Industry Input to Modernization Plan #3
Scope of 3rd Party Certification for Commercial Grade Digital Equipment

This document is offered as an input to the second public meeting on February 16, 2017 regarding Modernization Plan #3 (Commercial Grade Dedication of Digital Equipment) under NRC SECY-16-0070 (Integrated Strategy to Modernize the Nuclear Regulatory Commission's Digital Instrumentation and Control Regulatory Infrastructure). The purpose is to further clarify industry objectives and desired outcomes on this subject in a form consistent with industry comments on the NRC preliminary draft of the Integrated Action Plan previously presented by industry on April 22, 2016.

1.0 Discussion

The industry's safety culture has embraced the concept that nuclear technology is special and unique. Other process industries, however, can also adversely impact the health and safety of the public. The public, the nuclear industry, and the process industries, in general, all benefit when digital I&C is deployed safely and effectively.

Other process industries have made substantially more progress deploying digital I&C in safety applications than has the nuclear industry. There are certainly multiple reasons for this, but a couple of important and related ones are:

- The relative availability of safety related digital I&C equipment, and
- The existence of a mature and broadly used process by which high quality digital I&C equipment can become certified/qualified for safety related applications.

Nuclear licensees do not have a wide variety of options when it comes to selecting digital equipment for safety related applications. Most digital equipment used in nuclear safety related applications was not designed "from the ground up" under a 10 CFR 50 Appendix B Quality Assurance program; therefore, it must be evaluated and accepted for nuclear safety applications.

This is typically performed, for most equipment, in accordance with EPRI NP-5652, "Guideline for the Acceptance of Commercial-Grade Items in Nuclear Safety-Related Applications"; however, when digital equipment is involved, the process is supplemented through the use of one (or both) of the following:

- EPRI TR-107330, "Generic Requirements Specification for Qualifying a Commercially Available PLC for safety-Related Applications in Nuclear Power Plants"
- EPRI TR-106439, "Guideline on Evaluation and Acceptance of Commercial-Grade Digital Equipment for Nuclear Safety Applications".

Many, if not most, cases of this require first-of-a-kind efforts, involving uncertainties with respect to duration, cost, and overall success. In some cases, the effort is hampered by lack of Original Equipment Manufacturer (OEM) involvement, driven by the fact that the nuclear market is too small to justify the OEM resources necessary to support this process. Many other process industries avoid these

uncertainties by deploying digital equipment certified by an independent third-party to be appropriate for use in systems required to accomplish safety functions of a particular Safety Integrity Level (SIL). SILs are defined and used in several standards, including IEC 61508 (and related 61511) and ISA 84 (similar to IEC 61511). [Note that "Safety Integrity Level", as defined and used in these standards, is unrelated to "Software Integrity Level", as defined and used in pre-2012 versions of IEEE 1012.]

IEC 61508, "Functional Safety of Electrical/Electronic/Programmable Electronic Safety-Related Systems", contains requirements for ensuring systems (including both hardware and software) are designed, implemented, operated, and maintained to provide the required SIL, where each SIL corresponds to a range of target likelihoods of failure of a safety function. The standard was conceived with rapidly developing technology in mind, and its framework is sufficiently robust and comprehensive to cater to future developments. While IEC 61508 defines four SILs, the process industries almost exclusively use only SIL 1 through SIL 3. (For this reason, ISA 84 only includes three SILs.) The standard associates each successively higher SIL with an (approximate) order of magnitude reduction in risk.

The standard recognizes that, because software failure is systematic and not random, qualitative methods must be used in the case of software. SILs are used to define the rigor to be used in the development process. The software requirements apply to both software used in a safety related system and software used to develop a safety related system. These requirements provide details of the software safety life cycle, provide techniques and measures used for software development, and include detailed tables of design and coding standards and analysis and testing techniques used in software development. The requirements are applied using a graded approach that depends on the SIL of the software.

A wide range of manufacturers, system builders, designers, and suppliers of components and subsystems use the standard as the basis for conformity assessment and certification services. The nuclear industry is interested in leveraging these certification services, whereby digital equipment, ranging from a single digital device (e.g., a smart instrument sensor) to an entire digital platform (e.g., a PLC-based system), is certified to a particular SIL level, not by its manufacturer or its supplier, but by an independent, third-party organization having demonstrated expertise in performing such certification activities.

The NRC established regulatory precedent for this concept in 2001 when it issued an SER on a PLC-based platform that leveraged the results of a third-party certification. The staff reviewed the specific V&V performed on the software by TÜV-Rheinland. The TÜV-Rheinland software analysis evaluated measures taken to avoid common mode software failures (with emphasis on examining the software development process quality controls used). The following are direct quotes from this SER:

- "It should be noted, however, that acceptance of the… PLC system is based to a large degree on the TÜV-Rheinland independent review, and any future version of the… PLC system will require an equivalent level of independent V&V in order to be considered acceptable for safety-related use in nuclear power plants."
- "… the staff noted that a significant portion of its acceptance is predicated upon the

> independent review by TÜV-Rheinland and licensees using any… PLC system beyond Version 9.5.3 must ensure that similar or equivalent independent V&V is performed; without this, the… PLC system will not be considered acceptable for safety-related use at nuclear power plants."

In addition, the United Kingdom nuclear regulator already relies on IEC 61508 concepts to deal with embedded digital devices, using a tool called "EMPHASIS" to help evaluate a claim that a digital device is compliant with a particular SIL, as defined in IEC 61508, and to help support a conclusion that the SIL classification is accurate and that the digital device can be used in a nuclear safety application. The UK regulator has accepted safety systems/devices that demonstrate compliance with IEC 61508 SIL 3 requirements.

2.0 Desired Outcome

With respect to evaluation and acceptance of commercial grade digital equipment for nuclear safety applications, the nuclear industry wishes to leverage the infrastructure that currently exists within the process automation world for independent, third-party SIL 3 certification of digital equipment, recognizing that SILs are defined by, and have their context within, the IEC 61508 standard.

A successful outcome with respect to this issue would be the NRC acknowledging that a previously performed SIL 3 certification of commercially available "out-of-the-box" digital hardware and software (i.e., digital equipment as it is received from its manufacturer, prior to any user-specific configuration or application software development) by an independent third-party with demonstrated expertise and experience constitutes an acceptable demonstration of the digital equipment's basic quality. This would include all of the elements within the scope of an independent third-party SIL 3 certification, and it would exclude those elements not within such scope (e.g., seismic qualification). In this scenario, the NRC would continue to review and evaluate how licensees' apply these certified digital platforms and devices in their facilities (including user-specific configuration or application software), as dictated by the existing regulatory framework.

An implication of this outcome is that commercial grade dedication of digital equipment previously certified to SIL 3 would be streamlined. As described in EPRI TR-106439, most mechanical and electrical equipment critical characteristics fall into the "physical" or "performance" characteristic category. These categories also apply to digital equipment, but a third category, "dependability", becomes significantly more important when dedicating digital equipment including software. (EPRI TR-106439 defines dependability as "a broad concept incorporating various characteristics of digital equipment, including reliability, safety, availability, maintainability, and others".)

It's with respect to demonstrating "dependability" related critical characteristics that the nuclear industry seeks to leverage independent, third-party SIL 3 certification of digital equipment, within the NRC-endorsed EPRI TR-106439 process. For digital equipment previously certified to SIL 3, the basic quality of the hardware and software would have already been evaluated and established, thus requiring little or no additional effort. In cases where an entire digital platform (e.g., a PLC-based system) is involved, this would also simplify the associated Topical Report process.

3.0 Implications

The benefits of this proposal include, but are not limited to, the following:

- The acceptance of objective certification criteria for establishing the basic quality of commercially available DI&C equipment.
- It relieves the NRC of the burden associated with ongoing reviews of "out-of-the-box" digital I&C equipment (especially considering the rapidly changing product landscape and short product life cycles).
- It allows the NRC to focus regulatory resources on the application of DI&C equipment to nuclear power plants (which it is uniquely qualified to do).
- It reduces regulatory risk for both licensees and nuclear suppliers.

Nuclear industry recognizes that in order to implement this proposal in a way that benefits all involved, it will have to be explored in detail, including some questions that will require focused research to adequately answer. To that end, EPRI is performing research, starting in early 2017, to explore the efficacy of the independent third-party SIL certification process and to evaluate the basic quality of commercially available digital equipment that has received SIL certification.