IEEE STD. 1012 AND NEI 96-07, APPENDIX D – STRANGE BEDFELLOWS?

David Hooten
Altran US Corp
543 Pylon Drive, Raleigh, NC 27606
david.hooten@altran.com

ABSTRACT

The final draft of a revision to IEEE Std. 1012-2012, "IEEE Standard for System, Software and Hardware Verification and Validation", is expected to be approved for publication in June 2017. A draft of NEI 96-07, Appendix D, "Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications", has been submitted to the NRC staff for review and endorsement. What, if any, relationship exists between these two documents? How can the nuclear industry utilize the first one to help ensure success when applying the second one? NRC Regulatory Guides only endorse digital system and software related industry standards for application to safety-related systems and components, but the vast majority of digital modifications are made to non-safety related systems and components, so are these industry standards of little or no use when performing digital upgrades to non-safety related equipment? This paper answers these and other related questions and shows how application of a graded approach to verification and validation, utilizing the IEEE Std. 1012 concept of "integrity level", can increase the likelihood of a 10 CFR 50.59 evaluation outcome that does not require prior NRC review and approval for non-safety related digital modifications.

Key Words: verification, validation, 10 CFR 50.59, digital, modifications

1 INTRODUCTION

A revision to IEEE Std. 1012-2012, “IEEE Standard for System, Software and Hardware Verification and Validation”, is expected to be approved in June 2017 and published as IEEE 1012-2017 during the late summer or fall. The Nuclear Energy Institute (NEI) submitted NEI 96-07, Appendix D, Draft Revision 0, “Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications”, to the U.S. Nuclear Regulatory Commission (NRC) on April 4, 2016, requesting that the NRC staff review and comment on the document.

Considering the fact that the vast majority of digital modifications implemented in the US commercial nuclear industry have involved non-safety related systems and components, it appears, at first glance, that these two documents are, for the most part, unrelated. Upon closer examination, however, it can be seen that prudent application of IEEE Std. 1012 during execution of the various life cycle phases of a particular subset of non-safety related digital modifications can significantly contribute to a 10 CFR 50.59 evaluation that results in the licensee being able to implement the modification without prior NRC review and approval. Furthermore, this can be achieved with a verification and validation (V&V) effort of lesser scope, intensity, and rigor than would be required for a safety related digital modification.

This paper seeks to explain the rationale for these assertions after first establishing adequate context for the discussion by providing brief backgrounds on IEEE Std. 1012 and NEI 96-07, Appendix D.

2 IEEE STD. 1012 BACKGROUND

IEEE Std. 1012 is sponsored by the Software and Systems Engineering Steering Committee of the IEEE Computer Society (not by the Nuclear Power Engineering Committee). It was originally published as IEEE Std. 1012-1986, “IEEE Standard for Software Verification and Validation Plans”, and focused on the content of a software V&V plan. Subsequent versions (i.e., IEEE Std. 1012-1998 and IEEE Std. 1012-2004) changed the focus from the software V&V plan to software V&V processes. The scope and title were expanded in the IEEE Std. 1012-2012 revision to include systems and hardware V&V processes, in addition to software V&V processes.

The recently approved IEEE Std. 1012-2017 revision aligns more completely with the terminology and structure of ISO/IEC/IEEE 15288:2015(E), “Systems and software engineering – System life cycle processes” and ISO/IEC 12207:2008, “Systems and Software Engineering – Software Life Cycle Processes”. (This was done by the working group to facilitate making IEEE Std. 1012 an international standard.) No new V&V activities or tasks have been added other than to address the new or modified processes from ISO/IEC/IEEE 15288:2015(E). Some V&V tasks have been rearranged to facilitate understanding and ease of use.

V&V processes are used in conjunction with life cycle processes to determine (1) whether the development products of a given activity conform to the requirements of that activity, and (2) whether the product satisfies its intended use and user needs. These are sometimes casually summarized as “build the product correctly” and “build the correct product”, respectively. V&V supports building quality into the system during the development life cycle. That being the case, V&V is performed in parallel with all of the life cycle phases, rather than at the conclusion of the development process.

IEEE Std. 1012 specifies V&V life cycle process requirements not in a “one size fits all” manner, but for different “integrity levels”, the determination of which establishes the importance of the (system, subsystem, software entity, hardware entity, etc.) based on factors such as complexity, criticality, risk, safety level, security level, desired performance, reliability, or other system-unique characteristics. Users of the standard have the flexibility to define the various software and hardware entities at an appropriate level of granularity for purposes of integrity level assignment. While Annex B provides an example of a risk-based, four-level integrity schema, users of the standard generally have the flexibility to define and document their own integrity schemas. NRC Regulatory Guide 1.168, Revision 2 (which endorses IEEE Std. 1012-2004), however, states, “The licensee or applicant should assign integrity level 4 or the equivalent to software used in nuclear power plant safety systems, as demonstrated by a mapping between its approach and integrity level 4.”

The scope of V&V processes encompasses systems, software, and hardware, and it includes their interfaces. The standard applies to systems, software, and hardware being developed, maintained, or reused (e.g., legacy, commercial-off-the-shelf, non-developmental items). The term “software” also includes firmware and microcode, the inclusion of which encompasses Field Programmable Gate Arrays (FPGAs) and Programmable Logic Devices (PLDs), and each of the terms “system”, “software”, and “hardware” includes documentation. V&V processes include analysis, evaluation, review, inspection, assessment, and testing. V&V personnel actually perform testing under the following conditions:

- Software – all types of testing (component, integration, qualification, acceptance) for integrity levels 4 and 3
- Hardware – qualification and acceptance testing for integrity levels 4 and 3
- Systems – all types of testing (integration, qualification, acceptance) for integrity level 4

V&V personnel review testing under all other conditions for integrity levels 4, 3, and 2. There are no required V&V testing related activities for integrity level 1.

In addition to the general concept of integrity levels, other key IEEE Std. 1012 concepts can be summarized as follows:

- A set of minimum V&V tasks are specified for each integrity level.
- Optional V&V tasks are identified.
- The degree of intensity and rigor applied to V&V tasks can be tailored in accordance with integrity level.
- Detailed criteria are provided for execution of the various V&V tasks.
- The standard now takes a systems engineering viewpoint and is no longer software centric. (Note: This has been an ongoing trend for a number of years with respect to both IEEE and IEC standards. It has also been the subject of recent Electric Power Research Institute (EPRI) Nuclear Sector research, with the publishing, in 2015, of Technical Report 3002005368, "Systems Engineering Methods: A Feasibility Assessment", and, in 2016, of Technical Report 3002008018, "Systems Engineering Process: Methods and Tools for Digital Instrumentation and Control Projects".)
- The standard aligns with international and other IEEE standards.

2.1 US Nuclear Industry Use of IEEE Std. 1012

NRC Regulatory Guide 1.168, Revision 2, which states that it "applies to all aspects of the software life cycle within the system life-cycle context", concludes, "IEEE Std. 1012-2004 provides an acceptable approach to the NRC for meeting the agency's regulatory requirements on the V&V of safety system software with the exceptions and additions listed …" These exceptions and additions pertain to the following areas:

- Software Integrity – Integrity level 4 should be assigned to safety system software.
- Software Reliability – "… the NRC staff's acceptance of quantitative reliability goals for computer-based safety systems is predicated on deterministic criteria for the computer system in its entirety (i.e., hardware, system software, firmware, application, and interconnections)."
- Independence of Software V&V – "… any organization with reviewers performing the verification function should not be part of the design organization's development effort, and should use an independent organizational structure with regard to technical, financial, and managerial independence of its reviewers that is not subject to the budgetary and scheduling constraints of the design organization or project management function."
- Conformance of Materials – The NRC defers to EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications", regarding acceptance of preexisting (i.e., pre-developed) software (e.g., commercial-off-the-shelf software).
- Quality Assurance (QA) – Retention, as QA records, of V&V documentation for safety-related software is driven by NRC regulations, not IEEE Std. 1012.
- Tools for Software Development – The NRC defers to IEEE Std. 7-4.3.2 (as endorsed by NRC Regulatory Guide 1.152, Revision 3) regarding the handling of software tools.
- V&V Tasks – The NRC considers some of the "optional" V&V tasks to be necessary (e.g., audits, regression analysis and testing, security analysis, test evaluation, and evaluation of user documentation).
- Annexes – The informative annexes are not endorsed.

The working group that developed both IEEE Std. 1012-2012 and IEEE Std. 1012-2017 includes several members of the NRC staff, as well as other commercial nuclear industry professionals. To date, the 2004 version of the standard remains the most recent to receive endorsement via NRC Regulatory Guide 1.168. During informal discussions at working group meetings, NRC staff indicated that a revision to Regulatory Guide 1.168 has been drafted that would endorse (with exceptions) IEEE Std. 1012-2017. Whether or not such a revision eventually gets approved and issued remains to be seen.

There is no consensus approach in the US nuclear industry regarding the use of IEEE Std. 1012 on non-safety related digital modifications. A handful of the more critical non-safety related projects (e.g., replacement of analog turbine controls with digital turbine controls) have included V&V activities – most, however, have not. The deciding factor in such decisions is typically project technical risk (since there is no direct regulatory driver) – if new critical digital equipment malfunctions or misbehaves, then the economic consequences can be significant, and well executed V&V can help mitigate this risk. In many cases, however, it has been judged that, considering its additional cost, V&V would not deliver commensurate value toward the project's success. In some cases where V&V was performed, it was done after the design was complete, rather than in parallel with the life cycle phases, resulting in missed opportunities to correct errors and improve weaknesses in requirements specifications *before* application software was developed and other detailed design decisions were made.

3 NEI 96-07, APPENDIX D BACKGROUND

NEI 96-07, "Guidelines for 10 CFR 50.59 Implementation" was originally published in 1996. Revision 1 was issued in November 2000 in response to the NRC's 1999 revision of 10 CFR 50.59, its regulation controlling changes, tests and experiments performed by nuclear plant licensees. The new rule, however, established criteria that are difficult to apply to software based systems; therefore, it was decided that additional guidance to supplement that contained in NEI 96-07, Revision 1 was needed to assist licensees implementing digital modifications. In March 2002, a joint task force of NEI and EPRI published "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" (NEI 01-01 from this point on). This document was subsequently endorsed (with qualifications) by the NRC on November 25, 2002 via Regulatory Issue Summary (RIS) 2002-22.

In a November 5, 2013 letter from the NRC to NEI, concerns were identified with licensee execution of 10 CFR 50.59 activities for several particular digital modifications (both safety and non-safety related examples), and some general concerns were identified, including the following:

- There is a need to revise some of the definitions in NEI 01-01. [Note: Definitions are critical in determining what constitutes a "digital modification" (e.g., as applied to FPGA and PLD based systems).
- There have been changes to some of the NRC documents referenced in NEI 01-01.
- Licensees' interpretations of NEI 01-01 are not resulting in the appropriate application of 10 CFR 50.59.
- Several clarifications in the Safety Evaluation associated with RIS 2002-22 are needed.

In a July 1, 2014 letter from NEI to the NRC, the nuclear industry acknowledged that it shared the NRC's concerns regarding the adequacy and implementation of NEI 01-01 guidance. Working closely with a variety of industry representatives, NEI determined that the content of NEI 01-01, which includes a combination of licensing and technical material, should be separated into two documents, while recognizing the necessity of a certain degree of overlap between them. The licensing oriented document became NEI 96-07, Appendix D, Draft Revision 0, and the technical oriented document, currently being drafted, will become NEI 16-16, "Guidance for Addressing Digital Common Cause Failure".

NEI 96-07, Appendix D provides focused application of the 10 CFR 50.59 guidance contained in NEI 96-07, Revision 1 to activities involving digital modifications. Appendix D includes guidance for performing both 10 CFR 50.59 screens and 10 CFR 50.59 evaluations, but it does not include guidance regarding digital modification design. (Such guidance can be found in EPRI Technical Report 3002002989, "Digital Instrumentation and Control Design Guide", and EPRI Technical Report 3002005326, "Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems".) Appendix D applies to digital modifications involving both safety related and non-safety related systems and components. Appendix D applies to digital modifications that replace either analog or digital equipment. In short, it provides guidance on how to justify and document 10 CFR 50.59 conclusions based on technical input. After the NRC staff's review comments are adequately addressed, it is NEI's intension that Appendix D will supersede NEI 01-01. NEI also intends to request NRC endorsement of the finalized Appendix D in a Regulatory Guide.

4 RELATIONSHIP BETWEEN IEEE STD. 1012 AND NEI 96-07, APPENDIX D

If the 10 CFR 50.59 screening process for a digital modification determines that a full 10 CFR 50.59 evaluation is required, then evaluation criterion #2, "Does the activity result in more than a minimal increase in the likelihood of occurrence of a malfunction of a structure, system, or component (SSC) important to safety?", can pose a challenge, especially if the modification involves custom application software (i.e., "first-of-a-kind" software developed specifically for the digital modification in question). As NEI 01-01 points out, "… there is no consensus method for determining the likelihood of malfunction of software." Consequently, 10 CFR 50.59 evaluation criterion #2 must be addressed qualitatively, at least with respect to the software portion of the modification.

This brings into play the *attributable* and *discernable* criteria described in NEI 96-07, Section 4.3.2, which states, "The effect of a proposed activity on the likelihood of malfunction must be discernable and attributable to the proposed activity in order to exceed the more than minimal increase standard. A proposed activity is considered to have a negligible effect on the likelihood of a malfunction when a change in likelihood is so small or the uncertainties in determining whether a change in likelihood has occurred are such that it cannot be reasonably concluded that the likelihood has actually changed (i.e., there is no clear trend toward increasing the likelihood). A proposed activity that has a negligible effect satisfies the minimal increase standard."

For digital modifications with the potential to affect the likelihood of occurrence of a malfunction of an SSC important to safety (i.e., that satisfy the *attributable* criterion), addressing 10 CFR 50.59 evaluation criterion #2 essentially comes down to determining whether or not the modified system(s) and/or component(s) are less dependable, by more than a negligible amount, than the pre-modified system(s) and/or components (i.e., determining whether or not they satisfy the *discernable* criterion). Such a determination must consider hardware, base software (i.e., the platform software as provided by the original equipment manufacturer before any software configuration or application software development by, or on behalf of, the end user), and application software.

For most commercially available digital instrumentation and control (I&C) equipment, it's not difficult to make the case that the new hardware and the associated base software is at least as dependable, if not more so, than the old analog or legacy digital I&C equipment being replaced. This is due, to a significant degree, to the relatively large installed bases and track records of successful operating history that these digital platforms typically bring to the table. The challenge comes in making that same case with respect to any newly developed application software, which is often "first-of-a-kind" software developed specifically for the particular digital modification in question using base platform software tools that typically involve function block programming or another programmable controller standard programming language.

While the various individual function blocks, which are part of the base software, have widespread use and proven track records, how can one credibly assert that high dependability is achieved by a customized assembly of interconnected function blocks that implement the unique design requirements of a particular digital modification? Application software of this type can appeal to neither a large installed base nor a track record of successful operating history to support a dependability claim.

4.1 Verification and Validation to the Rescue

There has been a longstanding general consensus, across a variety of engineering disciplines, within the commercial nuclear power community that industry standards can, and ought to be, used to demonstrate quality. This notion is supported by NEI 96-07, Appendix D, Draft Revision 0, which states, "Software developed and hardware designed in accordance with a defined process, complying with the applicable industry standards and regulatory guidance does not result in more than a minimal increase in the likelihood of a malfunction." Regarding non-safety related equipment, the document goes on to say, "Although there exists relatively little regulatory guidance for non-safety-related digital equipment, a graded approach for application to non-safety-related digital equipment can provide a significant reduction in the likelihood of a malfunction."

It is currently unknown whether or not this draft Appendix D language will survive the process of NRC review and (possible) endorsement; however, insight into the NRC staff's thinking on the matter may be gleaned from their recently distributed draft RIS 2017-XX, which is intended to update the guidance contained in RIS 2002-22 (i.e., the document that endorsed NEI 01-01). The scope of plant equipment to which RIS 2017-XX applies includes non-safety systems, as well as safety support systems, and excludes reactor protection systems and engineered safety feature actuation systems. Enclosure 2 of the draft RIS provides a qualitative assessment framework that supports the process for drawing several types of conclusions, one of which is a "no" response to 10 CFR 50.59 evaluation criterion #2 (i.e., that the activity does not result in more than a minimal increase in the likelihood of occurrence of a malfunction of an SSC important to safety).

Specifically, Enclosure 2, Table 1 – Qualitative Argument Areas, highlights four general categories of proposed design-related characteristics that need to be evaluated to formulate effective qualitative arguments used in addressing questions such as 10 CFR 50.59 evaluation criterion #2. Important to note is Table 1's statement, "for software, the concern is centered on lower volume, custom or user-configurable software applications" – exactly the same vulnerability identified earlier in this paper. For our purposes, the key area addressed in Table 1 is "Quality". Two of the four description bullets associated with that category are directly supportable by the application of IEEE Std. 1012. They are:

- Compliance with industry codes and standards
- Development process rigor

The first bullet makes it obvious that application of and compliance with IEEE Std. 1012 can contribute to a successful argument when addressing 10 CFR 50.59 evaluation criterion #2 for non-safety related digital modifications. One might point out here that other standards could also be used in support of this bullet; however, the structure and attributes of IEEE Std. 1012 make it particularly well suited for use on non-safety related digital equipment. The V&V effort can be accomplished with less time and cost burden than would be involved for safety related digital equipment due to the standard's built-in graded approach using integrity levels. It is reasonable to believe that most non-safety related digital equipment involved in plant modifications subject to 10 CFR 50.59 evaluations would be classified at integrity level 2 (or possibly 3) in a typical integrity schema. As a result, V&V for equipment of those lower integrity levels would involve fewer tasks and/or a lesser degree of intensity and rigor applied to those tasks that are required to be performed than would be the case for safety related digital equipment.

The second bullet, however, may make the application of and compliance with IEEE Std. 1012 even more significant in contributing to a successful 10 CFR 50.59 evaluation criterion #2 argument. The fact that proper V&V is performed in parallel with all of the development life cycle phases helps ensure that a rigorous development process is both maintained and documented throughout the project. Areas of departure from appropriate execution of the development process could be identified promptly, before errors are propagated to later life cycle phases. Such an approach stands in stark contrast to the typical nuclear industry practice of design verification, which is usually performed after the design is complete and, therefore, is poorly suited to helping ensure development process rigor.

In order to take advantage of the benefits that V&V can provide in support of a 10 CFR 50.59 evaluation, however, the decision to implement IEEE Std. 1012 must be made early in the project. Consequently, it is critical for the licensee to perform a preliminary 10 CFR 50.59 screen as soon as sufficient information is available to support it, so that if a 10 CFR 50.59 evaluation is needed, the decision to perform V&V can be made and development of a V&V plan can begin.

5 CONCLUSIONS

This paper has attempted to demonstrate that the application of a graded approach to verification and validation, utilizing IEEE Std. 1012 with its concept of integrity levels, can increase the likelihood of a 10 CFR 50.59 evaluation outcome that does not require prior NRC review and approval for non-safety related digital modifications. While such an outcome cannot be ensured solely as a result of applying this standard, well executed verification and validation performed throughout the digital equipment's development life cycle can provide a powerful argument in the service of a 10 CFR 50.59 evaluation.

6 ACKNOWLEDGMENTS

The author would like to express his sincere appreciation to those members of the IEEE Std. 1012 Working Group and those members the NEI Digital I&C Regulatory Issues Focus Group who reviewed and provided comments on the draft version of this paper.

7 REFERENCES

1. IEEE Std. 1012-1986, *IEEE Standard for Software Verification and Validation Plans,* Institute of Electrical and Electronics Engineers, New York, NY (1986).
2. IEEE Std. 1012-1998, *IEEE Standard for Software Verification and Validation,* Institute of Electrical and Electronics Engineers, New York, NY (1998).
3. IEEE Std. 1012-2004, *IEEE Standard for Software Verification and Validation,* Institute of Electrical and Electronics Engineers, New York, NY (2004).
4. IEEE Std. 1012-2012, *IEEE Standard for System and Software Verification and Validation,* Institute of Electrical and Electronics Engineers, New York, NY (2012).
5. IEEE Std. 1012-2017, *IEEE Standard for System, Software and Hardware Verification and Validation,* Institute of Electrical and Electronics Engineers, New York, NY (2017).
6. IEEE Std. 7-4.3.2-2003, *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations,* Institute of Electrical and Electronics Engineers, New York, NY (2003).
7. Code of Federal Regulations, Title 10, Part 50.59, *Changes, Tests and Experiments.*
8. NRC Regulatory Guide 1.152, Revision 3, *Criteria for Use of Computers in Safety Systems of Nuclear Power Plants,* U.S. Nuclear Regulatory Commission, Rockville, MD (2011).

9. NRC Regulatory Guide 1.168, Revision 2, *Verification, Validation, Reviews, and Audits for Digital Computer Software Used in Safety Systems of Nuclear Power Plants,* U.S. Nuclear Regulatory Commission, Rockville, MD (2013).

10. NRC Regulatory Issue Summary 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",* U.S. Nuclear Regulatory Commission, Rockville, MD (2002).

11. NEI 96-07, Revision 1, *Guidelines for 10 CFR 50.59 Implementation,* Nuclear Energy Institute, Washington, DC (2000).

12. NEI 96-07, Appendix D, Draft Revision 0, *Supplemental Guidance for Application of 10 CFR 50.59 to Digital Modifications,* Nuclear Energy Institute, Washington, DC (2016).

13. *Guideline on Evaluation and Acceptance of Commercial Grade Digital Equipment for Nuclear Safety Applications,* EPRI, Palo Alto, CA: 1996. TR-106439.

14. *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,* EPRI, Palo Alto, CA: 2002. 1002833.

15. *Digital Instrumentation and Control Design Guide,* EPRI, Palo Alto, CA: 2014. 3002002989.

16. *Systems Engineering Methods: A Feasibility Assessment,* EPRI, Palo Alto, CA: 2015. 3002005368.

17. *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems,* EPRI, Palo Alto, CA: 2016. 3002005326.

18. S*ystems Engineering Process: Methods and Tools for Digital Instrumentation and Control Projects,* EPRI, Palo Alto, CA: 2016. 3002008018.

19. NRC Letter from Mr. John Thorp to Mr. Anthony R. Pietrangelo, NEI, dated November 5, 2013.

20. NEI Letter from Mr. Christopher E. Earls to Mr. John Thorp, NRC, dated July 1, 2014.

21. NEI Letter from Mr. S. Jason Remer to Mr. Lawrence Kokajko, NRC, dated April 4, 2016.