NEI Responses to NRC Staff Comments on NEI 20-07, Draft B

Includes comments/feedback through the April 21, 2021 Public Meeting

NRC Comment 1	**NEI Response**
ACTION 1-A - NEI has the action to clarify the 10.1.3.2 SDO regarding whether it's a global analysis or just the scope of application software and platform software/hardware development with regard to Position 1 of the SRM to SECY 93-087 Item II.Q.	Changed SDO 10.1.3.2 to the following: "*A hazard analysis method is used to identify hazardous control actions that can lead to an accident or loss, and application software requirements and constraints are derived from the identified hazardous control actions. The hazard analysis is focused on the system (not just the application software) and should consider plant-level and system-level functions and processes. The hazard analysis should include faults and failures as well as misbehaviors in the absence of any faults or failures*."
NRC Comment 4	**NEI Response**
ACTION 4-A - NEI agreed to clarify this point on what is considered a "platform". This is a general clarification for the document.	Added the following definition in Section 3: ***Platform*** *– Software and hardware that is integrated to provide basic generic functionality for use by various applications (e.g., programmable logic controller).*
ACTION 4-B - NEI to take the action to look at whether the EPRI research report provides evidence that shows that CCF did not occur as per NEI 20-07's claims in Section 9.1 or describe what is the basis for how the certifier and/or investigator determined that no CCF occurred for the given failure set. This is with regard to the EPRI research document.	NEI revised this section to provide the necessary technical justification for accepting SIL3/SC3 certification as a means to adequately address CCF at the platform level.
Section 9.1 of NEI 20-07 states the following, in part, "The researchers found no instances of software CCF in any of the SIL 3 certified platforms. The report concluded that SIL certifications appear to be an accurate indicator of software reliability at the platform level. Based on the results of the EPRI report, SIL 3 systematic capability has been selected as a reasonable benchmark to excluding platforms for software CCF consideration."	Section 9.1 of NEI 20-07 was revised to provide a holistic technical justification for why CCF at the platform level can be adequately addressed by a SIL3/SC3 certification.

ACTION 4-C (1) - Explain why the methodology referenced above would have identified software CCFs.	
ACTION 4-C (2) - NEI to describe the technical basis in the EPRI research report that justifies these statements.	NEI 20-07 Section 9.1 was revised to provide a holistic technical justification for why CCF at the platform level can be adequately addressed by a SIL3/SC3 certification.
ACTION 4-D - NEI should explain how it can make the claim that SIL 3 platforms may be excluded from evaluation for software CCF consideration, given the context of the above quoted statement.	NEI 20-07 Section 9.1 was revised to explain the justification for excluding SIL3/SC3 platforms from further consideration of software CCF.
NRC Comment 5	**NEI Response**
ACTION 5-A - NEI to clarify what by the term "immune" in NEI 20-07 and to which parts of the system architecture this applies to.	A search for "immune" in Draft B 0f NEI 20-07 revealed no hits. The term "immune" was not used in NEI 20-07 Draft B, nor is it used in Draft C of NEI 20-07.
ACTION 5-B - NEI agreed to provide examples of licensing packages that exercises NEI 20-07 processes. This includes documents and design information necessary for a licensee/applicant to submit for review if employing NEI 20-07. NEI stated that they could provide an example in the near term but not likely during any of the remaining April public meetings.	NEI agreed to provide an example licensing package at a later date.
ACTION 5-C - NEI plans to add the justification in the next version of NEI 20-07 Executive Summary statement that clarifies the SIL3 certification and supporting EPRI research is for a platform in isolation and not to a specific system configuration.	NEI 20-07 Section 9.1 was revised to provide a holistic technical justification for why CCF at the platform level can be adequately addressed by a SIL3/SC3 certification. The revision to NEI 20-07 specifies that a chosen platform must be integrated in a system architecture within the functional limits of the SIL3/SC3 certified function and used in conformance with the requirements of the associated safety manual. Going beyond these limits in the platform certification can limit the degree to which the platform in an architecture can be assumed to have CCF adequately addressed.
ACTION 5-D - NEI committed to providing sufficient technical information to justify specific claims made with regard to software CCF.	Sections 9 and 10 were revised to provide additional information for justifying the claim that use of a SIL3/SC3 platform and development of the application software hosted by that

	platform, using the same software techniques and measures, will provide reasonable assurance that software CCF in both the platform and application software has been adequately addressed.
ACTION 5-E - NEI committed to clarifying in NEI 20-07 what is meant by use of the term, "synthesized". This includes providing information on the methodology/process used to determine which criteria in IEC 61508 should be imported into NEI 20-07, why the particular criteria are adequate with a supporting technical basis. This includes how SDOs that are currently documented in NEI 20-07 are the correct set to meet the scope/requirements of NEI 20-07 with regard to eliminating consideration of software CCF. This action includes potential origin of SDO synthesis considering NEI stated that, for example, some automotive standards were used as a source.	Section 10 was revised to include what is meant by the term "synthesizing" as well as the methodology/process used to determine which criteria in IEC 61508 should be imported to NEI 20-07.
ACTION 5-F - NEI with action to clarify what is meant be "highly recommended" within NEI 20-07.	Section 10 was revised to add discussion on what is meant by "highly recommended". Section 13 was revised to include guidance that the Assurance Case will demonstrate the use of techniques that are Highly Recommended for SIL 3 when providing the argument and evidence to meet the applicable SDOs.
ACTION 5-G - NEI will clarify what is meant by "system" in NEI 20-07 with regard to the scope.	Added the following definition to Section 3: ***System*** *– Defined as either protection, control or monitoring and comprised of one or more programmable electronic devices, including integrated and supporting elements such as power supplies, sensors and other input devices, data highways and other communication paths, and actuators and other output devices [Adapted from IEC 61508-4].*
NRC Comment 6	**NEI Response**
ACTION 6-A - Figure B.1 of NEI 20-07 describes the assurance case structure necessary to demonstrate that software CCF is addressed using the "sufficiently low" concept. NEI has an action to clarify within the assurance case process	Section 11 was revised to include additional information on the Assurance Case. The Assurance Case is used to document adherence to platform and application software SDOs such

that, if the sufficiently low aspect is removed from this case structure, what does the assurance case look like going forward.	that an auditor can clearly discern how each SDO was applied. Additional clarification provided in Section 11 that the Assurance Case will demonstrate the use of the techniques that are Highly Recommended for SIL3.
NRC Comment 7	**NEI Response**
ACTION 7-A - NEI to take the action to clarify and address what SDOs in NEI 20-07 that allow for exclusion of SWCCF that are distinct from the software development guidance that is currently endorsed by the staff. Once verified, this information should be included in NEI 20-07 once it's been revised.	NEI presented a comparison table between the SDOs and guidance provided in RGs, endorsed IEEE standards, associated BTPs, and the Standard Review Plan during the public meeting on 4-21-21. NEI does not intend to provide this information within NEI 20-07 because 1) it is not the basis for the technical justification for establishing the SDOs, and 2) information in the table may change as standards and RGs are revised.
NRC Comment 8	**NEI Response**
ACTION 8-A - NEI to define the scope of the hazard analysis under SDO 10.1.3.2 and what this analysis specifically entails within NEI 20-07. This action also includes clarifying in NEI 20-07 that this type of analysis cannot be fulfilled by a conventional FMEA or similar level of analysis. Also clarify whether the hazard analysis is only used to derive new requirements/constraints on the application software and platform hardware/software.	See response to Action 1-A. Note that, as stated in the Draft B, the hazard analysis is used to: • identify hazardous control actions that can lead to an accident or loss • derive application software requirements • derive application software constraints Identification of the hazardous control actions, requirements and constraints are all factored into the application software design. The proposed text in the response for Action 1-A requires the analysis of hazards as a result of "misbehaviors in the absence of any faults or failures". This perspective is beyond the scope of an FMEA. Therefore, an FMEA will not satisfy the requirements of the hazard analysis defined in NEI 20-07.
ACTION 8-B - NEI to also clarify in NEI 20-07 how specific hazards (i.e. sources of CCF) that are identified by the hazard analysis in SDO 10.1.3.2 are specifically addressed by the processes	The system hazard analysis required by SDO 10.1.3.2 involves analyzing for potential systematic failures in the HSSSR system. An important aspect of the system hazard analysis is identifying HSSSR systematic misbehaviors in the

described in NEI 20-07 or by other means (e.g. defensive measures or other design features).	absence of any HSSSR faults and failures. The results of such a systematic approach to a hazard analysis identifies HSSSR systematic failures that can rise to a CCF. For each systematic failure identified in the hazard analysis under SDO 10.1.3.2, control methods are determined to avoid the hazard. The hazard analysis is also used to identify application software requirements and constraints. The SDOs are used to ensure high-quality application software is developed, considering the requirements and constraints identified in the hazard analysis.
ACTION 8-C - NEI to clarify in NEI 20-07 how exceptions (i.e. not addressing certain SDOs) are handled and how it should be documented including providing a technical basis on why the exception is acceptable.	Section 11 of NEI 20-07 includes the following statements: "*Any exceptions taken to application of SDOs should be clearly documented with an explanation of why the excluded SDO was not applicable or essential to software development quality*." and, "*It is expected that the assurance case will demonstrate the use of the techniques, or variations with adequate justification, that are Highly Recommended for SIL3 when providing the argument and evidence to meet the applicable SDO associated with them*." These two statements in Section 11 clarify how exceptions are handled in the Assurance Case.
NRC Comment 9	**NEI Response**
ACTION 9-A - NEI to clarify with more detail how the guidance of Section B.3.1.2 of BTP 7-19 Revision 8 is applicable to application/platform software as its not apparent this concept is a one-for-one correlation conceptually. NEI 20-07 should be updated to reflect this understanding.	**NEI clarified in the 4-21-2021 public meeting that the guidance proposed in NEI 20-07 is intended to address BTP 7-19 Revision 8, Section B.3.1.3 and not Section B.3.1.2. The staff found this clarification acceptable and this action can be considered closed.
ACTION 9-B - (1) NEI has action to explain what a D3 assessment would look like if a licensee or applicant incorporates NEI 20-07's processes into the design. Clarify what aspects of a D3	The second paragraph in the Executive Summary of NEI 20-07 was revised to include the following: "*When a Diversity and Defense-in-Depth (D3) analysis for the HSSSR system is performed, and the assurance case demonstrates that the*

assessment would remain (i.e. the gaps) if the processes in NEI 20-07 are implemented.	*platform and the associated application software has adequately addressed CCF, then these parts of the system can be exempted from being postulated as a source of CCF. This does not exclude the need for an HSSSR system D3 analysis because other CCF vulnerabilities may be identified (e.g., data communications).*"
ACTION 9-B - (2) NEI to clarify in NEI 20-07 next revision that there is still an expectation that a D3 assessment is still required even though application software and platform hardware/software may be excluded.	The Executive Summary was revised to include the following wording: "*When a Diversity and Defense-in-Depth (D3) analysis for the HSSSR system is performed, and the assurance case demonstrates that the platform and the associated application software has adequately addressed CCF, then these parts of the system can be exempted from being postulated as a source of CCF. This does not exclude the need for an HSSSR system D3 analysis because other CCF vulnerabilities may be identified (e.g., data communications)*." Section 13 was added and includes the following wording: "*An HSSSR system D3 analysis is still required to assess the system as a whole and identify other CCF vulnerabilities. Examples of other CCF vulnerabilities include the use of data communications and any external hazards that could impact multiple redundancies of the HSSSR system*."
ACTION 9-B - (3) NEI to explore providing an example scenario of a proposed digital modification LAR that utilizes NEI 20-07 including what documents would comprise the example LAR.	NEI agreed to provide an example at a later date.
ACTION 9-C - Typically, the NRC endorses guidance as one acceptable way of meeting a regulatory requirement. It is not clear from this meeting's discussions what regulatory basis could be cited to support an eventual endorsement action (e.g. regulatory guide endorsement). NEI to provide additional information on which regulatory requirement(s) does NEI 20-07 provide a method to satisfy?	NEI 20-07 Appendix A was revised to address this comment.

ACTION 9-D - NEI has action to talk internally about the NRC's points regarding diversity and defensive measures and follow up at a later date.	A new Section 11 was added to provide a discussion on diversity.
NRC Comment 12	**NEI Response**
ACTION 12-A - NEI to clarify in NEI 20-07 that Section 3.1.3 of BTP 7-19 revision 8 is the section for which this document is intended to address.	NEI added the following statement to the Executive Summary: *"Branch Technical Position (BTP) 7-19, Revision 8, provides three separate methods licensees can use to eliminate CCF hazards from further consideration. These three methods are (1) use of diversity within the DI&C system, (2) use of testing, or (3) use of defensive measures. NEI 20-07 is best aligned with the third method presented in BTP 7-19, Revision 8 (Section 3.1.3) - the use of defensive measures. NEI 20-07 provides objective criteria in the form of safe design objectives (SDOs) that are used to provide a defense against software CCF resulting from a software design defect. The SDOs are used for selection of platform hardware and software, and the development of application software."*
NRC Comment 13	**NEI Response**
ACTION 13-A - NEI to revise Section 6 of NEI 20-07 to better connect first principles/SDO concepts to current regulations. NEI to also include Appendix A for update to provide better connectivity to regulations.	NEI 20-07 Appendix A was revised to address this comment.
ACTION 13-B - NEI to also clarify in NEI 20-07 that for the list of regulations provided in NEI 20-07, that a particular systems, that if the processes of NEI 20-07 are applied, you meet listed regulations ONLY for the scope of software/hardware addressed by NEI 20-07's scope. Staff also suggested this clarification be made earlier within the document.	NEI 20-07 Appendix A was revised to address this comment.
ACTION 13-C - NEI to also clarify in the Executive Summary what type of reactor designs the processes of NEI 20-07 applies to – operating reactors, new reactors, advanced reactors, etc.	Added the following paragraph to the Executive Summary: "*NEI 20-07 applies to all holders of operating licenses under Title 10 of the Code of Federal Regulations (10 CFR) Part 50, "Domestic Licensing of Production Facilities" and all holders of*

	combined licenses under 10 CFR Part 52, "Licenses, Certifications, and Approvals for Nuclear Power Plants." Although the guidance in NEI 20-07 primarily focuses on power reactors, other licensees may also use the guidance in NEI 20-07 when selecting platforms and developing application software in HSSSR systems. However, certain aspects of NEI 20-07 guidance discuss regulatory requirements that may not fully apply to these licensees (e.g., Appendix B, "Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants")."
NRC Comment 14	**NEI Response**
ACTION 14-A - NEI agreed to present the set of SDO concepts from NEI 20-07 (i.e. IEC 61508) that have a corollary item in existing RGs and which SDO concepts NEI 20-07 do not have a corollary item in current RGs with a focus on the latter category to facilitate staff's understanding of the gaps between NEI 20-07 and current endorsed processes.	NEI provided a comparison table during the April 21, 2021 public meeting that compared the SDOs in NEI 20-07 with existing RGs, IEEE standards and the SRP.
NRC Comments on Specific SDOs	**NEI Response**
<u>SDO 10.1.3.7</u>: NEI will adjust the wording to this SDO and clarify what is meant by the phrase "...best- and worst-case performance".	SDO 10.1.3.7 was changed to the following: "*If data communications are required between application software elements and/or between application software elements and external systems, data requirements are specified, including best- and worst-case performance requirements. Best-case performance is based on ideal conditions. Worst-case performance is based on conservative assumptions of conditions (e.g., communication retries).*"
<u>SDO 10.2.3.1</u>: NEI to clarify what 'entities' is referring to in the context of NEI 20-07.	SDO 10.2.3.1 was changed to the following: "*When the application software can include or affect a number and/or variety of system elements, and responsibilities for application software design of such elements are split among two or more organizational entities[1], then a clear division of responsibility (DOR) is developed and agreed upon by all entities, and the DOR is maintained throughout the course of application software development activities.*"

	[1] An organizational entity is either a group of people within a corporate structure or a separate corporate entity.
SDO 10.2.3.3: NEI to clarify what 'entities' is referring to in the context of NEI 20-07.	See response to 10.2.3.1 above.
SDO 10.2.3.8: NEI to clarify why it would not be preferable to employ the self-monitoring in all situations, and not just in cases where a full variability language is used. NEI to also follow up on whether there is an SDO that covers all self-monitoring and/or self-diagnostic features or explain why there isn't one. Staff noted during discussions on this SDO that self-testing features play a significant role in many licensing activities for both operating plants and new reactors and an SDO that addresses self-testing as a design feature would seem essential.	SDO 10.2.3.8 was revised to the following: "*The application software design includes self-monitoring of control flow and data flow, and on failure detection, appropriate actions are taken*."
SDO 10.4.3.3: NEI to look at the "when" statement to see whether the "when" should be an "If" as the staff noted that beginning the SDO with "when" gives the impression that the SDO provides an expectation that you do integrate the design tools. NEI noted during this discuss that the statement as written is satisfactory because the ultimate goal of the SDO is to reduce the potential for human error.	NEI reviewed the SDO and concluded no change was necessary.
SDO 10.4.3.9: NEI to follow up on what criteria is used to perform a suitability assessment and whether the list of various aspects in the SDO is complete or are there other aspects that a licensee would have to consider when determining suitability.	SDO 10.4.3.9 was revised to the following: "*The application software design representation or programming language uses a translator that is assessed for suitability at the point when development support tools are selected. The suitability assessment evaluates qualities such as the use of defined language features, support for detection of mistakes, and support for the design method for the project*."
SDO 10.4.3.14: NEI action to clarify what criteria are used to determine that a new tool doesn't have any	SDO 10.4.3.14 was changed to the following: "*Qualification of each new version of an offline tool may be demonstrated by qualification of an earlier version if the functional differences will*

significant faults. Staff also recommended the term "consequential" rather than "significant".	*not affect compatibility with other tools, and evidence shows that the new version is unlikely to contain significant faults. The evaluation that the new version is unlikely to contain significant faults includes identifying the changes made for the revision, a review of the verification and validation activities performed on the revision, and review of any relevant operating experience with the revised version*."
SDO 10.6.3.1: NEI to define what is meant by "module" within the context of NEI 20-07.	The following definition was added to Section 3: ***Software Module*** *- Construct that consists of procedures and/or data declarations and that can also interact with other such constructs [IEC 61508-4, Definition 3.3.5]*
SDO 10.12.3.3: NEI to clarify what is meant by "independent" in the context of this SDO. This clarification also includes verification that, as written, this SDO accounts for components with more than one safe state.	SDO 10.12.3.3. was changed to the following: "*When equipment under the control (EUC) of the I&C system is normally in the state needed to perform a safety function, the I&C system design has no inputs that will change state when the EUC is in its normal state, and non-normal states in the EUC are readily detectable via means independent of the application software controlling the EUC. Administrative controls limit the duration of non-normal EUC states and limit the EUC in a non-normal state to one channel or division.*"