20351A249). The staff reviewed draft NEI 20-07 as well as the submitted comment in preparation for this meeting and developed clarification questions/comments for NEI's consideration.

Meeting Summary

NEI began the meeting with a presentation that provided an overview of the guidance in NEI 20-07, Draft B (ADAMS Accession No. ML21006A006). Based on the staff's review of this document prior to this meeting, the comments below represent what the staff considers "major" comments regarding NEI 20-07, Draft B. The staff defines major comments as comments that require resolution prior to completion of the pre-submittal period which ends December 2021. These comments are requested to be resolved prior to the request for staff's review of NEI 20-07 for NRC endorsement.

CONTACT: Tekia V. Govan, NRR/DRO
(301) 415-6197

NRC Staff's Question/Comments – NEI 20-07

1. **Assessing CCF Vulnerabilities**

a. Does the methodology described in draft NEI 20-07 require an assessment of potential common cause failure (CCF) vulnerabilities in a proposed system, prior to implementation of this methodology?

b. How does the prescribed methodology in draft NEI 20-07 protect against potential CCF vulnerabilities in a generic sense, when different systems may have unique characteristics such as different platforms, application software, architectures, etc.?

2. Executive Summary Comment – Alignment with Related Guidance

Draft NEI 20-07 appears to leverage a 'frequency' argument to resolve CCF considerations in a similar manner to RIS 2002-22, Supplement 1, but for HSSSR systems. RIS 2002-22, Supplement 1, allows for frequency (i.e. likelihood) arguments because it is focused on lower safety significant systems whose failure consequences of CCF is well understood and acceptable.

It's not clear how the approach in draft NEI 20-07 is consistent with RIS 2002-22, Supplement 1 or BTP 7-19, Revision 8, SRM to SECY 93-087 as well as SECY 18-0090 with regard to using a frequency argument to remove CCF from further consideration, but for an HSSSR system.

a. NEI should be prepared to address this potential misalignment.

b. Is it NEI's position that any CCF of a HSSSR has **severe** consequences and that the approach in NEI 20-07 is attempting to justify the safety system design through a very low likelihood of occurrence of software CCF?

3. Executive Summary Comment – Current Processes versus NEI 20-07

The Executive Summary states the following:

> *This approach begins by establishing a set of first principles for the protection against software CCF in digital instrumentation and control (DI&C) systems and then subsequently decomposing these first principles into safety design objectives (SDOs).*

a. Is it NEI's position that existing, endorsed IEEE standards (e.g. IEEE Std. 1012, IEEE Std. 7-4.3.2) have a potential gap that the methodology of NEI 20-07 is addressing? This statement seems to presume that SDO concept are unique to IEC 61508.

b. Is it NEI's position that the methodology described in NEI 20-07, when used in conjunction with the currently endorsed standards, can provide a lower likelihood of software CCF in HSSSRs than current processes alone?

The present regulatory infrastructure for HSSSR systems acknowledges that it is possible to identify a potential CCF vulnerability due to a latent defect has such a low likelihood of occurrence that it may be treated as "beyond design basis", and therefore its consequences may be evaluated using best-estimate methods. The use of best-estimate methods was

intended to be less burdensome for licensees and applicants than typical reactor safety thermal-hydraulic analysis methods. The consequences of very low likelihood of occurrence of CCFs due to latent defects still need to be evaluated to demonstrate reactor safety objectives and regulatory dose acceptance criteria limits are being met. As currently written, NEI 20-07 seems to suggest otherwise.

4. Executive Summary Comment – EPRI Research

EPRI research appears heavily leveraged in this document. The staff would need to understand more details on this research and its applicability and technical assumptions as it pertains to addressing CCF in nuclear applications, types of devices/components considered, software applications, etc., and how they're organized/configured. This is to ensure we have relevant comparison of data. For example, with regard to 1.6 billion operating hours, how much of that data is valid with respects to the components, systems, operating system platforms, etc. that are currently in use?

5. Executive Summary Comment – IEC 61508

The Executive Summary states the following:

> *Based on this research, it can be reasonably concluded that use of the guidance in IEC 61508 when developing platform software and extrapolating to application software will result in reasonable assurance that a latent software defect will not lead to a software CCF.*

a. Is it NEI's position that implementation of IEC 61508 in an adequate manner is sufficient to render SWCCF not credible (sufficiently low for platforms, not applications)? What about the application software?

b. Standards are generally written to be followed in totality to achieve the stated goals within. In the context of NEI 20-07, is IEC 61508 being utilized in its entirety or are only certain portions of IEC 61508 being utilized? If only partially, what is that scope?

c. The methodology in NEI 20-07 appears to be a process that uses aspects of IEC 61508 without necessarily requiring the platform/application software to be compliant with IEC 61508. Is that the approach being taken by NEI 20-07? (Note: IEC 61508 is not a nuclear standard but an industrial standard. IEC 61513 is a nuclear though and it's not clear why this standard was not used).

6. Executive Summary Comment – Applicability to 10 CFR 50.59

The Executive Summary states, in part, the following:

> *Although this guidance can be used for digital upgraded implemented under 10 CFR 50.59….*

a. Is it the intention of this document to provide methodologies that are consistent with the guidance of RIS 2002-22 Supplement 1 and its definition of sufficiently low) and requirements under 10 CFR 50.59?

b. How does NEI envision this document being used under 10 CFR 50.59?

c. Is this document consistent with NEI 96-07, Appendix D? Does the document identify residual gaps between it and technical guidance that complements NEI 96-07, Appendix D?

7. Introduction Section Comment – Software Development Process

NEI 20-07 states the following in the "Introduction" section:

> *This document focuses on systematic failures due to a latent defect in software, and an approach to providing reasonable assurance through a quality software development process that the common cause systematic failure of an application is adequately addressed.*

NRC staff already requires rigorous software development process (e.g. BTP 7-14) and has previously determined that a high-quality software development process is sufficient to consider software CCF a beyond design basis event, but not necessarily sufficient to eliminate the potential for CCF. NEI should describe how the methodology in NEI 20-07 is sufficiently different than current processes such that potential software CCF consideration can be eliminated.

8. Background Section Comment – Additional Analysis

The "Background" section of NEI 20-07 states the following:

> *This document provides an approach to adequately address software CCF HSSSR systems.*

a. Is it NEI's position that there is no evaluation/analysis needed if this document is implemented?

b. Is there any sort of evaluation/analysis this document points to that is performed to highlight potential CCF vulnerabilities?

Some analysis of the design (architecture) beyond the "software" seems implied by SDOs relating to 6.3's 1st principle. For example, 10.1.3.2 through 10.1.3.5. 10.1.3.2 identifies constraints derived from hazardous control actions, which may imply something that enforces the constraint that is not the application software itself. 10.1.3.4 identifies "hardware constraints." 10.1.3.5 identifies "constraints imposed by the I&C system design."

9. Section 5 Comment – SRM to SECY 93-087 and Scope

General Comment on Section 5 titled, "NRC Regulatory Framework Versus Implementation Level Activities to Address Software CCF"

NEI 20-07 addresses several regulatory criteria but does not address SRM to SECY 93-087, for which BTP 7-19, Revision 8, is the implementable guidance of.

a. It's not clear how NEI 20-07 maps to SRM to SECY 93-087 and why SRM to SECY 93-087 is not referenced.

b. BTP 7-19, Revision 8, includes sources of digital CCF to be both software and hardware, consistent with SRM to SECY 93-087. Is it NEI's position that NEI 20-07 provides adequate coverage with respect to the scope of CCF considerations in BTP 7-19, Revision 8?

10. Section 5 Comments – Gaps in Current Regulatory Processes

Section 5 of NEI 20-07 states the following:

> *NEI 20-07 is intended to **fill the gap** between the NRC regulatory framework and implementation level activities associated with development of HSSSR software.*

Is the approach of this document to "fill the gap" that is perceived within current NRC processes (e.g. BTP 7-14) or is it attempting to be complimentary to current processes, or both? Industry has not formally communicated of such a gap to the NRC. Industry has previously expressed concerns with the level of effort with current NRC practices and NEI 20-07 would appear to add an additional layer of complexity to licensing and design work.

11. General Comments on Section 6, titled "First Principles of Protection Against Software CCF"

a. The principles listed in this section have a description (with the subsection headers themselves acting as the principle itself) but do not appear to have guidance. It's not clear how a licensee or application can apply them without specified acceptance criteria or similar type of consideration.

b. Without specified acceptance criteria, it's not clear how a licensee or applicant can adequately determine whether the stated goals of this document (i.e. sufficiently low finding with regard to software CCF) has been achieved.

12. General Comments on Acceptance Criteria

a. Does draft NEI 20-07 describe/provide general acceptance criteria for all portions of the methodology that are used to ultimately make a determination of "sufficiently low" with regard to the likelihood of software CCF?

b. Does draft NEI 20-07 address relevant acceptance criteria in BTP 7-19, Revision 8, including Section 3.1.3?

13. Section 6 Comment

Section 6 of the document states the following:

> *The first principles listed in this section are considered bounding and complete and represent the starting point for decomposition of SDOs.*

a. Clarify what is the basis for stating that the first principles in Section 6 is both "bounding" and "complete". On the surface, with regard to software development, there would appear to be more considerations than what's currently listed.

b. What is meant by the term "bounding"? Bounding with current regulations?

14. Section 6 Comment

Section 6 of the document states the following:

> *The first principles of protection against software CCF will be achieved by executing the SDOs.*

The principles listed in this section are generally understood to be identified/covered within existing IEEE standards the NRC staff has already endorsed and the subsections in Section 6 are silent in this respect. Is it NEI's position that existing, endorsed IEEE standards (e.g. IEEE Std. 1012, IEEE Std. 7-4.3.2) have a potential gaps that the methodology of NEI 20-07 is addressing?

15. Section 9 Comment

Section 9.1 of the document states the following, in part:

> *Use of IEC 61508 as a source for developing SDOs to protect against software CCF…*

Does NEI intend to include the relevant portions of IEC 61508 as part of this review or does NEI believe that NEI 20-07 has sufficient information contained therein to facilitate the staff's review?

16. Software Quality Assurance Argument of NEI 20-07 (B.1 Figure)

RIS 2002-22 Supplement 1, describes the qualitative assessment concept where the aggregate of considerations of deterministic design features, software quality and operating experience can be used to make a sufficiently low determination. The RIS supplement is clear that operating experience alone cannot be used as a sole basis for a sufficiently low determination and isn't truly a substitute for the two other aspects. NEI 20-07 Section 6.4, 9.1.2 and other sections would appear to make the case that a focus on software quality and supplemental operating history (presumably of the exact same software package) alone are sufficient to demonstrate a sufficiently low likelihood of failure of an entire HSSSR system. This appears to be the case in lieu of additional consideration of architectural design or deterministic design features (e.g. defensive measures) that can also demonstrate high reliability/dependability. This would not appear consistent with either the RIS supplement 1 or BTP 7-19, Revision 8, which both provide for reliance on these aspects to demonstrate system reliability/dependability to the effects of a digital CCF (hardware or software) or to prevent its occurrence, in addition to software quality.

a. Is it NEI's position that software quality and operating experience (presumably of the same software package) alone, is sufficient to demonstrate a sufficiently low likelihood of failure for an entire system?

b. Are there any aspects of the methodology of NEI 20-07 that focus on architectural design and/or design features to also demonstrate high reliability/dependability?

Comments from a Member of the Public

After the staff's discussion with NEI, a member of the public presented an overview of the comments he submitted to the NRC staff on draft NEI 20-07 (ADAMS Accession No. ML21008A094). The staff will consider these comments as they continue their review of pre-application activities for draft NEI 20-07.

Next Steps

The staff discussed the following next steps with meeting participants:

- NEI can begin to review the major staff comments, while the NRC staff develops its final set of comments.

- The next public meeting to discuss the complete set of NRC staff comments on draft NEI 20-07 is expected to take place the between the end of February and early March 2021.

Conclusion

At the end of the meeting, NRC and industry management gave closing remarks. NEI and members of the public expressed appreciation for the open dialogue.

The enclosure provides the attendance list for this meeting.

Enclosure:
As stated

SUBJECT: SUMMARY OF THE PUBLIC MEETING TO DISCUSS THE NUCLEAR ENERGY INSTITUTE'S PRE-SUBMITTAL OF NEI 20-07, DRAFT B, HELD ON JANUARY 12, 2021

DISTRIBUTION:
RidsRgn1MailCenter
RidsRgn2MailCenter
RidsRgn3MailCenter
RidsRgn4MailCenter
RidsNrrDro
RidsNrrDex
RidsResDe
RidsNRR
RidsOgcMailCenter

ADAMS Accession No.: ML21025A392 *via e-mail

OFFICE	NRR/DEX/ELTB/TR	NRR/DEX/ELTB	NRR/DRO/IRSB/PM
NAME	WMorton*	JJohnston*	TGovan*
DATE	01/21/2021	01/25/2021	01/25/2021

OFFICIAL RECORD COPY

LIST OF ATTENDEES

PUBLIC MEETING TO DISCUSS THE NUCLEAR ENERGY INSTITUTE'S PRE-SUBMITTAL OF NEI 20-07, DRAFT B

January 12, 2021 1:00 PM to 4:00 PM

Teleconference

ATTENDEE	ORGANIZATION
1. Eric Benner	NRC
2. Wendell Morton	NRC
3. Tekia Govan	NRC
4. Maxine Segarnick	NRC
5. Bob Weisman	NRC
6. Rossnyev Alvarado	NRC
7. David Rahn	NRC
8. Jeanne Johnston	NRC
9. Sheldon Clark	NRC
10. Mike Waters	NRC
11. Ismael Garcia	NRC
12. Steven Arndt	NRC
13. Norbert Carte	NRC
14. Steve Vaughn	NEI
15. Jana Bergman	Curtiss-Wright
16. Neil Archambo	Duke Energy
17. Steve Geier	NEI
18. Warren Odess-Gillett	Westinghouse/NEI
19. Mark Burzynski	New Clear Day
20. Ken Scarola	Nuclear Automation Engineering
21. Paul Phelps	Dominion Energy
22. Jeremy Chenkovich	Dominion Energy
23. Ron Jarrett	NEI
24. Brian Haynes	Unknown
25. David Hooten	Sargent and Lundy
26. Mike Wiwel	PSEG Nuclear LLC
27. David Sehi	Unknown
28. Lou Gaussa	Westinghouse
29. Pareez Golub	Unknown
30. Guy Wilkerson	Entergy
31. Cory Carmin	Unknown
32. John Schrage	Entergy
33. John Connelly	Exelon
34. Bernie Dittman	NRC
35. David Herrell	MPR
36. Joseph Carman	Unknown
37. Ty Rogers	GE Hitachi Nuclear Energy
38. Matthew Armstrong	Unknown
39. Jo Jacobs	NRC
40. Matt Gibson	Unknown
41. Ted Quinn	Unknown

Enclosure

42. Jay Boardman	PWROG
43. Charles Mohr	Unknown
44. Raymond Herb	Southern Nuclear
45. Robert Armistead	Member of the Public
46. Richard Supler	Enercon
47. Sushil Birla	NRC
48. Anthony Masters	NRC
49. William Catullo	NRC
50. Alan Able	Cooper Nuclear Stations
51. Larry Nicholson	Unknown
52. Dan C.	Unknown
53. Bob Hirmanpour	Unknown
54. Rob Austin	Unknown
55. Eugene Keller	NRC
56. Steve Erickson	Enercon
57. Jason Remer	Idaho National Lab