



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

August 30, 2021

Mr. Alan D. Campbell
Technical Advisor
Nuclear Energy Institute
1201 F Street, NW, Suite 1100
Washington, DC 20004

SUBJECT: NRC STAFF COMMENTS ON NUCLEAR ENERGY INSTITUTE 17-06
REVISION 0, "GUIDANCE ON USING IEC 61508 SIL CERTIFICATION TO
SUPPORT THE ACCEPTANCE OF COMMERCIAL GRADE DIGITAL
EQUIPMENT FOR NUCLEAR SAFETY RELATED APPLICATIONS"

Dear Mr. Campbell:

On February 23, 2021, the U.S. Nuclear Regulatory Commission (NRC) received a submittal from the Nuclear Energy Institute (NEI) requesting review and endorsement of Revision 0 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" (Agencywide Documents Access and Management System (ADAMS) Accession No. ML21083A147). In this request, NEI stated that NEI 17-06 establishes guidance for an acceptable approach to procure and accept commercial grade digital equipment for nuclear safety-related applications, when the equipment has an accredited third-party safety integrity level (SIL) certification per International Electrotechnical Commission (IEC) 61508. The staff are currently engaged in evaluating NEI 17-06 for potential endorsement. If found acceptable, the endorsement would include the development of a draft regulatory guidance document and other necessary steps to develop a final regulatory guide. The staff have generated comments in the enclosed "Open Items" table that should be addressed by NEI in order for staff to continue its endorsement review.

For dedication of commercial grade digital equipment, leveraging the SIL certification process as described in NEI 17-06 in lieu of individual supplier surveys is considered a practical alternative to the commercial grade survey methodology currently used by dedicating entities. However, the process as described in NEI 17-06 is currently informal and not specific enough to adequately define an approach that can be endorsed by the NRC without additional clarifications and exceptions. To have confidence in the accreditation process, a more formal quality assurance oversight process by a specified owner is necessary. The proposed inclusion of additional accreditation and certifying bodies that have not been adequately vetted by the NEI and NRC does not appear prudent or defensible; especially, given the shortcomings observed by the staff and NEI with the American National Standards Institute (ANSI) National Accreditation Board (ANAB) exida audit as discussed during the June 23, 2021 public meeting (ADAMS Accession No. ML21223A311). Unlike the agreements in place between the International Laboratory Accreditation Cooperation and NEI as a stakeholder member in the accreditation organization, there is no such formality described in NEI 17-06 Revision 0 for the international governing bodies responsible for International Standards Organization 17065 and IEC 61508.

These and other topics are further discussed in specific comments on NEI 17-06, Revision 0 are outlined in the enclosed "Open Items" table. The comments are binned and ranked according to their possible classification as an exception, clarification or suggestion; and, they broadly span the areas of QA oversight, NEI 17-06 scope, and use of EPRI 3002011817.

The staff has scheduled a phone call for September 9, 2021, if needed, to allow NEI an opportunity to ask clarifying questions to assist in understanding NRC's comments. To facilitate the review schedule established to develop a draft regulatory guide, responses to these comments are expected by September 24, 2021.

The next public meeting to discuss the final set of comments on NEI 17-06, Revision 0, and the proposed NEI resolutions to the staff's comments, is scheduled for September 28, 2021.

If you have any concerns or questions, please contact Ms. Serita Sanders, Project Manager, at (301) 415-2956, or through e-mail to Serita.Sanders@nrc.gov.

Sincerely,

Eric J. Benner, Director
Division of Engineering and External Hazards
Office of Nuclear Reactor Regulation

cc: Maria Assard

SUBJECT: STAFF COMMENTS ON NUCLEAR ENERGY INSTITUTE 17-06 REVISION. 0,
 "GUIDANCE OF USING IEC 61508 SIL CERTIFICATION TO SUPPORT THE
 ACCEPTANCE OF COMMERCIAL GRADE DIGITAL EQUIPMENT FOR
 NUCLEAR SAFETY RELATED APPLICATIONS" DATED: AUGUST 30, 2021

DISTRIBUTION:

PUBLIC

RidsACRS_MailCTR Resource

RidsNrrDEX Resource

RidsNrrDorl Resource

RidsNrrDorlLlpb Resource

RidsNrrPMSSanders Resource

RidsNrrLADHarrison Resource

RidsNRRDEXEltb Resource

NRR FO Technical Assistants

SSanders

EBenner

JJohnston

MWaters

KKavanagh

CCook

DMorey

DTaneja

DRahn

GGalletti

OAYegbusi

BDittman

JZhao

SBasturescu

IGarcia

ADAMS Accession Nos.:**ML21237A305 (Letter)****ML21223A311 (NEI 17-06 Staff Review June 23, 2021 Public Meeting Summary)****ML21083A147 (NEI 17-06 Guidance Document)**

OFFICE	NRR/DORL/LLPB/PM	NRR/DORL/LLPB/LA	NRR/DEX/EICB/BC
NAME	SSanders	DHarrison (RButler for)	MWaters
DATE	8/25/2021	8/25/2021	8/26/2021
OFFICE	NRR/DRO/IQVB/BC	NRR/RES/ICEEB/BC	NRR/DORL/LLPB/BC
NAME	KKavanagh	CCook	DMorey
DATE	8/26/2021	8/26/2021	8/26/2021
OFFICE	NRR/DEX/ELTB/BC	NRR/DEX/D	
NAME	JJohnston	EBenner	
DATE	8/30/2021	8/30/2021	

OFFICIAL RECORD COPY

NEI 17-06 Staff Comment Open Items

STAFF COMMENTS ON NEI 17-06 REVISION 0, "GUIDANCE OF USING IEC 61508 SIL CERTIFICATION TO SUPPORT THE ACCEPTANCE OF COMMERCIAL GRADE DIGITAL EQUIPMENT FOR NUCLEAR SAFETY RELATED APPLICATIONS"

Comment No.	Page and Section	Comment	Comment Significance & Type
1	General	As the proposed commercial grade dedication (CGD) methodology will be considered a reduction in commitment in accordance with Title 10 of the <i>Code of Federal Regulations</i> (10 CFR) 50.54(a)(4), the report should add an action, that the licensee use of this approach will require a change to their approved quality assurance program manual. For comparison purposes, Nuclear Energy Institute (NEI) 14-05, states, in part, "Prior to a licensee implementing the methodology outlined in NEI 14-05A, Revision 0, the U.S. Nuclear Regulatory Commission (NRC) required a licensee to submit a revision to its Operating Quality Assurance Program (OQAP) for NRC acceptance in accordance with 10 CFR 50.54(a)(4) since implementation of NEI 14-05A represented a reduction in commitment."	Potential Exception QA Oversight
2	Page 3, Section 1.3	<p>Section 1.3, "Acceptance of Safety Integrity Level as Verification of Dependability Critical Characteristics," leverages the results of the American National Standards Institute (ANSI) National Accreditation Board (ANAB) audit of exida and the supplemental effort by the NEI working group to complete the supplemental audit checklist related to the implementation of the International Electrotechnical Commission (IEC) 61508 technical criteria at exida. The report concludes that the SIL accreditation process is sufficient, robust, and repeatable, such that other ABs that are signatories of the International Accreditation Forum (IAF) should also be considered acceptable for these purposes.</p> <p>The NRC's approach to approving NEI 14-05 regarding use of the ILAC process in lieu of CGD activities, were based on the NRC and the industry evaluated multiple accreditation bodies (ABs) and certifying bodies (CBs) performing work in accordance with the established ILAC programs and agreements as it pertained to the implementation of the International Standards Organization (ISO) 17025 standard, to gain assurance that the process was stable,</p>	Potential Exception QA Oversight

Comment No.	Page and Section	Comment	Comment Significance & Type
		<p>robust, and repeatable. This report is essentially based on conclusions drawn from a single audit observation (done twice) of one AB and one CB, by the NRC and NEI, and additional inference from a report by Electric Power Research Institute (EPRI) that has not been formally evaluated by the NRC.</p> <p>As a result, the NRC does not consider it appropriate to include or suggest that other, non-vetted ABs, are acceptable in the report. Given the observations made during the implementation audit conducted by ANAB of exida, which were discussed at the June 23, 2021 public meeting, and the need to perform supplemental verification external to the ANAB process (supplemental checklist), NEI 17-06 should clearly limit the applicability of using this alternative currently to ANAB with restrictions, with provisions for potentially adding other ABs after adequate vetting by NEI, US Nuclear licensees, and the NRC.</p>	
3	Page 3, Section 1.3	<p>Similarly, the sole observation of ANAB auditing the capabilities and programmatic controls at exida, and the need to perform a supplemental checklist due to observed weaknesses in the ANAB accreditation process, should not be used as the basis for approval of other CBs without continued direct observation of the accreditation activities of ANAB for those other CBs and completion of the supplemental checklists.</p>	<p>Potential Exception QA Oversight</p>
4	Page 20, Section 4.1	<p>The first sentence in the paragraph, "The approach being laid out in this document for performing commercial grade dedication of digital equipment is based on the conclusion pointed out in Section 3.3 of this document" implies that EPRI research is the sole source of information that leads to conclusion that SIL certifications can be used as the evidence of acceptability of dependability critical characteristics (CC), as defined by EPRI TR-106439. Whereas, NEI's observation of ANAB's audits of exida that used the NEI audit checklist (based on EPRI TR-106439 dependability CC) is an alternative to the EPRI research. Since the NRC endorsement of NEI 17-06 is not relying on EPRI research, revise this paragraph to provide adequate basis for the stated claim.</p>	<p>Potential Exception Use of Ref. 8 EPRI 3002011817</p>

Comment No.	Page and Section	Comment	Comment Significance & Type
5	Page 25, Section 4.4	In the "SIL Certification Process Method of Verification" column reference is made to the EPRI research report (Reference 8). Since the EPRI report is not being evaluated by the NRC, reference should only be made to the relevant IEC 61508 consensus standard sections. In general, any information from the EPRI research report that is necessary for this CGD process (that relies on safety integrity level (SIL) certification) should be included within NEI 17-06.	Potential Exception Use of Ref. 8 EPRI 3002011817
6	Page 30, Section 5.5	Section 5.5, Compensatory Measures, identifies a long-term and short-term path to resolve the observed accreditation process weaknesses. The long-term path is to work with ANAB to improve the assessment of Section 7.1.2 of ISO 17065. However, that action has been noted as preliminary in nature and will take an unspecified length of time to achieve, if at all. Given the nature of this as preliminary, at best, the NRC cannot endorse a compensatory measure that has not been formalized. NEI should provide a more definitive set of actions that have been agreed to and accepted by both parties and a timeline to achieve full implementation.	Potential Exception QA Oversight
7	Page 30, Section 5.5	Furthermore, the short-term compensatory measure described also lacks adequate specificity to enable the NRC to endorse as an acceptable means to meet the regulatory requirements. Specifically, the action to have the U.S. nuclear industry develop a supplemental accreditation checklist to be applied to each CB that would assess their scheme's compliance with IEC 61508 within the context of the dependability CC in Table 4-1 of EPRI TR106439. Details regarding the methods by which this will be performed and by whom more specifically (i.e., NEI working group, Nuclear Procurement Issues Corporation (NUPIC), individual licensees), and a description of necessary and sufficient administrative controls to ensure consistent application of the checklist should be provided. This may include the need to evaluate and accept the EPRI report as well as the IEC 61508 standard as it pertains to the checklist provided in Appendix D.	Clarification QA Oversight

Comment No.	Page and Section	Comment	Comment Significance & Type
8	General	<p>The intended scope of applicability of NEI 17-06 should be clear to support its efficient potential endorsement in a Regulatory Guide (RG). The staff considers scope of NEI 17-06 to only apply under the following conditions/circumstances. 1) Applies only to digital I&C equipment, 2) Applies only to CGD for the critical characteristic of dependability, 3) Applies only to 10 CFR Part 50 and 10 CFR Part 52 power reactors, 4) Applies only where the item has a certification of compliance to an IEC 61508 SIL by a functional safety certifying body, and 5) Applies only where the functional safety certifying body has been accredited by signatory to the International Accreditation Forum. If 1 through 5 above do not correctly set the limit of NEI 17-06's intended application, would NEI clarify and indicate whether a clarification would also be included in the body of NEI 17-06?</p>	<p>Clarification NEI 17-06 Scope</p>

Comment No.	Page and Section	Comment	Comment Significance & Type
9	General	<p>Alignment on NEI's intended scope of endorsement of NEI 17-06 should be clear to support its efficient potential endorsement of a RG. The staff considers scope of NEI 17-06 to be endorsed by the NRC to include the following items. 1) For a commercial item with a SIL certification, the guidance in NEI 17-06 that applies the ISO 17065 accreditation process as supplemented is acceptable for use as a commercial-grade survey of a SIL certification service provided by an IEC 61508 functional safety certifying body, 2) For a commercial item with a SIL certification, the guidance in NEI 17-06 that applies a SIL certification by an accredited certifying body is acceptable for use when assessing the suitability of the commercial item for its critical characteristic of dependability, 3) When applying EPRI TR-106439 and EPRI 30020002982 to a commercial item with a SIL certification, the guidance in NEI 17-06 that applies a SIL certification by an accredited certifying body to establish the dependability characteristics of the commercial equipment is an acceptable substitute for methods: 2– Commercial-Grade Survey of Supplier, and 4–Acceptable Item Performance Record when performing a CGD. If 1 through 3 above do not correctly represent what NEI seeks in an NRC endorsement of NEI 17-06, would NEI clarify and indicate whether a clarification would also be included in the body of NEI 17-06?</p>	<p>Clarification NEI 17-06 Scope</p>
10	General	<p>It appears that NEI 17-06's scope does not include or reference a method to determine the SIL level upon which a particular piece of digital I&C equipment's dependability would be evaluated using NEI 17-06 as guidance. NEI to clarify if NEI 17-06's endorsement should leave open the method for determining the SIL level of the digital equipment being dedicated?</p>	<p>Clarification NEI 17-06 Scope</p>

Comment No.	Page and Section	Comment	Comment Significance & Type
11	Page 9, Section 2.1	Revise second sentence from "This accreditation is typically in accordance with ISO 17065" to "This accreditation is typically in accordance with ISO 17065 supplemented by IEC 61508 SIL certification scheme." Change fourth sentence from "The AB performs audits and monitors activities of the CB in order to confirm that their processes and procedures, and their corresponding implementation follows ISO 17065" to "The AB performs audits and monitors activities of the CB in order to confirm that their processes and procedures, and their corresponding implementation follows ISO 17065 supplemented by IEC 61508 scheme."	Suggestion QA Oversight
12	Page 21, Section 4.1	When procuring a SIL certified equipment, the dedicating entity should receive the SIL certificate from the original equipment manufacturer (OEM) and not the CB. CB grants the SIL certificate to the OEM and has no obligation of providing the SIL certificate to the dedicating entity. In addition, the dedicating entity should also receive a set document from the OEM that describes the application limitation of their SIL certified product. Please update this figure to correct these relationships.	Suggestion NEI 17-06 Scope

Comment No.	Page and Section	Comment	Comment Significance & Type
13	Page 22, Section 3	<p>NEI 17-06 states that the estimated failure rates of the observed logic solver failure data are conservative since 323 failures were expected but only 205 occurred. It also states: "These results also illustrated how the probabilistic failure rates and the <i>systematic integrity</i> could both be evaluated through the review of field failure data." The document also states that "it is valuable to note that systematic integrity is a parallel concept to the nuclear industry's concept of common cause failure." The NRC finds this statement to be unclear and potentially misleading to potential users of NEI 17-06. The integrity of a component does not in itself establish systematic integrity of the system's safety function. Absent this additional consideration of system architecture and application of safety features, NRC understands such individual logic solver failure data can at best represent only the reliability of the specific platform device configuration that was incorporated into a system of devices designed to achieve a plant safety function. Please clarify what is meant by stating that systematic integrity of a single platform can be considered a "parallel concept" to the nuclear industry's concept of common cause failure, which usually addresses failure causes which can occur concurrently in redundant channels.</p>	<p>Clarification NEI 17-06 Scope</p>
14	Page 22, Section 4.2	<p>This guidance limits the use of SIL certified equipment to a risk-based selection process. Does NEI intend to provide guidance or example for selection of a SIL level that is appropriate for a safety function application using a deterministic process, e.g., can a SIL 3 certified component be used in an ESFAS with 3 or 4 divisions?</p>	<p>Suggestion NEI 17-06 Scope</p>

Comment No.	Page and Section	Comment	Comment Significance & Type
15	Page 30, Section 5.5	<p>Section 5.5, Compensatory Measures, states, in part, that “after five years, these assessments would be reperformed to ensure the CB’s schemes have remained compliant, unless the long-term path has already been realized. Five years is an appropriate amount of time because the IEC 61508 standard is a very stable document, and the accreditation activities will continue to happen annually.”</p> <p>Although the accreditation process may be stable, the NRC considers a 3-year timeframe rather than the proposed 5-years is appropriate, given industry precedent for similar evaluations of the supply chains quality programs at a period not to exceed 3 years. NRC suggests it is appropriate to reflect this long-standing practice for this activity as well. (see comment to Section 7.3, Paragraph 2)</p>	<p>Suggestion</p> <p>QA Oversight</p>
16	Page 30, Section 5.5	<p>Implementation of the supplemental checklist will require NRC licensees, or their representatives, to have access to the ANAB processes as well as the CBs internal programs, procedures, and specific evaluations of sample products that have been vetted by the CB. This document does not address any formal agreements by the ABs, CBs, and either NEI, other US licensee organizations, such as NUPIC, or individual NRC licensees to have access to conduct such audit activities or grant access during audit performance. Please describe how the implementation of the supplemental checklists will be accomplished and how has this been formally adopted?</p>	<p>Clarification</p> <p>QA Oversight</p>

Comment No.	Page and Section	Comment	Comment Significance & Type
17	Page 32, Section 6.5	Section 6.5, "Corrective Action," states in part, that the dedicating entity is required to notify licensees and the NRC of deviations/defects which could result in substantial safety hazards as required by 10 CFR Part 21. In accordance with 10 CFR Part 21 the dedicating entity need only report to the NRC not licensees, and only defects and failures to comply associated with substantial safety hazards for dedicated items need to be reported, not deviations. Please revise this to reflect the regulation language.	Suggestion QA Oversight
18	Page 1, Section 1.1	Accreditation body (AB) in the United States is now called ANAB (ANSI National Accreditation Board), a wholly owned subsidiary of the American National Standards Institute (ANSI). (see https://anab.ansi.org/). Update NEI 17-06 accordingly (consistent with Section 5.3 identification).	Suggestion QA Oversight
19	Page 3, Section 1.3	EPRI 3002002982 is endorsed by RG 1.164, which is not referenced in NEI 17-06. In the same way NEI 17-06 includes a reference to the NRC safety evaluation of EPRI TR-106439, NEI 17-06 should include a reference to RG 1.164.	Suggestion NEI 17-06 Scope
20	Page 21, Section 4.1	Manufacturer's safety manual and related documents may only be made available upon procuring the equipment from OEM. The steps should identify where in the procurement process of the SIL certified equipment this information is made available and any additional documents that should be a part of the procurement.	Suggestion NEI 17-06 Scope
21	Page 21, Section 4.1	ANAB issued CB's accreditation certificates are publicly available on their website. Is this also true of other ABs? The steps should clarify how to obtain the accreditation certificate.	Clarification QA Oversight

Comment No.	Page and Section	Comment	Comment Significance & Type
22	Page 23, Section 4.3	This sections states, in part, "and must be certified to meet or exceed the SIL that has been established for the application (as described in Section 4.3)." This would be true when the safety instrumented system (SIS) is designed using IEC 61511 methodology. However, none of the operating reactor's safety systems have been designed using the SIS process. This "must" requirement would require the plants to determine the SIL level of the safety systems prior to using a SIL certified component in their plants. Is this the intent of this guidance?	Clarification NEI 17-06 Scope
23	Page 24, Section 3	Certain statements made within NEI 17-06 imply a general condition exists for all CBs when the data provided seems to support work performed by a particular CB. For example, in Section 3.3 it is stated that CB's "oversee" the compliance of a vendor to quality standards. Some evidence of this was observed by the NRC staff at its observations of the ANAB accreditation of a particular CB, but no evidence is provided that all CBs perform oversight of a vendor's self-validation process. NEI 17-06 should provide evidence that all CBs perform oversight of a vendor's self-validation process.	Suggestion QA Oversight
24	Page 27, Section 4	Regarding the SIL Certificate and Safety Manual: The steps to be followed should include actions that address the need to identify whether the safety manual identifies any precautions, conditions of operation, or limitations in the use of the equipment for which the SIL Certificate applies. Specifically, to maintain certification, the safety manual specifies implementation, configuration, or maintenance or diagnostic requirements to be followed, to maintain compliance with the certificate reliability statements.	Suggestion NEI 17-06 Scope

Comment No.	Page and Section	Comment	Comment Significance & Type
25	Page 31, Section 6.1	Section 6.1, "Organization," states, in part, that the dedicating entity retains overall responsibility for assuring that purchased digital devices meet applicable technical and regulatory requirements and that reasonable assurance of quality exists. There are no special requirements beyond 10 CFR Part 50, Appendix B. It should be noted that the dedicating entity must also meet the requirements of 10 CFR Part 21. This should be added for completeness and accuracy.	Suggestion QA Oversight
26	Page 33, Section 7.2	Section 7.2, "Verification that the SIL Certification Process Continues to be Consistent with NRC Endorsed Practices," states, in part, that "as part of the continued oversight, a nuclear industry team, through NEI, will monitor the IEC 61508 SIL certification requirements to verify that they continue to cover the EPRI TR 106439 Dependability Critical Characteristics." Please describe the compliment of that team, whether there is a documented commitment to support these activities among the team members, and the nature of any commitment.	Clarification QA Oversight

Comment No.	Page and Section	Comment	Comment Significance & Type
27	Page 33, Section 7.2	<p>Section 7.2, "Verification that the SIL Certification Process Continues to be Consistent with NRC Endorsed Practices," states, in part, that "If changes adversely impact coverage of the EPRI TR 106439 Dependability Critical Characteristics, then the nuclear industry through NEI has the ability to provide feedback to the IEC 61508 standards development committee to change the draft revision to encompass these critical characteristics." Does this require NEI to have a formal agreement with the IEC to affect such revisions?</p> <p>The NRC's approval of the methodology described in NEI 14-05 regarding use of the ILAC accreditation process relied, in part, on the formal relationship NEI and the ILAC organization had created through NEI's formal stakeholder membership in the organization. Under the proposed methodology outlined in Section 7.2, "Verification that the SIL Certification Process Continues to be Consistent with NRC Endorsed Practices," there is no parallel discussion of how NEI and the nuclear industry would formally affect changes to the ISO or IEC standards central to this report other than a statement that the IEC 61508 standard will be periodically reviewed and comments provided to IEC for consideration. There is no discussion regarding ISO 17065 in this regard. Describe what formal methods have been established to ensure issues identified by NEI, NRC licensees, or third-party dedicating entities will be resolved by the ISO and IEC organizations.</p>	<p>Clarification</p> <p>QA Oversight</p>
28	Page 34, Section 7.3	<p>Section 7.3, "Verification that Implementation of the IEC 61508 SIL Certification Process Continues to be Consistent with NRC Accepted Practices," states in part, that the U.S. nuclear industry observations will be performed initially on a 3-year frequency with the possibility of reducing the frequency if it is observed that the process is demonstrably consistent. The initial 3-year frequency is consistent with the guidance in NRC RGs 1.28 and 1.144 for auditing. However, this appears to be inconsistent with the requirement for 5-year assessments described in Section 5.5 of the report (see comment to Section 5.5, Paragraph 3).</p>	<p>Suggestion</p> <p>QA Oversight</p>