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.
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.
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.
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.
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.

Specific Comments

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).

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