Steven Arndt's Comments on Draft NEI 17-06 Revision B, "Guidance on Using IEC 61508 SIL Certification to Support the Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Related Applications"

General Comments

1) One of the key concerns I have with this process, is that if we approve this, we will not have access (for review, audit or inspection) the key software development documentation, needed to demonstrate that the products key dependability characteristics. For this to be effective we need to be able to have (along with the certificate of SIL certification) the supporting documentation (safety case documentation). This does not need to include everything, just enough to support the certification.

The point of evaluating the accreditation process is to establish a chain of trust down to the level of the OEM's development process. The chain looks like this:

- The IEC 61508 requirements have been determined to be technically adequate to provide reasonable assurance of dependable operation, in terms of systematic integrity
- The CB's processes have been verified to be adequate to confirm the OEM has complied with the requirements of IEC 61508
- The AB's processes have been verified to be adequate to confirm the CB is competent and consistent in their reviews of OEMs

By having confidence in the standard, the CBs, and the ABs it removes the need to have access to the details that support the CBs' determinations. This is also why we don't need to observe the CBs performing any audits of the OEMs.

2) Another concern is the statements through out NEI 17-06 (including in section 1.1 Purpose) that the process would rely on the SIL certification in lieu of conducting a commercial grade survey and a critical design review. The concern is that although using the evidence of a SIL certification to demonstrate the acceptability (i.e. the commercial grade survey is reasonable complete and acceptable) it cannot be used in lieu of the critical design review. These are not the same thing. A commercial grade survey is an acceptance method to assure that the critical characteristics are adequately controlled. The critical design review identifies the criterial characteristics and needs to be reviewed outside of the SIL process. In section 2.2 the report seems to agree, but in section 1.1) it does not.

We agree that the CDR and the CGS are two different types of activities, but in the context of dependability critical characteristics the SIL certificate does address both. For the CDR, the SIL certification process provides confidence in the technical aspects of the OEM's process, then for the CGS, the accredited SIL certificate confirms acceptability of the dependability critical characteristics. The aspect of determining the critical characteristics is accomplished through a

technical evaluation (per EPRI 3002002982). The CDR can contribute to the technical evaluation but it is not mandatory for determining the critical characteristics.

3) The information presented in Section 3, is not enough. It discusses the EPRI research but does not provide very much of the supporting analysis or data that would be adequate for NRC to be able to endorse this approach. Section 3 is a "what we did" report of the EPRI research, not the needed summary of the evidence and analysis that lead to the conclusions that the SIL process will be adequate.

It is very important for the NRC to be familiar with the EPRI report. It is not possible to include all the relevant content in the NEI report.

4) There needs to be more discussion of which SIL (2 or 3) needs to be chosen for which nuclear power plant application and how that is done for this process. There does not seem to be any discussion of this in the current document.

No specific SIL is being prescribed intentionally. Any SIL is potentially valid to satisfy the EPRI TR-106439 dependability critical characteristics. The NRC Safety Evaluation Report of EPRI TR-1064339 explains how a graded approach is to be utilized that is based on safety significance and complexity. The implementation of the graded approach is them documented as engineering judgement for achieving reasonable assurance.

5) There seems to be not discussion in the document (maybe it is in the EPRI report) about the differences between the use of components in nuclear applications and non-nuclear applications (different operation environments, different times between damages for on demand systems, different surveillances requirements, etc.). To determine that this process will work for basic components in nuclear applications this should be evaluated.

Those are qualification aspects that are outside the scope of this effort. Typically IEEE 323 based methodologies apply.

<u>Specific Comments</u>

1) In section 1.2, regulatory basis, NEI spends a lot of time quoting from other documents. This does not add anything to the discussion and is hard to follow (because in some cases the quotes are not complete).

We can look at updating that section.

2) In section 1.3, the third paragraph that start "Based upon the conclusion that…" is circular logic. The first sentence should be rewritten.

We will look at rewording that sentence.

3) At the end of section 2.2 there is a discussion of Table 4-1 in EPRI TR 106439. This table should be included in the document for ease of reading.

The relevant information from Table 4-1 is already summarized within the text of section 2.2. Table 4-1 is four pages long and would be difficult to include.

4) In section 3.1 there was a statement in the last paragraph that EPRI had analyzed the information they had developed to assess the level of validity and the measurable level of safety reliability afforded to the SIL process. More information on this analysis in this document would help support the conclusions that the SIL process can be used as described.

This analysis is described in more detail in section 3.2, but ultimately reference to the EPRI report is necessary because it is an important technical reference for this project.

5) In section 4.2, Figure 4-2 needs to be further discussed. The use of the SIL certification to replace implement the method 2 and 4 acceptance strategy is clear, but it is not clear how it will replace the dependability review earlier in the process.

Table 4-2 of NEI 17-06 is an enhanced version of Table 4-1 of EPRI TR-106439. The third and fourth columns of Table 4-2 of NEI 17-06 are meant show the correlation of the SIL certification with Method 2, 4, and the design review. Section 4.2 will be reviewed for opportunities to better clarify and explain this.