NEI Comment Responses and NRC Comment Status on NEI 20-07, Draft B

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
	Policy Consideration		
1	**Assessing CCF Vulnerabilities** The Executive Summary states, *However, a software defect in a digital system or component can introduce a safety hazard through a potential software common cause failure (CCF).* This statement seems to presume a licensee or applicant has identified hazards that can result in a software CCF.		The staff understands that the response to this comment was partially covered during the discussions regarding the response to Comment 9. Additional follow up discussions on this comment may occur dependent upon the remaining discussions regarding Comment 9. **Action 1-A (related to Comment 9 discussion)** - Most of this response was covered in the discussions with Comment 9. 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.
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?	The CCF vulnerability assessment would be performed as part of, rather than prior to, applying the guidance in NEI 20-07. Results of the CCF vulnerability assessment would be provided in the Assurance Case. For example, SDO 10.1.3.2 requires use of a hazard analysis method to identify hazardous control actions that can lead to an accident or loss. SCCF would be a primary focus of the hazard analysis. Application software requirements and constraints will be derived from the identified hazardous control actions. It is possible that, as part of the standard digital design process, a CCF hazard analysis/CCF vulnerability assessment would have already been developed prior to implementation of NEI 20-07. If this is the case,	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
		then the results of the prior hazard analysis/CCF vulnerability assessment (if it meets the requirements of NEI 20-07) could be used and presented in the Assurance Case.	
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.?	The SDOs are independent of any platform technology and application software. The hazard analysis SDO, for example, performed for each system would consider integration of different systems from an application software perspective. Software development for each system would be assessed separately following the guidance in NEI 20-07 using the information collected in the hazard analysis. NEI 20-07 focusses on addressing CCFs resulting from design defects in the internal platform software/hardware and application software. The SDOs address the level of quality needed to reach the conclusion that CCFs resulting from design defects in the platform and application software need not be further considered or postulated. NEI 20-07 does not address external system architecture - only platform hardware/software and application software. Some aspects of the system architecture will be addressed by ensuring the platform is installed using the Safety Manual requirements (part of the SIL3/SC3	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
		certification). However, it is not the intent of NEI 20-07 to address all CCFs resulting from other aspects of the system architecture (e.g., date communications).	
2	**Executive Summary Comment – Alignment with Related Guidance** This document 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 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 this approach in NEI 20-07 aligns with RIS Supplement 1 or BTP 7-19, 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.		The staff understands that the response to this comment was partially covered during the discussions regarding the response to Comment 9. Additional follow up discussions on this comment may occur dependent upon the remaining discussions regarding Comment 9. No further update at this time.
a	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.	NEI 20-07 is not intended to be related to, consistent with, or parallel with RIS 2002-22 Supplement 1. One risk-informed aspect to NEI 20-07 is the way an HSSSR system is determined. BTP 7-19 allows for site-specific PRA, if available, to support the determination of a HSSSR system. NEI 20-07 is expected to be used for the highest safety-significant safety-related SSCs - the consequences of failure are therefore very high. NEI 20-07 adopts a level of quality to reach the conclusion that CCFs resulting from a design defect in the internal platform software/hardware or application software need not be further considered or postulated. Similar to what has been achieved for hardware (e.g., HW Equipment Qualification), NEI's intent is that there is an achievable level of software quality over and beyond what is currently required to meet the NRC endorsed IEEE software standards. The SDOs provided in NEI 20-07 were selected to achieve this next level of software quality.	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
		Thus, NEI 20-07 is not based on failure likelihood or acceptable consequences. NEI 20- 07 will be modified to remove the language that implies frequency of occurrence.	
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?	NEI's position is that, by definition, the consequences of failure of a HSSSR SSC is high. NEI 20-07 provides guidance on platform selection and application software development where software quality is the focus. Similar to HW qualification, NEI's position is that it is possible to develop software with such high quality that a CCF resulting from an application software design defect or internal platform software/hardware design defect no longer needs to be postulated. Note that CCFs resulting from the system architecture will still need to be addressed (i.e., CCF resulting from other sources in the system architecture other than application software or platform hardware/software).	
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….*		NEI confirmed that they are removing all frequency/likelihood argument content from NEI 20-07. NEI also clarified that their position is that you should not use this under 10 CFR 50.59 change process and it was only intended for LSSSR systems. It's strictly going to be a deterministic process for NEI 20-07. Staff agreed with NEI's path forward with regard to removing 50.59 content. However, this is to be confirmed in NEI 20-07, draft C. However, closure of this comment is dependent upon receipt and review of the revised version of NEI 20-07. Once staff confirms the adequacy of the changes, this comment can be closed.

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
			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 that, if the sufficiently low aspect is removed from this case structure, what does the assurance case look like going forward.
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?	NEI 20-07 is not intended to be related to, consistent with, or parallel with RIS 2002-22 Supplement 1 nor is NEI 20-07 intended to be used for SSCs implemented under 50.59. The reason for mentioning 50.59 was to indicate that, if desired, a licensee could use the guidance in NEI 20-07 for projects implemented under 50.59 - although it is not recommended. For clarity, NEI plans remove any reference to 50.59 in NEI 20-07.	
b	How does NEI envision this document being used under 10 CFR 50.59?	NEI does not envision NEI 20-07 being used for projects implemented under 50.59. NEI 20-07 is intended to be used on HSSSR SSCs that would typically require a LAR to implement. NEI intends to remove any reference to 50.59 in NEI 20-07.	
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?	NEI 20-07 will be used for activities that will require a LAR to implement. The "Assurance Case" referred to in NEI 20-07 would be part of the LAR package. The initial draft of NEI 20-07 mentioned 50.59 in case a licensee desired to use the guidance in a lesser safety-significant SSC. However, NEI realizes that most, if not all, licensees will continue to use the RIS Supplement on lesser safety-significant projects. As such, NEI intends to remove mention of 50.59 in NEI 20-07.	

NEI Comment Responses and NRC Comment Status on NEI 20-07, Draft B

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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 a number of regulatory criteria but does not address SRM to SECY 93-087, for which BTP 7-19 is the implementable guidance of.		NEI stated that its approach in NEI 20-07 is intended to be consistent with the component testing approach (BTP 7-19 Revision 8, Section B.3.1.2) with respect to eliminating SWCCF from further consideration but for the application and platform hardware/software. NEI stated that NEI 20-07 is not intended to replace a D3 assessment and not intended to address the SRM directly. Staff needs more clarification on how this argument can be used for demonstrating that platform hardware/software design, integration, and application software development achieving the SDOs may be used to exclude such features from further consideration of potential CCFs. This process seems to be not consistent with the B.3.1.2.b testing approach, which deterministically demonstrates any identified vulnerabilities found during testing were eliminated in the final version of the design to be installed. **ACTION 9-A** – NEI to clarify that this is the intended approach in NEI 20-07 and how its specifically applies to platform hardware/software design, integration, and application software development. 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. Staff clarified that, as currently written, the processes in NEI 20-07 may be inconsistent with Item II.Q., Positions 1-3 of SRM to SECY 93-087 (as well as the technical basis that supports the SRM). Positions 1-3

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
			directs staff to postulate/address CCF for the aspects of the system architecture that are within the scope of NEI 20-07. NEI stated that NEI 20-07 was intended to fit within the context of BTP 7-19 but not to specifically be consistent with each relevant position of SRM to SECY 93-087. This potential inconsistency will be the subject of further discussions moving forward. NEI stated that a D3 assessment still needs to be performed to cover the "gaps" - NEI 20-07's processes only removes the application software and platform hardware/software (NEI 20-07's "scope") from a D3 assessment. Essentially, with regard to CCF coverage, there is a gap between what is addressed in the scope NEI 20-07 and the plant-level, overall considerations addressed by a comprehensive D3 assessment as described in BTP 7-19 Revision 8. **ACTIONS 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 assessment would remain (i.e. the gaps) if the processes in NEI 20-07 are implemented. (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 (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. This would facilitate staff's understanding of how NEI 20-07 fits into current regulatory processes.

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
			With regard to a future version that includes the entire system architecture, NEI stated that it's a greater technical challenge than they wanted to take on at this time and that the current scope of NEI 20-07 does provide the best benefit to industry at this time. **ACTIONS 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?
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.	NEI 20-07 addresses Position 1 of SECY 93-087: Identify CCF vulnerabilities in the systems. NEI 20-07 is based on the position that internal platform software/hardware and application software can be selected/developed with such high quality that SCCF resulting from a design defect in the platform internal software/hardware or application software no longer needs to be considered or postulated. There may be other CCFs that need to be postulated (e.g., due to various system architecture configurations), but SCCF due to a design defect in the application software or internal platform software/hardware would no longer need to be considered.	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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?	BTP 7-19 provides an exclusion of software that meets the specified testing criteria. Similarly, NEI 20-07 is providing an exclusion for platforms and application software that meet the SDOs. NEI 20-07 focuses only on internal platform software/hardware and application software development. A SIL 3/SC3 platform certification does address internal hardware of the platform. Additionally, SDO 9.2.3.1 states that when platform elements are integrated at the system level, subsystem level, or among other elements, they are integrated in accordance with the Safety Manual that complies with IEC 61508-2 Annex D or 61508-3 Annex D. The Safety Manual does address some elements of external architecture hardware.	
	Relationship of NEI 20-07 with related endorsed standards and RGs		
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).*		

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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.	The existing gap is between the level of software quality required to postulate the effects of a CCF as a beyond design basis (BDB) event (i.e., software quality level achievable using existing endorsed standards), vs. the level of quality required to conclude a CCF is adequately addressed and does not need to be postulated (i.e., additional level of software quality provided by NEI 20-07). Note that if a licensee is committed to specific IEEE standards for software development, then that licensee would be expected to use these IEEE standards in addition to NEI 20-07. NEI 20-07 is not intended to replace the IEEE standards - NEI 20-07 is intended to provide guidance that results in raising the level of quality beyond that provided by the IEEE standards. NEI considers the SDO concept 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	Yes. NEI 20-07 is expected to be used in conjunction with the currently endorsed software development standards. As stated in the response to Question 2a, NEI's position is that there is a level of software quality over and beyond what is currently required to meet the NRC endorsed IEEE software standards. The SDOs provided in NEI 20-07 were selected to achieve this next level of software quality. The goal of NEI 20-07 is to provide guidance on platform selection and application software development with such high quality that a licensee no longer needs to consider the internal platform software/hardware or application software or as a source of CCF. Comparable to applying the testing criteria in BTP 7-	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
	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.	19 to eliminate software as a source of CCF, the SDOs provide a set of criteria that can be applied to eliminate consideration of SCCFs resulting from internal platform software/hardware and application software design defects in the D3 analysis. There may be other sources of CCF that need to be evaluated as part of the overall system architecture other than the platform hardware/software and application software. NEI 20-07 only addresses CCFs resulting from design defects in the application software and internal platform software/hardware. External system architecture considerations such as channel interconnections, network communications etc. are not addressed in NEI 20-07. NEI recognizes that all potential sources of CCF must be considered as part of the overall system design and integration.	
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.*		
a	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.	It is NEI's position that the processes are complimentary and overlap but address different objectives. The current set of NRC- endorsed software development standards allow crediting a CCF as a BDB event. Applying the SDOs provided in NEI 20-07 would allow an applicant to deterministically assess that CCF associated with design defects in the platform and application software has been adequately addressed and need not be further considered or postulated.	

NEI Comment Responses and NRC Comment Status on NEI 20-07, Draft B

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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.*		
a	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 potential gaps that the methodology of NEI 20-07 is addressing?	NEI is not taking the position that there are any identified gaps with IEEE standards. The IEEE standards have a different objective than NEI 20-07 as expressed in the response for 10a. Rather, NEI's intent is that NEI 20-07 is a means to adequately address CCFs caused by latent design defects in the platform software/hardware and associated application software.	
	Intended NEI 20-07 scope and process, and technical basis		
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 this item, more interaction with NEI is needed after NEI and EPRI verify what conclusions are actually made within EPRI Report 3002011817 regarding software CCF and systematic failures that a user may expect when using SIL3 certified platforms are consistent with the claims made in NEI 20-07. **ACTION 4-A** – NEI clarified that within the context of NEI 20-07, "Platform" = a programmable logic controller (PLC). NEI agreed to clarify this point on what is considered a "platform". This is a general clarification for the document. **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.

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
			ACTIONS 4-C - 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.*" **(1) Explain why the methodology referenced above would have identified software CCFs.** *(2) NEI to provide the explanation of the technical basis to justify these quoted statements. Specifically, NEI to describe the technical basis in the EPRI research report that justifies these statements.* For example, Appendix F of EPRI 3002011817 states: "Due to the inability to quantify systematic safety integrity, it is not expected that field failure data based upon warranty returns will knowingly contain distinguishable, software (or other systematic) failure information. Despite that, this effort will attempt to determine how OEMs track software failures as well as other systematic failures, and how this information is used (if at all) in the SIL recertification process." It is not clear in the EPRI research report whether <u>any</u> of the failures quantified in Chapter 6 were due to software events, systematic failures, or whether they were all due to random hardware events. It also appears that no specific application information was considered with regard to the analysis of these failures.

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
			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.
a	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?	NEI 20-07 is heavily leveraged on research conducted by EPRI on the efficacy of SIL certification for nuclear power [EPRI Technical Report 3002011817, dated July 2019]. Some in the NRC staff have reviewed this EPRI report as it was used in the development of NEI 17-06, Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications, which is currently under NRC review for endorsement. Some in the NRC staff also conducted an audit of the SIL certification process as part of development of NEI 17-06 and are familiar with the application and requirements of IEC 61508. Regarding the 1.6 billion operating hours in the EPRI research, all the EPRI harvested data is valid with respect to components, systems, operating systems, platforms, etc. that are currently in use. The research evaluated the systematic process for programmable logic solvers (i.e., IEC 61508 based SIL certification), and evaluated the predictive reliability of that process to the actual failure rate data. The conclusion was that the systematic process can predict accurately the failure rate of the logic solver.	
5	**Executive Summary Comment – IEC 61508** The Executive Summary states the following:		

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
	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?	Yes, it is NEI's position that IEC 61508 provides the level of SDOs for both platform and application software to eliminate their consideration as a source of CCF. The guidance in NEI 20-07 is intended to be used in the selection of platform software/hardware and for the development of high-quality application software such that SCCF due to a software design defect no longer needs to be considered or postulated. As previously stated, NEI 20-07 only addresses SCCF resulting design defects in the internal platform software/hardware and application software. CCFs resulting from the system architecture other than the platform hardware/software and application software still need to be addressed. In other words, simply meeting the requirements of NEI 20-07 does not ensure that the entire integrated system is immune from all potential sources of CCFs.	
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?	Per the guidance in NEI 20-07, platforms are required to meet SIL3/SC3 requirements as specified in IEC 61508. Thus, for platforms, IEC 61508 is being used in its entirety. The guidance in IEC 61508 was strategically synthesized to harvest only the necessary elements needed to develop high-quality application software.	
c	The methodology in NEI 20-07 appears to	To comply with the guidance in NEI 20-07, platforms	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
	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).	would need to meet the requirements of SIL3/SC3 as specified in IEC 61508. Thus, internal platform hardware and software are required to be compliant with IEC 61508. As described in the response to Question 5B, the SDOs for developing application software were strategically synthesized from IEC 61508. Only portions of the guidance applicable to application software were taken from IEC 61508-3. EPRI research focused on platforms developed using IEC 61508. Results of their research indicate very high quality and reliability in platforms that used IEC 61058 for development in applications where safety is a paramount concern. NEI 20-07 builds on the EPRI research. IEC 61513 was not considered when developing NEI 20-07. IEC 61513 is a system level standard whereas IEC 61508 is focused on single failures that can be consequential.	
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.*		The staff understands that the response to this comment was partially covered during the discussions regarding the response to Comment 4. Additional follow up discussions on this comment may occur dependent upon the remaining discussions regarding Comment 4. **ACTION 7-A** – NEI stated during the meeting that there is a 'delta' between the software development processes currently endorsed by the staff and the development processes as described NEI 20-07. It is this 'delta' provides a sufficient technical basis to allow for exclusion of software CCF from further consideration. 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

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
			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.
a	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.	The guidance provided in NEI 20-07 is based on a mature standard (IEC 61508) and years of EPRI research on quality platform and software development. Based on this research, NEI feels strongly that application of the guidance provided in NEI 20-07 will result in selection of the highest quality platform and development of the highest quality application software, beyond that which can be achieved using existing standards. As stated above, NEI 20-07 is intended to be used in addition to the existing NRC endorsed standards on software development. There is overlap between the two sets, but there are also SDOs not covered by BTP 7-14, RGs and endorsed IEEE standards.	
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?	It is NEI's position that if a licensee provides an Assurance Case that provides the arguments and evidence that the SDOs are met, there is no need to further consider or postulate SCCFs resulting from design defects in the internal platform software/hardware or application software. The Assurance Case would be provided as part of a LAR for the HSSSR system. A licensee would still need to consider CCFs resulting from other aspects of the system architecture and plant integration.	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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."	SDO 10.1.3.2 requires use of a hazard analysis method to identify hazardous control actions that can lead to an accident or loss. SCCF vulnerabilities are the primary focus of this hazard analysis. The hazard analysis specified by SDO 10.1.3.2 is a global analysis considering all aspects of the system and architecture, including both hardware and software. Thus, the identified hazardous control actions will cover much more than application software. Some of the hazardous control actions identified will not apply to the application software while others will. This SDO requires that results of the hazard analysis be used to generate specific application software requirements and constraints as they apply to the system - both hardware and software. SDO 10.1.3.4 requires identification of hardware constraints that need to be considered when developing the application software are documented and complete. For example, if a specific channel response time is identified as a system requirement, then the time required for the application software to process a given input signal would need to be considered in addition to the field instrumentation (hardware) response time. This may place a constraint on the application software processing time due to the fixed hardware response time. Overall system and performance requirements will typically be developed through two separate sources - basic system functional and performance requirements and requirements discovered when applying the hazard analysis process. SDO 10.1.3.5	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
		ensures that, in addition to requirements discovered through application of the hazard analysis process, system performance requirements and constraints are also documented and applied, as applicable, when developing the application software.	
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.	First principles do not need acceptance criteria. Rather, they provide a principle-based conceptual understanding of the phenomena. It is the SDOs that provide the analysis guidance and acceptance criteria to meet the first principles. NEI 20-07 states, "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 safe design objectives (SDOs)."	
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.	See earlier comments regarding the term "sufficiently low". Documented adherence to the SDOs provided in NEI 20-07 offers evidence that the acceptance criteria for selection of a high-quality platform and development of high-quality application software at a level such that a CCF due to a design defects in the internal platform software/hardware and application software no longer needs to be considered or postulated has been met. For example, the acceptance criteria for a platform not being a source of CCF is evidence that the	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
		platform meets the SIL3/SC3 requirements identified in SDO 9.1.3.1 and is integrated within the requirements of SDO 9.2.3.1. For application software, the acceptance criteria would be the documented evidence that all relevant application software SDOs were achieved. NEI 20-07 requires development of an "Assurance Case" to detail how the various SDOs were met for both the platform and application software.	
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?	See earlier comments regarding the term "sufficiently low". NEI 20-07 is not intended to be related to, consistent with, or parallel with RIS 2002-22 Supplement 1. To a degree, NEI 20-07 provides a deterministic approach for evaluating platform software/hardware and development of application software in that by applying the prescribed SDOs, a CCF due to a design defect in the internal platform software/hardware or application software does not need to be further considered or postulated. NEI 20-07 will add the following statement: "*Documentation that the acceptance criteria were met consists of documented evidence that relevant SDOs were addressed adequately. A licensee will build an Assurance Case as part of a LAR package to clearly detail how the SDOs were met.*"	

NEI Comment Responses and NRC Comment Status on NEI 20-07, Draft B

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
b	Does draft NEI 20-07 address relevant acceptance criteria in BTP 7-19, Revision 8, including Section 3.1.3?	Yes - If the SDOs in NEI 20-07 are applied, the design attributes/defensive measures that are used to meet those SDOs, will meet the acceptance criteria in BTP 7-19, Revision 8, 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.	NEI agrees that "bounding" is not an applicable term in describing the scope of the first principles. It is accurate to state that the first principles are "complete." NEI's position is that these first principles are complete. NEI welcomes NRC feedback regarding the first principles provided in NEI 20-07. NEI will revise NEI 20-07 to remove "bounding" from the discussion on first principles.	
b	What is meant by the term "bounding"? Bounding with current regulations?	See response to Question 13a.	
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*		
a	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?	NEI's intent is that NEI 20-07 has enough information to facilitate the staff's review and does not plan to submit any portions of IEC 61508 for review and endorsement by the NRC. As stated in NEI 20-07, the SDOs are synthesized from the relevant guidance in IEC 61508 and other industry standards.	

NEI Comment Responses and NRC Comment Status on NEI 20-07, Draft B

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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.	NEI 20-07 is not intended to mirror the guidance in RIS 2002-22 Supplement 1. The next draft of NEI 20-07 will remove any connection to RIS 2002-22 Supplement 1. NEI 20-07 does not rely solely on operating experience when assessing a platform's susceptibility to SCCF - the platform must meet the requirements of a SIL3/SC3 system set forth in IEC 61508. Additionally, operating experience, when used in the context provided in NEI 20-07, only applies to internal platform software and hardware. The concept of platform operating experience is derived from EPRI research on SIL certified platforms. EPRI reviewed several platforms currently in operation and those that were SIL3 certified and in operation for approximately 1.6 billion operating hours had no evidence of experiencing a SCCF. This supports the correlation between operating experience and quality. As stated previously, NEI 20-07 only addresses CCFs resulting from design defects in the internal platform software/hardware and associated application software (i.e., not the system architecture as a whole). The concept behind NEI 20-07 is that by applying the relevant SDOs, CCFs resulting from design defects in the internal platform software/hardware and application do not need to be further considered or postulated. NEI may consider to addressing the complete system architecture in NEI 20-07 in a future revision. However, at this time, NEI is focusing solely on SDOs for high-quality platform selection and application software development such that a software CCF does not need to be further considered or postulated.	NEI noted during discussions on this comment that NEI 20-07 does not solely rely upon or significantly rely on operating experience in the manner implied in staff comment 16. The staff understands that the response to this comment was partially covered during the discussions regarding the response to Comment 4. Additional follow up discussions on this comment may occur dependent upon the remaining discussions regarding Comment 4.

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
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?	NEI position is that it is possible to develop such high-quality software that SCCF caused by software design defects no longer needs to be considered or postulated. As stated above, NEI 20-07 does not rely solely on operating experience when assessing a platform's susceptibility to SCCF - the platform must meet the requirements of a SIL3/SC3 system set forth in IEC 61508. Software defects are only one contributor to CCF. Other aspects still need to be addressed, such as the whole system architecture. NEI 20- 07 does not currently address whole system architecture. Therefore, it is not NEI's position that adherence to the guidance in NEI 20-07 is enough to conclude that a fully integrated system is not susceptible to CCF.	
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?	Yes - If architecture in this question is referring to HSSSR digital system architecture. SDO 9.1.3.1 requires the platform to meet or exceed a Systematic Capability of SC3 (as for a SIL 3 system) as described in IEC 61508. Part of the SC3 certification pertains to the internal architecture of the platform, which includes both hardware and software. SDO 9.2.3.1 addresses platform integration and states, in part, that when platform elements are integrated at the system level, subsystem level, or among other elements, they are integrated in accordance with the Safety Manual that complies with IEC 61508-2 Annex D or 61508-3 Annex D. The Safety Manual requires application of specific external architectural design elements in order to maintain the SC3 certification. With respect to both platform and application software, NEI 20-07 presents specific design	

Ref #[1]	NRC Comment	NEI Response	Comment Status as of 04-07-2021
		objectives that, when met, will constitute a safe system that is, highly reliable and dependable. Note that the focus of NEI 20-07 is on HSSSR platform and application software because these elements are the most probable cause of CCF in a HSSSR system.	