

Need For NRC to Further Qualify or Modify its Endorsement of NEI 01-01

- History
- Background
- LaSalle 10 CFR 50.59 for Rod Control Management System and IN 2010-10
- Harris 10 CFR 50.59 for Implementation of Complex Programmable Logic Device (CPLD)-Based Replacement Cards
- NRC Concerns with respect to NEI 01-01
- Discussion of Regarding the NRC staff's future endorsement of NEI 01-01

History

- In 2002 “Guideline on Licensing Digital Upgrades, TR-102348 Revision 1, NEI 01-01: A revision of the EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule” was published
- Later in 2002 NRC endorsed NEI 01-01 in Regulatory Issue Summary (RIS) 2002-22
- As part of NEI 01-01’s Summary the reasons for updating were given as 1) the revision of 10 CFR 50.59 and 2) the availability of new regulatory guidance.
- Since NEI 01-01 was published many plants have included NEI 01-01 in their procedures for evaluating digital upgrades
- After the conclusion of the Digital I&C Project in 2011, the NRC and NEI identified a number of issues to continue to work on including the 10 CFR 50.59 process and the guidance in NEI 01-01
- In December 2012 NRC again brought up the need to update/revisit NEI 01-01

Background

- Since the publication NEI 01-01 there has been a significant number of new regulatory guidance documents, and agency positions published (as a result of plant upgrades using digital systems). These include ISG-04, ISG-06, the software quality regulatory guides (Regulatory Guide 1.168, 1.169, 1.170, 1.171, 1.172, 1.173), Regulatory Guide 1.152, BTP-07-19.
- In addition to changes in regulatory guidance we also have operating experience (LaSalle 50.59 for Rod Control Management System and Harris 50.59 for implementation of Complex Programmable Logic Device (CPLD) Based Replacement Cards) that indicates the guidance in NEI 01-01 is not always being correctly interpreted.

LaSalle 10 CFR 50.59 for Rod Control Management System and IN 2010-10

- In December 2009, NRC inspectors identified a concern regarding the replacement of an analog-based rod control management system (RCMS) with a computer-based system at LaSalle County Station, Unit 2.
- The RCMS is a nonsafety system; however, it is important to safety because it directly affects core reactivity.
- The inspectors determined that the licensee had not properly evaluated NEI 01-01, Appendix A, “Supplemental Questions” associated with software common-cause failure and the potential for spurious, uncontrolled simultaneous withdrawal of four control rods.
- During discussions with the inspectors, the licensee stated their belief that a software common-cause failure did not need to be considered in the 10 CFR 50.59 evaluation, based on the guidance in NEI 01-01, Section 4.4.6.

LaSalle 10 CFR 50.59 for Rod Control Management System and IN 2010-10

- The licensee interpreted NEI 01-01, Section 4.4.6. to allow changes if the likelihood of a software common-cause failure could be justified as sufficiently low because of the high quality of the software application
- The licensee incorrectly determined that the software quality was sufficiently high to provide reasonable assurance that the likelihood of software failure was not creditable and therefore the digital upgrade would not require prior NRC review on the basis of software common-cause failures
- The licensee implemented compensatory actions to mitigate the consequences of a software common-cause failure of the RCMS.
- IN 2010-10 stated the staff's intent to further qualify the endorsement of NEI 01-01 to address the issues discussed in the IN

Harris 10 CFR 50.59 for Implementation of Complex Programmable Logic Device (CPLD) Based Replacement Cards

- Earlier this year, NRC inspectors identified a concern with the 10 CFR 50.59 evaluation associated with a modification that implemented Complex Programmable Logic Device (CPLD) based replacement cards for the Solid State Protection System (SSPS) at Harris.
- The SSPS circuit boards provide the coincidence logic to produce actuation signals for operation of the reactor trip and engineered safety features of the reactor protection system. Unlike the original SSPS boards, which use fixed logic devices, the replacements SSPS boards use CPLD technology.
- The CPLD-based SSPS boards (CPLD boards) require the use of software tools to develop an application-specific software (data file), which resides in the memory of the CPLD, that program the boards' logic to perform a desired function.

Harris 10 CFR 50.59 for Implementation of Complex Programmable Logic Device (CPLD) Based Replacement Cards

- The inspectors identified concerns with the licensee's the 50.59 evaluation. For instance the CPLD boards contained software, but the 50.59 did not address the quality of the software
 - The licensee did not perform engineering evaluations addressed in Section 4.4.6 and described in Chapter 5 of NEI 01-01 to evaluate the quality and design processes to determine if there is reasonable assurance that the likelihood of failure due to software was sufficiently low
 - These evaluations are necessary to assess whether failures due to software, including software CCF, need to be addressed further

Harris 10 CFR 50.59 for Implementation of Complex Programmable Logic Device (CPLD) Based Replacement Cards

- The inspectors found that the licensee did not perform defense-in-depth and diversity (D3) analysis and software CCF engineering evaluations
 - These evaluations are required by 3.2.2 of NEI 01-01 and should have been preformed for the Human Systems Interface (HSI) functions.
 - Section 3.2.2 states in part, that for digital modifications, the D3 aspects of the upgraded design are analyzed to assure that where there are potential vulnerabilities to software CCF, the plant has adequate capability to cope with them.
- Failure to address D3 and software CCF prevented the licensee from being able to demonstrate that the new CPLD boards did not create the possibility of a malfunction the SSPS with a different result from that analyzed in the UFSAR.

NRC Concerns with Respect to NEI 01-01

- NEI 01-01 Definitions
 - Although current at the time, the change in technology, particularly associated with more extensive use of CPLD's and FPGAs, and the more extensive use of software tools to support both software based systems and logic devices, has left some definitions in NEI 01-01 in need of revision
 - These definitions include hardware, firmware, computer, computer program, diversity, defense-in-depth and software tools
- References to NRC Guidance and Discussion of the Guidance
 - As a result of the NRC Digital Instrumentation and Control Project and routine guidance maintenance a significant number of NRC guidance documents referenced in NEI 01-01 have changed. These include Regulatory Guides 1.152, 1.168-1.173, ISG-02, ISG-4, ISG-6, BTP-07-19, etc.
 - Of particular concern is the interpretation of “simple devices” in BTP-07-19
 - Regulatory positions taken associated with the Wolf Creek FPGA implementation, SERs on software tools, etc.

NRC Concerns with Respect to NEI 01-01

- As a result of the experience from the LaSalle and Harris 10 CFR 50.59 inspections it is clear that some of the guidance in NEI 01-01 is not being interpreted in a way that leads to appropriate application of 10 CFR 50.59.
 - A Diversity and Defense-in-Depth analysis must be performed and appropriate design decisions and support 10 CFR 50.59 analyses criteria must be examined (Sections 3.2.2, 4.4.6 and Appendix A)
 - It appears that licensees may be interpreting the NEI 01-01 to exclude from consideration software common-cause failure vulnerabilities based on a high-quality software design, implementation, and verification and validation program.
 - Section 3.2.2 states in part, that for digital modifications, D3 is analyzed to assure that where there are vulnerabilities to software CCF, the plant has adequate capability to cope. However, it also contains language that can be interpreted as not requiring a D3 analysis for software deemed to have low likelihood of failure.

NRC Concerns with Respect to NEI 01-01

- There are a number of examples (such as Example 4-1) and text (section 4.3.2) that may provide misleading direction associated with screening out of systems with software
 - “In such a case, even when it affects redundant systems, the digital upgrade would screen out.”
- Even though the example given is appropriate, the extension to all other systems may not be, and needs to be updated to more appropriately support current applications

Discussion

- Because of ongoing challenges with the interpretation of NEI 01-01, changes in regulatory guidance since its endorsement, and the wide-spread use of new technology, NRC plans to further qualify or modify its endorsement of NEI 01-01 (RIS 2002-22)
- Several paths are being considered:
 - Re-endorsing NEI 01-01 with additional regulatory positions to provide additional clarity to guidance associated with the difficulties that have been experienced
 - Endorsement of an updated version of NEI 01-01 that addresses all changes to regulatory guidance, new technology, and lessons learned from LaSalle and Harris
 - A combination of the above two options in which, the NRC, in the short term further qualifies its endorsement, while a new version is developed