November 5, 2013

Anthony Pietrangelo
Sr. Vice President & Chief Nuclear Officer
Nuclear Energy Institute (NEI)
1201 F Street, NW, Suite 1100
Washington, DC 20004

SUBJECT: SUMMARY OF CONCERNS WITH NEI 01-01

Dear Mr. Pietrangelo:

On July 31, 2013, staff from the U.S. Nuclear Regulatory Commission (NRC) participated with representatives from the Nuclear Energy Institute (NEI) and industry in a periodic Category 2 public meeting. The purpose of the meeting was for the NRC staff and industry to discuss ongoing activities in the area of digital instrumentation and control (DI&C). Meeting presentations and attendee lists can be found in the Agencywide Document Access and Management System (ADAMS) package for the meeting (ADAMS Accession No.: ML13193A229). A copy of the notice and agenda can be found in ADAMS Accession No. : ML13193A231.

One of the topics discussed at the meeting covered the NEI guidance document NEI 01-01, "Guideline on Licensing Digital Upgrades: EPRI [Electric Power Research Institute] TR [Technical Report] -102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 [Code of Federal Regulations, Title 10, Section 50.59, "Changes, tests and experiments"] Rule." NEI 01-01 is endorsed in Regulatory Issue Summary (RIS) 2002-22, "Use of EPRI/NEI Joint Task Force Report, 'Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: a Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule'," (ADAMS Accession No.: ML023160044). The NRC staff discussed the application of 10 CFR 50.59, "Changes, Tests, and Experiments," for the LaSalle County Station rod control management system (see Information Notice (IN) 2010-10, "Implementation of a Digital Control System Under 10 CFR 50.59," ADAMS Accession No. : ML100080281) and the Harris application for the Complex Programmable Logic Device (see Unresolved Item No. 05000400/2013002-03, "Solid State Protection System Digital Modification," on page No. 18 of enclosure in ADAMS Accession No. : ML13120A340 – Portable Document Format (PDF) page 24 of 48; Shearon Harris Inspection Report, ADAMS Accession No. : ML13224A290).

The presentation identified NRC staff concerns with NEI 01-01. The general concerns reported in the NRC staff presentation included: the need for revisions of definitions in NEI 01-01; changes in NRC documents referenced in NEI 01-01; the interpretation of NEI 01-01 is not leading to the appropriate application of 10 CFR 50.59; and clarifications in the Safety Evaluation associated with RIS 2002-22.

NRC specific concerns with NEI 01-01 are listed in the enclosure to this memo.

If you have questions or require additional information, please feel free to contact, Norbert Carte at (301) 415-5890 or Norbert.carte@nrc.gov.

Sincerely,

/RA/

John Thorp, Chief
Instrumentation and Controls Branch
Division of Engineering
Office of Nuclear Reactor Regulation

Enclosure
Summary of Concerns

CC: Kati Austgen – NEI Project Manager, New Plant Licensing
John Butler, NEI
Gordon Clefton, NEI

NRC specific concerns with NEI 01-01 are listed in the enclosure to this memo.

If you have questions or require additional information, please feel free to contact, Norbert Carte at (301) 415-5890 or Norbert.carte@nrc.gov.

Sincerely,

/RA/

John Thorp, Chief
Instrumentation and Controls Branch
Division of Engineering
Office of Nuclear Reactor Regulation

Enclosure
Summary of Concerns

CC: Kati Austgen – NEI
John Butler, NEI
Gordon Clefton, NEI

DISTRIBUTION JHolonich SStuchell

ADAMS Accession No.: ML13298A787

OFFICE	DE EICB	RES	NRO	NRR/DE	NRR/DPR/PLPB	DE/EICB/BC
NAME	NCarte	PRebstock	DTaneja	SArndt	AMendiola	JThorp
DATE	10/25/2013	10/29/2013	10/28/2013	10/29/2013	11/01/2013	11/05/2013

OFFICIAL RECORD COPY

Summary of Staff Concerns Related to NEI 01-01,"Guideline on Licensing Digital Upgrades: EPRI TR-102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 Rule."

This attachment does not constitute a comprehensive discussion of all U.S. Nuclear Regulatory Commission's concerns (NRC) with NEI [Nuclear Energy Institute] 01-01,"Guideline on Licensing Digital Upgrades: EPRI [Electric Power Research Institute] TR [Technical Report] - 102348, Revision 1, NEI 01-01: A Revision of EPRI TR-102348 to Reflect Changes to the 10 CFR 50.59 [Code of Federal Regulations, Title 10, Section 50.59, "Changes, tests and experiments"] Rule," but rather that it constitutes a set of current highlights or selected issues, for consideration and discussion purposes.

1) Although current at the time, the change in Instrumentation and Control (I&C) implementation technology, particularly associated with more extensive use of Complex Programmable Logic Devices (CPLDs) and Field Programmable Gate Arrays (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. Of particular concern is the interpretation of "simple devices" in Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," (i.e., NEI 01-01 Examples 5.1 & 5.3 contain a description of a "simple device" and BTP 7-19 contains another. Which is more conservative? Which should be more conservative?).

   Example 5.1 states:

   > "…These failure modes are bounded by what was considered previously for the analog unit: spurious trip or failure to trip. The licensee determines that although the new device employs a microprocessor and associated software to implement the safety-function, there are no new failure modes at the system level and therefore no new or consequences other than what has been considered previously…"

   This example implies that the complexity of the internal software is not the parameter that should be used to determine whether a new failure mode exists, but rather it is the inputs and outputs that is used in the determination of new failure modes. However, BTP 7-19 states that it is the simplicity (i.e., testability) of the software that determines the need to consider Common Cause Failure (CCF). Example 5.1 is silent on CCF, implying that it does not need to be considered if the result of a CCF is the same as the result of a single failure in a single piece of equipment.

   In addition the evaluation criteria in NEI 01-01 Section 4.1.2, "Dependability and Risk of Failure Due to Software," for evaluating the likelihood of Software (SW) CCF are less conservative than those listed in Standard Review Plan (SRP) BTP 7-19.

2) Since NEI 01-01 was published in March of 2002, there have been a significant number of new regulatory guidance documents, revisions to regulatory guidance documents, and new documents regarding agency positions published (as a result of plant upgrades using digital systems). These include Interim Staff Guidance (ISG)-04, "Highly Integrated Control Rooms & Digital Communication Systems," ISG-06, "Licensing Process," the software quality regulatory guides (Regulatory Guide 1.168, "Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1.169,

"Configuration Management Plans for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1.170, "Software Test Documentation for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1.171, "Software Unit Testing for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," 1.172, "Software Requirements Specifications for Digital Computer Software Used in Safety Systems of Nuclear Power Plants," & 1.173, "Developing Software Life Cycle Processes for Digital Computer Software Used in Safety Systems of Nuclear Power Plants"), Regulatory Guide 1.152, "Criteria for Use of Computers in Safety Systems of Nuclear Power Plants," and BTP 7-19. What is the impact of these new versions and documents?

Alternatively, guidance for performing digital modifications could be removed from NEI 01-01, so that NEI 01-01 would not become outdated as quickly. (See also No. 8 below)

3) In addition to changes in regulatory guidance there is also operating experience (LaSalle 50.59 for Rod Control Management System and Harris 50.59 for implementation of CPLD based replacement cards) that indicates the guidance in NEI 01-01 is not always being correctly interpreted (possibly due to the subjectivity of NEI 01-01 criteria). Of particular concern are the Regulatory Positions taken associated with the Wolf Creek FPGA implementation (ADAMS Accession No. : ML090610317), Safety Evaluations (SEs) on software tools, and SW CCF.

4) What is the best way to document the understandings within the SE included in RIS 2002-22 in the new version of NEI 01-01? The SE included in RIS 2002-22 stated:

"…the staff believes that when using the submittal as guidance for the analysis of digital modifications of some safety-significant systems such as the RPS and ESFASs, it is likely these digital modifications will require prior staff review when 10 CFR 50.59 criteria are applied."

"It is the staff's position that there are no established consensus methods for accurately quantifying the reliability and dependability of digital equipment."

Note: 10CFR50.59(c)(2)(viii) states: "[A licensee shall obtain a license amendment pursuant to Sec. 50.90 prior to implementing a proposed change, test, or experiment if the change, test, or experiment would:] Result in a departure from a method of evaluation described in the FSAR (as updated) used in establishing the design bases or in the safety analyses."

"Licensees are required under 10 CFR 50.59 to maintain records that 'include a written evaluation which provides the bases for the determination that the change, test, or experiment does not require a license amendment.' Because such judgments may be difficult to duplicate and understand at a later time, it is the staff's position that the basis for the engineering judgment and logic used in the determination should be documented to the extent practicable. This type of documentation is of particular importance in areas where no established consensus methods are available, such as software reliability, dependability of digital systems, and the use of commercial-grade hardware and software that lacks full documentation of the design process."

"3.2.6 Security Considerations
In response to the staff's request at the October 2001 meeting, the submitters added Section 5.3.4.5, "Security Considerations." This section directs licensees to sections in the SRP and endorsed industry standards that address regulatory requirements and guidance for security issues. The staff has reviewed Section 5.3.4.5 and concludes that

it cites the appropriate regulatory requirements and NRC-endorsed guidance and, therefore, is acceptable."

NEI 01-01 Section 5.3.4.5, "Security Considerations" should be modified to clearly address the related NRC concerns in Regulatory Guide (RG) 1.152 Rev. 3, "Technically you should have the title following the number for the first time every RG is referenced," and RG 5.71.

5) Diversity and Common Cause Failures

As explained by the Atomic Energy Commission in the Nuclear Power Reactor Instrumentation Systems Handbook Volume 2 (Available on the internet -Vol.1: http://www.osti.gov/scitech/servlets/purl/4480112 Vol. 2: http://0-www.osti.gov.iii-server.ualr.edu/bridge/servlets/purl/4312290/4312290.pdf) of, "Nuclear Power Reactor Instrumentation Systems Handbook," (see: Section 12-3, "Design Techniques", Sub-Section 12-3.1 "Categories of Failures and Failure Defenses") different design techniques can be used to address different categories of failures. In summary, diversity is one of the design techniques used to address design failures (margin is another). Redundancy and independence are design techniques to defend against single failures of equipment or operation. NEI 01-01 Section 3.2.2, "Software Common Cause Failure," summarizes this discussion by stating:

"The safety model of a nuclear plant is based on an architecture of systems and equipment that uses a combination of multiple echelons of defense-in-depth and redundant equipment. This ensures that the event of an accident or malfunction the plant can be brought to and maintained in a safe state."

However, NEI 01-01 Section 3.2.2, goes on to state the requirement to address single failures:

"The plant is designed to cope with single active failures of hardware components in redundant safety systems…"

Therefore, this first paragraph of NEI 01-01 Section 3.2.2, starts by summarizing the diversity requirement and then transitions to describing the "Single Failure Criteria" without explicitly identifying this transition. The first paragraph then goes on to state:

"…but common cause hardware failures (as a result of design deficiencies or manufacturing errors as discussed in Institute of Electrical and Electronic Engineers (IEEE) 379) are considered beyond the design basis."

This last clause is too general, because, although "common cause hardware failures (as a result of design deficiencies or manufacturing errors as discussed in IEEE 379)" are not considered under the single failure criteria, CCF is addressed, in part, in the regulatory requirements for diversity (e.g., see last sentence of General Design Criterion (GDC) 22, "Protection System Independence,", which states: "Design techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."). In addition, SRM to SECY 93-087 II.Q requires that a D3 analysis be performed (i.e., CCF is part of the design considerations explicitly addressed). However, the analysis criteria for D3 are not the same

as the design basis analysis; the analysis criteria are more similar to the ATWS (10CFR50.62) analysis criteria (i.e., realistic or best estimate).

Traditional I&C safety systems were developed in such a manner that different protective functions were implemented on different equipment (e.g., cards) but with some common aspects (e.g., power supplies, racks, & cabinets). During a digital upgrade, it is possible (and often typical) to implement several (formerly distinct) functions on a common set of equipment. This can potentially weaken the plant's diversity and defense-in-depth (D3) strategy. In addition, the incorporation of software adds an additional aspect to be considered with respect to CCF. Therefore, there is a requirement for a D3 analysis, but not a requirement for a complete set of diverse safety systems. This analysis can be understood to operationally define one acceptable way to determine compliance with GDC 22.

NEI 01-01 Section 3.2.2 does not include design criteria for performance of a D3 analysis, and some have interpreted that a D3 analysis is only required for a "system upgrade" as opposed to multiple "component digitization." Additional guidance is needed in this area.

6) Draft RIS on Embedded Devices

The draft Regulatory Information Summary (RIS) issued for public comment can be found at ADAMS Accession No. ML12248A065. This draft identifies several different examples of components that could include embedded devices:

> "…safety system execute features (e.g., motor control centers, actuated equipment)" "an embedded digital device is a digital component consisting of one or more digital electronic parts that use software, software-developed firmware, or software-developed logic that is integrated into equipment to implement one or more system requirements"
>
> "…include plant systems and components such as emergency diesel generators, pumps, valve actuators, motor control centers, breakers, priority logic modules, and uninterruptible power sources."
>
> "electromechanical timer/relays with microprocessor-based timer/relays."

The examples provided in this draft RIS on Embedded Devices should be explicitly addressed in the Revision to NEI 01-01.

7) NEI 01-01 Section 4.3.2, "Software Considerations," states:

> "…for some upgrades the likelihood of failure due to software may be judged to be no greater than failure due to other causes, i.e., comparable to hardware common cause failure. In such a case, even when it effects redundant systems, the digital upgrade would screen out."

This conclusion is not correct. In the case of Westinghouse reactor protection systems, the RTS and ESF systems contained diverse trip functions that protected against some of the same events (See WCAP-7306, "Reactor Protection System Diversity in Westinghouse Pressurized Water Reactors," dated April 1969). Therefore, hardware CCF (e.g., a

hardware design error) in a particular card type would not disable the protection of the public. If one of these systems were replaced with a digital system where all of the protective functions were implemented in a single software entity, then this diverse protection would be reduced (i.e., there is probably one or more components or parts that are identical in both redundancies).

8) Two topics: (1) Guidance for Digital Modifications, and (2) Guidance for Implementing 50.59.

   NEI 01-01 contains guidance to address two topics: (1) guidance for performing digital modifications in accordance with NRC licensing criteria, and (2) guidance for implementing 10CFR50.59 to determine whether a license amendment is required. It may be better to extract the 50.59 related guidance from NEI 01-01 and incorporate (appropriately modified) it into NEI 96-07, "Guidelines for 10 CFR 50.59 Evaluations," which could be addressed by a revision to RG 1.187 "Guidance for Implementation of 10 CFR 50.59, Changes, Tests, and Experiments." NEI 01-01 could then reference the relevant parts of NEI 96-07. One motivation for reorganizing in this way is that the NRC licensing criteria change much more frequently than do the criteria for performing a 50.59 evaluation.

9) In Sections 4.1 and 4.2 as well as in Figure 4-2 there is an implication that if software common cause failure can be shown to be sufficiently unlikely then a D3 analysis need not be performed. This implied logic is not correct. This erroneous implication/conclusion appears to be based on an incorrect interpretation of NEI 96-07.

10) Traditional analog systems and older digital systems are typically implemented as independent systems. Digital modification can introduce interactions or couplings between previously independent systems (combining functions within a system is addressed by Nos. 5 & 7 above). These couplings in non-safety-related systems can also have an impact on the assumptions in the accident analyses. NEI 01-01 does not include guidance to address increases in coupling/interaction or decreases in independence.

11) Traditional analog systems have failure behaviors that are easier to characterize than complex digital systems. NEI 01-01 does not provide guidance for how to address the failure characterization of digital systems. That is, it is possible to design a single computer controlled system to control equipment associated with several functions. Is it necessary to assume the spurious actuation of all controlled components, in the worst possible way at the worst possible time? Why or why not?