



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

August 17, 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, HELD ON
JULY 1, 2021

On July 1, 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, "Guidance for Addressing Software Common Cause Failure in High Safety-Significant Safety-Related Digital I&C Systems." NEI has requested staff engagement on this guidance document prior to submitting a request for formal NRC endorsement.

Meeting Summary

During this meeting, NEI presented their proposal for a Draft D to NEI 20-07 (Agencywide Documents Access and Management System (ADAMS) Accession No. ML21173A286). This presentation discussed the restructuring of NEI 20-07 to include a risk informed approach to address Common Cause Failure (CCF); the proposed approach would be an alternative method as allowed by BTP 7-19, Revision 8 Section 3.1.3. In preparation for this meeting, the NRC staff developed advanced questions and comments, based on the presentation, for discussion with NEI during the meeting (ADAMS Accession No. ML21181A280). Below are the staff's notes from this meeting as a result of the discussion with NEI during this meeting. The questions/comments below with an asterisk (*) represent the highest priority for the staff's review of this pre-submittal guidance document.

POLICY CONSIDERATIONS – SRM to SECY 93-087 and BTP 7-19, Rev. 8. B.3.1.3

1. *What is NEI's position on the consistency of the new approach with SRM to SECY 93-087?
 - NEI stated they understand that the new approach is not going to be fully consistent with the current CCF policy (NEI believes the new approach will address Position 1 of SRM

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

to SECY 93-087 Item II.Q) and is not being developed as such. In particular, the new risk informed approach will not have a specific focus on the D3 assessment concept but is still intended to address the guidance of Section B3.1.3 of BTP 7-19 Revision 8 as an alternative approach to addressing CCF. NEI also clarified that the new risk informed approach should be considered a separate/alternative approach to performing a D3 assessment.

- The new risk informed approach now focuses on the entire system architecture.
- NEI clarified that PRA models and/or risk information would be used to develop a bounding consequence analysis in the form of a risk reduction objective (RRO). Control measures and other design features of the system would be linked to meeting an RRO.
- Determining hazards and control actions and what are the loss scenarios and what are the effective system control measures.
- Diversity can be a control measure; therefore, it is not off the table even though the new approach will not focus on diversity.
- Technical basis of new approach includes supporting research from the Massachusetts Institute of Technology (MIT) and Electrical Power Research Institute (EPRI). According to the NEI, the research cited will demonstrate the effectiveness of hazard analysis techniques (e.g. System Theoretic Process Analysis (STPA)) for assessing hazards in DI&C systems.
- Staff noted that, similar to previous conversations on supporting research and other supporting technical details on the new process, there should be a sufficient level of detail for all of these new aspects described within the next revision to NEI 20-07 to facilitate the review. Otherwise, the review may not be efficient and timely.
- NEI clarified the upcoming Draft D, the next revision to NEI 20-07 will supersede and replace Draft B and Draft C content in totality

2. *Does the proposed approach allow the most safety significant systems (HSSSRs, e.g. RPS and ESFAS) to have the modeled risks reduced to a value such that a consequence-based analysis (D3) need not be performed (i.e., risk has been lowered to be considered non-risk significant)?

Partially covered by Question #1 discussion. Staff will follow up upon receipt of NEI 20-07, Draft D.

3. *Does the proposed approach allow implementation of digital I&C for safety significant systems (i.e. HSSSRs such as RPS and ESFAS) without the application of any diversity (or any specific types of diversity)?

Partially covered by Question #1 discussion. Staff will follow up upon receipt of NEI 20-07, Draft D.

4. Will NEI 20-07 draft D contain the technical basis for its approach including but not limited to efficacy of control method(s) in addressing a vulnerability, validity of scoring each method as achieving a corresponding risk-reduction, and validity of accumulation of scored methods to achieve commensurate risk-reduction to the objective?

NEI stated that of NEI 20-07, Draft D, will include the technical justification for the scoring methodology.

5. Will the technical basis be demonstrated as addressing CCF concerns, such as: 1) sharing of resources or identical designs among redundant elements, combining RPS and ESFAS functions, independence between layers or echelons of defense?

Staff will follow up on this question upon receipt of NEI 20-07, Draft D.

6. Will NEI 20-07 draft D contain acceptance criteria associated with its approach?

NEI stated that of NEI 20-07, Draft D, will have acceptance criteria for the scoring aspects. The risk reduction objectives (RROs) are strictly informative and not necessarily a pass/fail.

PRA Questions

7. *The approach appears to perform a bounding consequence analysis for the risk significance of CCF failure. However, RG 1.174 provides guidance for integrated decision-making and not just the acceptance guidelines. Is the proposed approach consistent with the five principles of risk-informed decision-making in RG 1.174? If not, what is the delta between NEI 20-07 and the guidance of RG 1.174?

NEI stated that NEI 20-07, Draft D, will use the acceptance guidelines in RG 1.174 to establish the technical rigor of the control measures. NEI provided the following responses to the five principles during the meeting:

- Principle 1: Current Regulations Met – Is not challenged as it is the expectation of the LAR.
- Principle 2: Consistency with Defense in Depth Philosophy – The new process verifies that the modified system still maintains the overall defense in depth of the plant, as defined in NUREG 6303.
- Principle 3: Maintenance of Safety Margin –It is not expected for a potential LAR incorporating NEI 20-07, Draft D to challenge the safety margins.
- Principle 4. Acceptable Increase in Risk – NEI will follow up later on this point.
- Principle 5. Performance Monitoring – NEI will follow up later on this point after discussions with their PRA experts.

During this discussion to better understand the new process relative to RG 1.174, staff inquired as to whether risk information is used to determine loss scenarios. NEI responded that loss scenarios are not quantitative, but qualitative and this would be clear in Draft D.

8. *Given the complexity of the topic, and the unique application of this methodology, a white paper or an early draft of the revision that provides sufficient detail of the approach will be beneficial to inform the staff's internal discussions and ensure staff's resources are properly allocated to continue to facilitate an efficient review. **An example of a digital modification using the proposed new approach is highly recommended in the white paper or early draft.** This is especially important considering the revised product is not projected to be delivered until later this year.

NEI will follow up with staff at a later time on this point although NEI supported developing standalone examples that demonstrate how the new process works in all phases as well as the technical basis that supports the process. Staff reiterated that providing examples of the new process is considered essential in facilitating the review in a timely and efficient manner. Staff also reiterated that the examples should exercise

each aspect of the process including how the example scenario would be submitted as a LAR.

9. Slide 7 – What PRA models (e.g., internal events only or internal events and internal fire) are expected to be utilized for the bounding analysis? What provisions for PRA technical acceptability are part of the proposed approach?

NEI will follow up with staff at a later time on this point. Staff expects to this question to be addressed in NEI 20-07, Draft D.

10. *Slide 7 – How will the bounding analysis be performed if the design functions in HSSSR systems that are not included in the PRA models? Will the bounding analysis for a digital I&C system that performs multiple design functions (e.g., RPS and ESFAS) consider combined failure of both functions or only one at a time?

According to NEI, If the HSSSR system performs both RPS/ESFAS functions, the analysis would assume they both fail. NEI also stated that there are paths forward to include systems that are not modeled in a PRA, but details were not provided during the meeting. Staff noted that Draft D should very clearly describe these potential paths forward.

11. *How will key assumptions and sources of uncertainty in the PRA models that can impact the bounding assessment be addressed in the proposed approach?

NEI stated that this is consideration will be covered by the follow up action for Item #10 above that there are other avenues to account for systems not modeled under PRA.

STPA Questions

12. *Is it NEI's intent that staff would need to include endorsement of STPA as used within the NEI 20-07 process? Or does NEI expect the NRC staff to include an application specific action items for the applicant to demonstrate that the "systematic hazards analysis based on STPA" is adequate? The STPA process appears to be a foundational aspect of the technical processes of NEI 20-07. This comment can be extended to other referenced documents that appear to provide foundational technical content.

NEI clarified that the new process will be described in the NEI 20-07 with sufficient detail to allow use of STPA but NEI will work with staff on the level of detail needed in NEI 20-07. In other words, the key consideration would be how much information is needed to facilitate approval of a LAR that cites NEI 20-07. NRC Management also highlighted that there are a number of ways to endorse or approve the STPA aspect, but eventually we do need resolution on level of detail needed to approve a LAR.

13. Has NEI received any industry/licensee feedback on the use of the STPA approach and its efficacy for important-to-safety applications?

NEI referred to the NuScale application for use of STPA as an example of industry support for STPA.

14. *Is STPA, or similar method based upon it, going to be described in full detail in NEI 20-07? If not, why not? This includes providing definitions of terms unique to STPA such as “unsafe control actions”.

- a. In lieu of constraining the users of the NEI 20-07 guidance to STPA, did NEI consider the option of developing guidance that is independent of the HA methodology? As discussed in EPRI 3002000509, there are several HA methods, including STPA, that users can choose from in support of the analysis.
- b. Is it NEI’s intent that NEI 20-07 will allow flexibility for use of different HA methodologies (i.e. HA methods that are NOT STPA)?

NEI stated that the new approach will be focused on STPA. NEI also stated that a licensee on their own, would have to demonstrate an equivalency for a different HA if the licensee chooses NOT to use STPA.

SCOPE AND APPLICABILITY

15. *The presentation describes things that are not currently in NEI 20-07 draft C. Is this new material intended to augment and supplement the current material, or will some of the current material be removed or replaced with Draft D?

NEI confirmed that NEI 20-07, Draft D, will be a new process and will not include or leverage any of the previous draft’s content. This includes no longer citing the draft C supporting EPRI research.

Staff informed NEI that if the new MIT and EPRI research on the use of PRA will be used to support the technical basis of NEI 20-07, our previous comments regarding technical justification of cited research in previous drafts of NEI 20-07 remain valid and should continue to be considered. NEI would need to describe the technical justification in significant amount of detail to support the claims.

Staff provided additional feedback that even though a number of our previous comments may no longer be valid, many of the underlying themes still are valid and that NEI should ensure the previous staff comments have been reviewed to verify they are incorporated into NEI 20-07, Draft D. This will ensure a more efficient review. Otherwise we’ll be going back to them again with similar comments.

16. Is NEI 20-07, Draft D, going to leverage content from Draft C, as in, is draft D adding to what’s in draft C, or is it a complete replacement of that content. Does this presentation include the entirety of Draft D scope and dropping everything else (e.g. SIL3 certification information, EPRI research)?

NEI stated that NEI 20-07, Draft C, content would be fully replaced by upcoming Draft D.

17. *What exactly is the scope of the NEI 20-07 now? Is its applicability limited to HSSSRs (as Rev C was)? Does it include platform hardware/software and application software? Are the systematic CCFs being addressed limited to those associated with platform hardware/software and application software? Are the references (e.g. STPA, IEC 61508-1) included within the scope of the document?

NEI verified that the new scope of NEI 20-07 will include the entire system architecture. The process itself will include any interfaces or interconnectivities to other systems, such as the architectures of APR1400 and AP1000 and their various interfaces and interconnections would be covered by the new process.

18. *The slides do not clarify how the proposed approach will be used by licensees. Is NEI's intent and expectation that the proposed approach will be used by licensees for making changes to I&C systems under 10 CFR 50.90? Can licensee's use the approach in conjunction with 10 CFR 50.59? Please clarify the expectations consistent with existing regulations for which digital modifications will take place.

NEI verified that this process will not be applicable to 50.59 modifications. Staff will follow up on this question upon receipt of NEI 20-07, Draft D, to ensure this point clearly described.

HAZARDS ANALYSIS (HA) SCOPE

19. In what form, manner or degree of detail will information from applying the approach, including hazard analysis (HA), be provided for regulatory review?

Staff will follow up on level of detail for how HA is described in NEI 20-07. NEI confirmed that NEI 20-0,7 Draft D, would have sufficient detail to be a standalone document.

20. What is the scope of the hazards to be analyzed (e.g., limited to design to exclude operations and maintenance, inclusive or exclusive of safety hazards related to cyber security, inclusive or exclusive of hardware failure cascading effects or error propagation)?

NEI clarified that STPA credits looking at cybersecurity hazards as well. Staff stated that NEI should ensure that, if this is the case, NEI 20-07 should distinguish between control of access (RG 1.152) and Cyber (RG 5.71).

21. What is the scope of the HSSSR that will be subject to HA (i.e., does it include plant process components, all interfaces including with operators and its environment, or digital communications)?

NEI stated the new process covers all interfaces as well.

22. Is the scope focused on or limited to addressing systematic CCF of "platform hardware/software and application software" (as NEI 20-07, draft C was)?

NEI confirmed that the new process includes the entire system architecture.

23. Considering that the EPRI's Digital Engineering Guide already provides guidance for using HA methods and PRA for designing, implementing, testing, installing or operating and maintaining digital I&C system or component applications in commercial nuclear power facilities, how does the proposed NEI 20-07 Rev. D supplement or complement this EPRI guidance?

This question was tabled for the next engagement between NEI and NRC staff.

24. Are there any particular “systematic control methods” envisioned at this time (e.g., per Appendix A of EPRI TR-1025278 dated July 2012)?

NEI confirmed that the next draft of NEI 20-07 will not specifically list control methods. Staff stated that future examples developed by NEI should demonstrate how a control measure is traced within a LAR such that a staff reviewer can trace a control method to a specific design feature or software requirement.

Staff also inquired as to how sacrosanct are these control measures such that it would be an issue if control measures were altered by future changes to a particular system, such as changes performed under 10 CFR 50.59? How much flexibility is there and is this flexibility for an ‘acceptable’ level of changes, but maintaining the sanctity of the NEI 20-07 finding described in the document? Staff did not receive a specific response to this question. This will be a follow up question posed to NEI upon receipt of NEI 20-07, Draft D.

25. What is the relationship between different potential “systematic control methods”, the proposed scoring approach, and the RRO that need to be achieved (i.e., what score needs to be achieved for a particular RRO and/or what types of control methods are recommended for each RRO)?

Staff will follow up on this question upon receipt of NEI 20-07, Draft D.

26. Provide additional details on the scoring approach including the justification for the logarithm scoring and how the score for each “systematic control method” will be assigned.

Staff indicated that this is a significant point as to whether the scoring method will be defined and described in the next revision of NEI 20-07. The staff understands that the scoring method is an essential part of the process and highly encourage NEI to define and describe the methodology in the next revision. NEI stated that the scoring is predetermined but did not commit as to whether the scoring system itself would be defined. This will be a follow up question for staff upon receipt of NEI 20-07, Draft D.

Staff also raised the point that for the upper regions of the RRO bands, as shown in the presentation, it will be a significant challenge to demonstrate that the qualitative (subjective) approach to control measures is sufficient to justify not doing a D3 analysis or to not have diversity instantiated within. Staff provided additional emphasis by stating staff understood the qualitative approach for lower safety significant systems, but it's a higher threshold for HSSSR. This will be a follow up item for the next engagement.

27. *It appears that the scoring approach will be subjective and possibly licensee dependent, both of which can lead to review complications. Has consideration been provided to a focused evaluation of the dominant risk contributors from the bounding analysis in addition to the “systematic control measures?” Such an evaluation can identify the contributors with a

30 minutes coping time without operator actions and investigate the initiating frequency as well as mitigation features for the remainder.

NEI stated that this question will be covered by some aspects of the question #27. Staff will follow up on this question upon receipt of NEI 20-07, Draft D.

HAZARDS ANALYSIS (HA) APPROACH

Staff will follow up on these unanswered questions once NEI 20-07, Draft D is provided for staff's review.

28. Will the HA include all interactions between the system being analyzed and all entities with which it can interact?
29. Will the HA be performed at every level of system integration (composition and decomposition) including all possible interactions of each element with other elements?
30. Will the HA be performed at every phase in the development cycle (e.g., as indicated in IEEE Standard 1012)?
31. As the design changes from that submitted for regulatory review to the final version representing the "as built" system, how will change impact analysis be performed and controlled in consideration of the HA?
32. How will completeness and correctness of HA be assured?
33. How will IV&V be performed on the HA (for example: 1) performed by the developer, 2) independent party performs as a confirmatory HA, or 3) independent party reviews the developer's HA)?
34. What HA-related roles and relationships exist among the developers, IV&V agents, and safety engineering groups? Is human diversity planned to exist across these roles?
35. How will adequacy of competence be assured in each of these roles (e.g., competence criteria, an examination/certification process, use of a certifying authority, other like factors identified in 10CFR50 Appendix B)?
36. How will it be assured that the "as built" system is the same as the one on which HA was performed and subject to regulatory review?

SPECIFIC PRESENTATION QUESTIONS

Staff will follow up on unanswered questions once NEI 20-07, Draft D is provided for staff's review.

37. Slide 7 – Would you clarify whether the baseline assessment here that establishes the reference CDF (x-axis) is the pre-modified system and whether the delta CDF (y-axis) is either the pre-mod or post-mod system? Does a post-mod system have to include additional control methods to reduce CDF/LERF impact of an actual complete HSSSR system failure (post-mod)? Or is it just a hypothetical complete HSSSR system failure of the pre-mod system that is being used to establish a level of safety significance from which to derive a risk-reduction objective?
38. Slide 8 – What is the target risk to get to "sufficient effectiveness" as described on slide 9?

NEI stated that it chose to use the term “commensurate with...” instead of “sufficient effectiveness” going forward.

39. Slide 9 – What level of detail does NEI go to within its STPA-based process? Does it capture complex interactions between all levels of systems/components?

Based on Figure 14, NEI stated that it can provide control methods at the software level or the architecture level, which presumably, covers various interactions. It depends on the design. Staff will follow up on this question upon receipt of NEI 20-07, Draft D.

40. Slide 16 – What is a “systematic control method” that is used to **eliminate** or mitigate a loss scenario? Give an example, specifically an example that eliminates a loss scenario.
41. Slide 17 – Based on the controller model shown on slide 14, what is an example of a control method that would need to span multiple elements to be fully applied? Would the proposed control method focus on the ‘control algorithm’ or the controller black box?
42. Slide 19 – Explain and describe the method to pre-score the systematic control methods. Will the basis and description be in NEI 20-07? How does the scoring correlate to delta CDF and delta LERF that result in particular RROs be adopted?
43. Slide 20 – Need more descriptive details for each bullet as they are not clear in their intent.
44. Slide 21 – What is the motivation for adding administrative and procedural aspects as a control methods (types), as this was not previously described in draft C of NEI 20-07?
45. Slide 22 – Explain how entropy applies. Provide more details on how this correlates to scoring control methods? Scoring is a new and separate process that previously did not exist.

Staff noted we’d like to see an example of this aspect. NEI noted staff’s request and will follow up in the next engagement.

46. *Slide 26 – Will the formal endorsement that is being anticipated be as a generic topical report? Given the several plant-specific items (e.g., STPA, risk significance and RRO, control measures) that will need reviewed for each application, has thought been given to multiple pilot or lead applications that implement the proposed approach?

Enclosure 1 provides the attendance list for this meeting.

Next Steps/Action Item

1. NEI will provide an example of the type of modification that will utilize the guidance provided in NEI 20-07 and illustrate what such license amendment request will entail.
2. NEI discussed the development of a White Paper (interim product) that would provide detail on the new approach that will be outline in Draft D of NEI 20-07. However, since this meeting NEI has decided to expedite the development of NEI 20-07 and will submit the revised draft guidance to the NRC in September 2021 in lieu of submitting a white paper.
3. NRC staff to determine whether the scope change of NEI 20-07, Draft D, will require a new submittal for a review fee exemption.

Conclusion

At the end of the meeting, NRC and industry management gave closing remarks. No regulatory decisions were made. NEI and other nuclear industry representatives expressed appreciation for the open dialogue. No members of the public provided comment.

Enclosure:

As stated

SUBJECT: SUMMARY OF THE PUBLIC MEETING TO DISCUSS THE NUCLEAR
ENERGY INSTITUTE'S PRE-SUBMITTAL OF NEI 20-07, HELD ON
JULY 1, 2021

DISTRIBUTION:

RidsRgn1MailCenter
RidsRgn2MailCenter
RidsRgn3MailCenter
RidsRgn4MailCenter
RidsNrrDro
RidsNrrDex
RidsResDe
RidsNRR
RidsOgcMailCenter

ADAMS Accession No.: ML21229A160

*via e-mail

OFFICE	NRR/DRO/IRSB/PM	NRR/DEX/ELTB/TR	NRR/DEX/ELTB/BC	NRR/DRA/APLC/TR	NRR/DRO/IRSB/PM
NAME	TGovan*	WMorton*	JJohnston*	SVasavada*	TGovan*
DATE	08/13/2021	08/13/2021	08/13/2021	08/16/2021	08/17/2021

OFFICIAL RECORD COPY

LIST OF ATTENDEES
PUBLIC MEETING TO DISCUSS THE NUCLEAR ENERGY INSTITUTE'S PRE-SUBMITTAL
OF NEI 20-07

July 1, 2021 9:00 AM to 12:00 PM

Microsoft Teams Meeting

<u>ATTENDEE</u>	<u>ORGANIZATION¹</u>
1. Eric Benner	NRC
2. Wendell Morton	NRC
3. Tekia Govan	NRC
4. Shilp Vasavada	NRC
5. Jeanne Johnston	NRC
6. Tony Nakanishi	NRC
7. Muzammil Siddiqui	NRC
8. David Rahn	NRC
9. Sergui Basturescu	NRC
10. Sunil Weerakkody	NRC
11. Bill Roggenbrodt	NRC
12. Ismael Garcia	NRC
13. Norbert Carte	NRC
14. Paul Rebstock	NRC
15. Steven Erickson	Unknown
16. Jana Bergman	Curtiss-Wright
17. Neil Archambo	Duke Energy
18. Chris Cook	NRC
19. Warren Odess-Gillett	Westinghouse/NEI
20. Tom Basso	NEI
21. Gary DeMoss	PSEG Nuclear LLC
22. John Conly	Certrec
23. Bernie Dittman	NRC
24. David Herrell	MPR
25. Hongbin Zhang	Unknown
26. Han Bao	Unknown
27. Marty Flynn	Entergy
28. Michael Waters	NRC
29. Sushil Birla	NRC
30. Richard Supler	Enercon
31. Christina Antonescu	NRC
32. Frances Pimental	NEI
33. Dana Lovelace	Unknown
34. Alan Campbell	NEI
35. James Watkins	Unknown
36. Omran Samadi	Unknown
37. Rob Burg	EPM

¹ Unknown organization indicates that the participant's affiliation was not provided by the issuance of this meeting summary.