Comments and Questions for NEI 20-07 New PRA-Based Approach
(July 1, 2021 Public Meeting Presentation)
(Highlighted Items Represent Highest Priority Questions)

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

(Staff Priority Topic for July 1st Discussion)

1. What is NEI's position on the consistency of the new approach with SRM to SECY 93-087?
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)?
3. 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 without the application of any diversity (or any specific types of diversity)?
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?
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?
6. Will NEI 20-07 draft D contain acceptance criteria associated with its approach?

PRA (Staff Priority Topic for July 1st Discussion)

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?
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.
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?
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?

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?

STPA

12. Is it NEI's intent that staff would need to include endorsement of STPA as used within the NEI 20-07process? 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.
13. Has NEI received any industry/licensee feedback on the use of the STPA approach and its efficacy for important-to-safety applications?
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)?

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?
16. Is 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)?
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?
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..

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

HAZARDS ANALYSIS (HA) APPROACH

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 Questions

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?
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?
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.
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?