As of: 4/25/16 9:26 AM
Received: April 22, 2016
Status: Pending_Post
Tracking No. 1k0-8p7w-9m26
Comments Due: April 24, 2016
Submission Type: Web

PUBLIC SUBMISSION

Docket: NRC-2016-0068
Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure

Comment On: NRC-2016-0068-0001
Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure; Preliminary Draft Action Plan for Comment

Document: NRC-2016-0068-DRAFT-0004
Comment on FR Doc # 2016-07112

3/30/2016
81 FR 17740

(3)

Submitter Information

Name: Jason Remer

General Comment

See attached file(s)

Attachments

04-22-16_NRC_Submittal of Industry Comments on NRC Preliminary Draft of Integrated Action Plan to Modernize DI&C Regulatory Infrastructure

04-22-16_NRC_Submittal of Industry Comments on NRC Preliminary Draft of Integrated Action Plan to Modernize DI&C Regulatory Infrastructure_Attachment 1

04-22-16_NRC_Submittal of Industry Comments on NRC Preliminary Draft of Integrated Action Plan to Modernize DI&C Regulatory Infrastructure_Attachment 2

S. JASON REMER
Director, Plant Life Extension

1201 F Street, NW, Suite 1100
Washington, DC 20004
P: 202.739.8112
sjr@nei.org
nei.org

NUCLEAR ENERGY INSTITUTE

April 22, 2016

Ms. Cindy Bladey
Office of Administration, OWFN-12-H08
U.S. Nuclear Regulatory Commission
Washington, DC 20555-0001

Subject: Submittal of Industry Comments on NRC Preliminary Draft of Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (Docket ID NRC-2016-0068)

Project Code: 689

Dear Ms. Bladey:

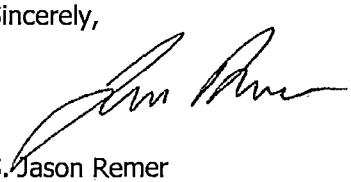
On behalf of the nuclear energy industry, the Nuclear Energy Institute (NEI)[1] appreciates the opportunity to provide comments on the Preliminary Draft of the *Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure* (Docket ID NRC-2016-0068). This draft action plan is in response to Staff Requirements Memorandum (SRM) SECY-15-0106 (ML16058A614) which directs the staff to develop an integrated strategy to modernize the NRC's digital instrumentation and control (DI&C) regulatory infrastructure.

NEI's comments on the draft action plan are provided in two attachments to this letter. Attachment 1 is the executive summary, which provides our overarching comments on the draft action plan and what we consider the significant factors and objectives that the plan must address. Attachment 2 contains a series of appendices that provide discussion, desired outcomes, implications, priority recommendations and a tentative milestone schedule for each of the key regulatory challenge areas referenced in the draft action plan. A cross reference between each appendix and the item in the draft action plan is provided.

[1] NEI is the organization responsible for establishing unified nuclear industry policy on matters affecting the nuclear energy industry, including the regulatory aspects of generic operational and technical issues. NEI's members include all utilities licensed to operate commercial nuclear power plants in the United States, nuclear plant designers, major architect/engineering firms, fuel fabrication facilities, materials licensees, and other organizations and individuals involved in the nuclear energy industry.

NEI looks forward to continued engagement with the staff in support of the development of the DI&C Integrated Action Plan and to address the identified issues in the plan. If there are any questions on this submittal, please contact Stephen Geier (202-739-8111; seg@nei.org) or me.

Sincerely,



S. Jason Remer

Attachment

c: Mr. Robert Caldwell, NRO/DEIA, NRC
Mr. Todd Keene, NRR/DE, NRC
Mr. John Lubinski, NRR/DE, NRC
Mr. Brian Thomas, RES/DE, NRC
NRC Document Control Desk

Attachment 1
April 22, 2016

Industry Comments

DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (Docket ID NRC-2016-0068)

Executive Summary and Overarching Comments

NEI, on behalf of the nuclear industry, provides this summary of our comments to the preliminary draft Integrated Digital Action Plan (DAP), which was issued for public comment on March 30, 2016 (FRN 17740; Docket ID NRC-2016-0068). SRM-SECY-15-0106 directed the NRC Staff to develop an integrated strategy to modernize the NRC's digital instrumentation and control (DI&C) regulatory infrastructure, with a plan provided to the Commission within 90 days of the date of the SRM. To this end, NRC has developed the draft DAP to address a broad context of DI&C regulatory challenges and present policy issues for the Commission to address, including those where significant disagreement on the optimal approach exists.

Within this summary are overarching comments on the significant factors, foundational attributes, and objectives that the DAP should address. Attachment 2 to this letter contains a series of appendices that provide discussion, desired outcomes, implications, priority recommendations, and a tentative milestone schedule for each of the key regulatory challenge areas referenced in the draft action plan. A cross reference between each appendix and the item in the draft action plan is provided.

The industry has reviewed the most recent draft of the DAP in the context of the urgent need to make progress and the importance of the topic as articulated by the Commissioners in the SRM and the accompanying voting sheet comments. While there are many areas of alignment between industry consensus positions and the draft DAP, industry believes there are opportunities to refine the draft DAP to enable greater progress sooner and with greater efficiency. The US nuclear industry is aligned in the belief that removing the barriers that are currently preventing wide application of digital technology is among the most important and urgent needs to support safe and reliable operation of the fleet on a sustained basis.

We want to highlight several issues that, if not implemented effectively and with urgency, will prevent application of digital I&C solutions to modernize nuclear plant infrastructure. These issues include the following, which are discussed in greater detail within the appendices in Attachment 2:

- The resolution of Common Cause Failure (CCF) concerns is the lead technical issue for addressing other issues related to digital I&C, with particular focus on the ability to credit all development practices and deterministic defensive measures within an I&C system that play a part in assuring that CCF will be unlikely.
- The NRC and the industry must reach a common understanding on improved guidance for 10 CFR 50.59 reviews of DI&C upgrades with resolution of the associated challenges, priorities, and potential solutions.

- Adoption of an improved licensing review process for DI&C submittals that would incorporate a phased approach that allows for NRC approvals at each stage to provide improved regulatory certainty aligned with investment decisions.

The principles articulated by the Commissioners in the SRM are sound and, with the implementation of an effective strategy, should provide for the necessary improvements. However, success of this effort should not be measured in terms of simply developing new or refined regulations and requirements that meet the SRM principles- Success must be measured in terms of the bigger picture and the more important objective of enabling and supporting wide-spread application of digital technology in US nuclear power plants.

There are numerous factors that collectively illustrate the need for wide-spread application of digital technology. Most relevant among them are:

- Objective evidence demonstrating that digital instrumentation and controls (DI&C) are more reliable than analog controls and that application of DI&C can greatly reduce the frequency of initiating events.
- Component performance and monitoring capabilities can be significantly increased with digital technology (i.e., accuracy, stability, self-diagnostics, and fault tolerance).
- Equipment obsolescence is an increasingly urgent issue in light of the age of the components in-service coupled with increasing difficulty procuring replacement analog components.
- Analog technology is a small and diminishing market with the resulting diminishment of quality suppliers for replacement equipment.
- The reality of marketplace economic pressures necessitate efficiency improvements and a focus of resources where they be most effectively utilized. Digital technology is a strong lever to improve safety, reliability and efficiency while decreasing operating costs.

From an industry perspective, a new regulatory framework must greatly reduce the risks currently involved with applying digital technology. The resulting regulatory framework must satisfy several key foundational attributes:

- Efficient – not burdensome in balancing safety benefits with cost and schedule impacts
- Unambiguous – removes uncertainty and overlap in requirements
- Timely – processes and approval steps ensure consistency with decision and investment milestones
- Scalable – consequence based and risk informed
- Predictable – clear expectations that guide industry and NRC actions
- Safe – ensures requisite safety in design and operations
- Agile – able to keep pace with evolving technology

- Consistent – facilitates similarity in application across NRC and industry

A regulatory framework that adheres to these criteria is critical to facilitate the industry in making important investment decisions to move forward with DI&C technology. Industry recommends that this vision of success be included in the DAP to support the ultimate objective and guiding principles.

Each element of the draft DAP was reviewed with these success criteria in mind. Our review focused on the following items:

- Do actions address the correct elements of the underlying issues,
- Is the priority of the action consistent with the need,
- Are the strategies likely to yield the mutually desired outcome of enhancing margins of safety
- Are there additional issues of significance that need to be addressed that are absent from the plan.

In summary, there are four elements of the DAP that industry recommends receive additional attention and refinement:

- The DAP priorities are not fully aligned with the needs of industry. In some cases, issues that are considered as high priority in the DAP are less urgent than items that the DAP considers as lower priority.
- In some cases, industry believes the proposed approach is unlikely to yield the desired outcomes, or at a minimum not on the schedule needed. For those instances the approach should be reconsidered and/or additional alternatives considered.
- There are opportunities to consolidate closely related, yet discrete actions into a single effort to improve efficiency, effectiveness, and timeliness of resolution.
- While the DAP may not yet be mature enough to contain specific deliverables and timelines, it can and should reflect a broad outline that defines a clear path to success. Further, it is important that this overall path consider the integration and prioritization of all activities.

Industry comments and suggestions regarding these potential refinements are captured in the attached series of appendices. These appendices, developed by a large and diverse group of industry DI&C stakeholders that included licensees, equipment vendors, and consultants, examine each topical issue in detail, identify alternatives worthy of consideration, enablers, success factors and proposed priority.

Specific to DI&C Regulatory Challenge item 5 in the draft DAP (NEI Appendix I), Cyber Security, NEI believes that this item should be eliminated from the action plan. Further, NEI recommends that the NRC suspend all work on Item 5, halt the development of any guidance, and reallocate those resources to support more pressing DI&C needs. The current regulatory framework is

more than adequate to address safety and security issues associated with DI&C systems. A requirement to implement specific technologies for communications isolation within the design of DI&C systems is unnecessary and would likely have many unintended adverse consequences.

Finally, in addition to these areas for refinement, industry also recommends the DAP include key elements that will provide a management framework for executing the plan. The DAP is essentially a Project Plan for the scope of work requested by the Commissioners in the SRM. To better enable eventual success, industry recommends treating the effort as a project with specific scope, milestones, success criteria, roles and responsibilities, etc. by including elements such as the following in the DAP:

- Vision of success – as described above, industry suggests including a more specific success criteria tied to meeting the ultimate objective of wide spread application of digital technology, not simply new regulations.
- Roles and responsibilities – for key participants, including NRC Staff, NRC Management, and the NRC Digital I&C Steering Committee.
- Interim milestones - for key tasks to enable monitoring progress, along with defined approach to assess progress against those milestones (ideally objectively measureable).
- Priorities – in addition to the high priority task areas to work, the DAP should prioritize the criteria likely involved in the decision-making that will inevitably be required to resolve the full list of issues in parallel.
- Constraints – if there are constraints on options for consideration, those should be clearly defined and articulated in the DAP.
- Gap Analysis – the DAP should include a process to work with the industry to clearly define the current situation as it compares to the vision of success, identify key gaps, and confirm that the planned actions adequately address all gaps/needs.
- Stakeholder participation – industry is poised and eager to support the NRC efforts. The DAP should clearly define the industry role, including NRC expectations of industry (as well as any other stakeholders outside the NRC Staff).
- Conflict Resolution – ideally, all stakeholders will align and effectively achieve the desired outcomes; however, elements of disagreement or differing views on prioritization are likely. The DAP should define in advance the processes/approaches to be used to resolve those conflicts.

NEI appreciates the opportunity to comment on the draft DAP and looks forward to further interactions with the NRC to participate in resolving this critical issue.

Attachment 2
April 22, 2016

Industry Comments

DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure

Table of Contents

Appendix A

Common Cause Failure

1.0 Discussion

The NRC and the industry agree that the resolution of Common Cause Failure (CCF) concerns is high priority and required for resolution of many other issues related to digital instrumentation & control (I&C), as identified by the NRC in the DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure – (Draft Digital I&C Integrated Action Plan, or DAP). However, there is a gap currently between the NRC staff and industry on CCF likelihood, impact, and methods to prevent or mitigate.

As noted in the Draft DAP, the US nuclear industry has been slow to adopt digital I&C systems despite need to replace obsolete analog and early digital components with modern technology. One of the primary barriers is the NRC policy toward on mitigating software (SW) common-cause failure (CCF) in I&C designs. This has led nuclear plants to adopt inferior technical designs in an attempt to respond to NRC concerns with SW CCF. The result has been, in many cases, more expensive and less capable systems that have not fully realized the safety or economic benefits available from digital technology.

The NRC staff has stated that the NRC policy on digital systems CCF is in the Staff Requirements Memorandum (SRM) to SECY-93-087 (Reference 1). This SRM states in part that the "...applicant shall analyze each postulated common-mode failure for each event that is evaluated in the... safety analysis report," and that the "...applicant shall demonstrate adequate diversity within the design".

The staff's interpretation of the policy is expressed in NRC Branch Technical Position (BTP) 7-19, which has evolved to the position that there are only two design attributes that may be credited to eliminate the need for further consideration of CCF: diversity within the digital I&C system, or "testability" based on device simplicity (Section 1.9, BTP 7-19 of Reference 2).

Both the current policy and the staff interpretation do not provide clear means to credit other digital I&C design attributes that are effective in reducing the likelihood of CCF, or allow for an engineering judgment that CCF is sufficiently unlikely that a deterministic analysis of coping is not required.

2.0 Desired Outcome

Nuclear utilities should be able to credit all development practices and deterministic defensive measures within an I&C system that play a part in assuring that CCF will be unlikely. Utilities also need to have efficient methods to demonstrate that unprevented CCFs are bounded by other previously analysed accidents. Potential vulnerabilities should be managed using a combination of defensive measures within the digital system, and mitigative measures and / or coping analysis outside the digital system.

The balance between defensive measures within the I&C system and mitigation or coping

measures outside the I&C system may be based upon engineering judgment, and exact solutions will be situational dependent. The specific defensive measures and how the coping analysis is performed should not be prescriptive. Digital technology continues to evolve, and utilities need to be able to apply current best practices. The proposed outcome is non-prescriptive and technology neutral.

This outcome may be to rescind BTP-7-19, and the section of the SRM to SECY 93-087 related to CCF. Industry anticipates the planned NRC Technical Basis Document on SW CCF will identify the specific NRC documents to be revised or rescinded. Industry welcomes any opportunity to review and provide specific comments on the draft Technical Basis Document.

3.0 Implications

Because the NRC policy via the SRM as interpreted in BTP-7-19 (Reference 2) effectively mandates that the licensee must show that the plant can tolerate a SW CCF, it is challenging for most utilities to evaluate these modifications as acceptable under the 10 CFR 50.59 rule. Arguments for establishing low CCF likelihood have not been accepted by the NRC, so CCF typically is treated as a new malfunction. This conclusion would force many modifications to be submitted as a license amendment request (LAR) under 10 CFR 50.90. In practice, the scope of these reviews has not been limited to how the applicant addressed CCF, but has included detailed review of the entire design per BTP 7-14 (Reference 3) and ISG-06 (Reference 4).

The net effect of the NRC focus on SW CCF discourages digital modifications, and in some cases has resulted in utilities adopting inferior technical designs in an attempt to address NRC concerns regarding SW CCF. For example, Duke Energy's Oconee plant installed diverse actuation for the Emergency Core Cooling System (ECCS) in spite of the very small (and possibly negative) safety benefit, and potential adverse impacts from spurious actuation (see EPRI 1016721). In another example, a utility elected to replace a voltage regulator on their emergency diesel generator (EDG) on only one train, leaving the other train with an analog regulator. In this case, the utility reduced the chance of SW CCF at the cost of reduced reliability on one train of their EDG's. These examples and others can be discussed during future engagements.

Operating experience from the nuclear industry indicates that common cause failures in safety-related I&C systems are unlikely (see EPRI Reports, References 5 and 6). This operating experience also indicates that software faults have not been a dominant contributor to potential or actual CCFs affecting digital I&C in nuclear plants. Multiple hardware failures, failures of shared resources (such as power supplies) and human errors (such as entering incorrect set points) have been more prevalent.

EPRI research has also established that application of diversity in the I&C system, as recommended in BTP 7-19, can have a negative impact on safety through increased design complexity and the potential for spurious actuation of safety systems by the diverse actuation system (see for example Reference 8 and 9). This research also shows that many accident sequences where CCF is considered are bounded by existing plant analyses.

EPRI and others' research shows that extensive testing should not be relied upon as a sole CCF preventive measure. Testing will not reveal a requirements error or omission, which is a common source of design errors leading to potential CCF. Note that testing is still a very valuable activity simply to reveal design and implementation errors, but its value in reducing software design errors that could lead to CCF is at best debatable.

In many cases, the effect of CCF is bounded by other analyses that have already been done, either as part of the Safety Analysis Report or as part of other beyond-design-basis event analysis, such as fire, earthquake or flooding. EPRI has developed a methodology (Reference 10) to be published in May 2016 that supports this need. Other methodologies, for example IEC 61508 or other industries safety-critical programmable systems standards, should also be acceptable.

Based upon the operating experience and research to date, it is not reasonable for many systems to always assume a SW CCF and then perform a deterministic coping analysis. It is also not reasonable to not allow credit for design practices and defensive measures that can reduce or eliminate the possibility for CCF. If sufficient preventive measures have been implemented to render the expected CCF likelihood low compared to Final Safety Analysis Report (FSAR) events, then assuming a SW CCF and demonstrating coping capability through a deterministic analysis should not be necessary for licensing or 10 CFR 50.59 purposes.

Additionally, if a SW CCF cannot become a significant contributor to plant risk because of the systems it could affect and available mitigative measures, it should not need extensive defensive measures. Furthermore, given the relative rarity to date of SW CCF and the overall robust design of the plants, it is not reasonable to assume a SW CCF occurs during a worst case accident, and then design the entire system around this very rare event to the potential detriment of more frequent events.

4.0 Priority

This is a high priority item with a detailed action plan, and will be closely coordinated with the 10 CFR 50.59 (Appendix B), procurement (Appendix C) and regulatory infrastructure topics (Appendices D & E) covered herein.

5.0 Tentative Level 0 Schedule

- EPRI 3002005326, "Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems", schedule:
  - Publish document – 2Q2016
  - Industry training and workshops – 3Q2016 -2017
  - Update document based on feedback and lessons learned –2018
- NRC CCF policy assessment schedule:
  - Complete evaluation of existing position and regulations related to common mode failures - 2Q2016

- Engage industry and public stakeholders in workshops and targeted meetings to gather insights on key technical and policy issues - March 21, 2016 (actual) with additional meetings in 2Q2016
- Prepare a technical basis document to summarize the evaluation of current NRC position and regulations - July 2016
- Present Technical Basis to the ACRS - July 2016
- Request independent peer review of technical basis - August 2016
- Request general comments from the public - August 2016
- Receive comments from independent reviewers - August 2016
- SECY paper to the Commission identifying proposed action to modify or affirm existing position - TBD
- Implement resolution identified in SECY paper TBD

6.0 References

Following is a list of references used throughout this document.

1. SECY-93-087, "Policy, Technical and Licensing Issues Pertaining to Evolutionary and Advanced Light-Water Reactor (ALWR) Designs," U.S. Nuclear Regulatory Commission.

2. NUREG-0800, SRP Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth in Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission.

3. NUREG-0800, SRP Branch Technical Position (BTP) 7-14, "Guidance on Software Reviews for Digital Computer-Based Instrumentation and Control Systems," U.S. Nuclear Regulatory Commission.

4. Digital I&C ISG-06, Revision 1, "Interim Staff Guidance Associated with Digital Instrumentation & Controls, Task Working Group #6, Licensing Process," U.S. Nuclear Regulatory Commission.

5. EPRI 1016731, "Operating Experience Insights on Common-Cause Failures in Digital Instrumentation and Control Systems," EPRI Palo Alto, CA (December 2008).

6. EPRI 1022986, "Digital Operating Experience in the Republic of Korea," EPRI Palo Alto, CA (November 2011) .

7. NUREG/CR-6928, "Industry-Average Performance for Components and Initiating Events at U.S. Commercial Nuclear Power Plants," U.S. Nuclear Regulatory Commission (February 2007).

8. EPRI 1019183, "Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants," (December 2009).

9. EPRI 1016721, "Benefits and Risks Associated with Expanding Automated Diverse Actuation System Functions," (December 2008).

10. EPRI 3002005326, Rev. 1 Draft, "Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems," Electric Power Research Institute Report, November 2015.

Appendix B

10 CFR 50.59 Guidance

1.0 Discussion

NRC and industry stakeholders agree that NEI 01-01, the current guidance for implementing Digital I&C (DI&C) upgrades under the regulatory change requirements of 10 CFR 50.59 has been a continuing challenge. There is a need for clarity and alignment of industry and NRC understanding on the proper use of guidance during industry execution of the 10 CFR 50.59 process for DI&C plant modifications. NEI committed to developing supplemental guidance for digital modifications and submitted NEI 96-07, Appendix D, to the NRC on April 4, 2016 for review and approval.

Secondary issues with this item include the scope of the CCF policy, versus the range of Structures, Systems and Components (SSCs) that fall under the scope of 10 CFR 50.59. Changes made under 10 CFR 50.59 are reviewed based on adverse impact to design functions of SSCs described in the FSAR without consideration for the CCF policy which imposes different requirements and assumptions on the credibility or likelihood of CCF for those items in scope. The 10 CFR 50.59 regulation and guidance do not differentiate between safety and non-safety and certainly not between protection and safety.

2.0 Desired Outcome

Industry desire for the outcome of executing the plan is to reach a common understanding of the DI&C challenges, priorities, and potential solutions to develop guidance for 10 CFR 50.59 reviews of DI&C upgrades. This includes improving the clarity for assessing common cause failure and associated criteria applied in 10 CFR 50.59 reviews. In addition, the desired outcome is for the NRC to endorse NEI 96-07, Appendix D, as an acceptable method for addressing the digital specific issues associated with 50.59.

- NRC endorsement of NEI 96-07, Appendix D.
- Acknowledgement from the NRC (including appropriate coordination with regional inspectors) that, for many digital changes, a CCF susceptibility analysis can demonstrate that likelihood of CCF can be reduced to acceptable levels through preventative and limiting measures in the design and application of digital technology, such that CCF may be considered no more likely than those other failures currently considered in the licensing basis and the associated digital modifications can be accomplished without prior NRC approval.
- Consistent and robust digital 50.59 reviews by licensees, using the new endorsed guidance. The guidance includes examples of acceptable and adequate screens/evaluations to improve industry consistency in documenting the 50.59 reviews.

Success is measured by licensees implementing needed digital upgrades that do not require NRC prior approval while following clear guidance provided by NEI 96-07, Appendix D.

3.0 Implications

In the absence of clear guidance with respect to digital modifications, many needed important to safety digital projects are on hold, or are being planned as less capable analog projects, due to the risk from unclear regulatory expectations.

Many of these waiting changes are to safety related support systems and not large scale protection system upgrades, such as; safety related chillers, emergency diesel generator voltage regulator controls, and post-accident monitoring systems.

Unless a clear regulatory path to implement more digital modifications under 10 CFR 50.59 and without prior NRC approval is identified, the industry and NRC will remain reactive, implementing digital modifications only when necessary to maintain safety, rather than proactively utilizing digital technology to continuously improve safety.

4.0 Priority

This is a high priority item with a detailed action plan, and will be closely coordinated with the digital CCF issue.

5.0 Tentative Level 0 Schedule

- Obtain NRC alignment with NEI 96-07, Appendix D – 2Q2016
- Begin preparations for training workshops and industry/NRC rollout – 3Q2016
- NRC enter Regulatory Guide endorsement process for NEI 96-07, App. D – 3Q2016
- NRC issue a letter endorsement while RG is processing (to facilitate effective guidance rollout) – 3Q2016
- Conduct industry and NRC workshops to rollout guidance and transition to implementation – 2017
- NRC issue RG endorsement for NEI 96-07, App. D – 3Q2017

Appendix C

Digital Device Procurement

1.0 Discussion

There exists a gap in the DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure – (Draft Digital Action Plan, or DAP) in the area of procurement of digital devices involving commercial grade dedication (CGD) of digital equipment, which is not currently within the scope of the plan. This appendix addresses that gap and includes regulatory issues related to embedded digital devices.

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 undergo CGD.

CGD 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 CGD's for digital equipment are 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 the CGD 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 in 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 (approximately) 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.

2.0 Desired Outcome

The nuclear industry is proposing independent, third-party SIL 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 entrusting certification (for use in nuclear safety related applications) of "out-of-the-box" commercially available 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) to independent third parties with demonstrated expertise and experience. This would include all of the elements within the scope of an independent third-party SIL 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 licensees' applications of certified digital platforms and devices, 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 could be performed using only EPRI NP-5652 (i.e., it would no longer need to be performed using either EPRI TR-106439 or EPRI TR-107330). In other words, it could be performed using the same process as other, non-digital equipment because the basic quality of the "out-of-the-box" hardware and software would have been previously established and certified. In cases where an entire digital platform (e.g., a PLC-based system) is involved, this would also simplify the associated Topical Report process (see Appendix G).

Another implication is that use, in multiple nuclear plant applications, of digital equipment previously certified to SIL 3 and subsequently having undergone commercial grade dedication, could provide sufficient basis for concluding that software common cause failure (CCF), across multiple instances of the subject digital equipment, is "unlikely" and need not be considered further. This concept would have its greatest applicability when deploying digital devices of limited functionality with only a modest amount of configuration by, or on behalf of, the end user (sometimes referred to as "embedded digital devices").

These types of digital devices are also addressed in draft NRC Regulatory Issue Summary (RIS) 2016-XX, "Embedded Digital Devices in Safety-Related Systems". Regarding its applicability to the "Nuclear Reactor Sector", this draft document emphasizes the fact that embedded digital devices (EDDs) in safety-related applications are subject to the existing digital I&C regulatory infrastructure, just as are safety-related digital protection and control systems, and, therefore, the following must be addressed:

- The need to ensure adequate quality and reliability of EDDs that exist in actuation

equipment.

- The need to address potential vulnerabilities to CCFs.
- The need to ensure sufficient procurement planning and material control to identify, review, test, and control EDDs.

The nuclear industry generally agrees with the main points of this RIS as applied to the "Nuclear Reactor Sector".

3.0 Implications

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

- 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 is uniquely qualified to do).
- It establishes objective certification criteria for "out-of-the-box" DI&C equipment.
- 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, it is recommended that the NRC and EPRI develop a cooperative/shared research plan to facilitate working out the details associated with this proposal.

4.0 Priority

Developing a detailed action plan to evaluate, and then establish within the digital I&C regulatory framework, the proposal to leverage independent, third-party SIL certification of digital equipment for commercial grade dedication, and other purposes suggested in this appendix, is a medium-to-high priority.

5.0 Tentative Level 0 Schedule

- Identify and budget for 2017 investigative and research activities needed to evaluate the proposal regarding independent, third-party SIL certification of digital equipment (NRC and EPRI – 3Q2016)
- Begin investigative and research activities (NRC and EPRI – 1Q2017)
- Complete investigative and research activities (NRC and EPRI – 4Q2017)
- Draw conclusions regarding the proposal and identify regulatory framework changes needed to implement them (NRC and NEI – 2Q2018)
- Implement resulting regulatory framework changes (NRC – 4Q2018)

Appendix D

Regulatory Document Infrastructure

1.0 Discussion

The industry believes that the overall regulatory document infrastructure (regulatory guides, standard review plan, branch technical positions, ISGs, etc.) that applies to digital I&C technology being considered for use in nuclear power plants make it difficult to achieve efficient, effective and consistent staff evaluation of licensing submittals. A full assessment of the Standard Review Plan (SRP) content and organization related to digital I&C (DI&C), and the multiple associated DI&C-related regulatory guidance documents needs to be performed.

The current digital DI&C regulatory framework is overly complex and difficult to navigate. There are both too many total documents and too many types/categories of documents with which licensees must be familiar in order to consistently succeed in executing DI&C upgrades that will pass muster (1) when prior NRC review and approval is necessary, and (2) during post-implementation NRC inspection activities. Significant ambiguity and inconsistency exist across the full spectrum of DI&C regulatory guidance documents that challenge licensees considering significant DI&C projects without undue regulatory and project risk. This has led industry to defer some digital upgrade projects that, if implemented, would have provided significant plant safety improvements.

2.0 Desired Outcome

The desired outcome is a clear, stable, efficient, and predictable regulatory framework which facilitates the deployment of modern I&C equipment without licensee concern of undue regulatory risk. If digital technology is the right choice to achieve high reliability/availability and to overcome equipment obsolescence, licensees should not fear the application of the digital upgrade process because of the construed regulatory morass.

With few exceptions, for each topical area, the regulatory framework should have a single staff review guidance document (which establishes a clear, concise, and verifiable set of requirements) so that licensees understand what the staff needs in order to perform their review. Guidance documents should link to the regulations and GDCs they support, i.e., requirements traceability should be the foundational approach. There should be clear differentiation between regulatory requirements and regulatory guidance. The various document types (BTPs, ISGs, SRMs, RIS, etc.) that contain pieces/parts of the staff's review guidance should be integrated into a single document. Layering documents or issuing successive documents to interpret portions of preceding documents without subsuming those documents only generates further confusion (examples of this may be Information Notices, ISGs, and RIS that address common aspects of regulatory guidance but does not address the guidance in its entirety).

Industry consensus standards should be utilized as the basis for industry technical guidance and

staff review guidance. With few exceptions, these standards should be endorsed without exceptions and caveats. At the same time, industry standards should not be in the regulations since by design, they evolve in 5-10 year increments. IEEE 603, for example, is not written with sufficient clarity to function as a regulatory requirements document.

Well-vetted international standards (e.g., IEC 62671:2013, Nuclear Power Plants - Instrumentation and Control Important to Safety - Selection and Use of Industrial Digital Devices of Limited Functionality) should be endorsed when possible to expedite putting a simpler framework in place. MDEP/CORDEL and other efforts are already working towards harmonizing standards - taking advantage of these efforts add efficiency to the process (e.g., MDEP Common Position 7, "Common Position on Selection and Use of Industrial Digital Devices of Limited Functionality").

The action plan should include steps that ensure the regulatory framework will be consistently applied between the various NRC offices:

- NRR, NSIR, and NRO;
- Headquarters and regional inspection staff.

The industry concurs with the SRM that a modern regulatory framework should apply the following principles:

- Any new or revised requirements addressed in the Draft DAP should be performance-based rather than prescriptive.
- DI&C safety requirements should be technology neutral, however, guidance should be tailored if necessary. In addition, the same requirements should apply to operating and new reactors.
- NRC requirements and guidance should not pose an unnecessary impediment to advancement in nuclear applications of digital technology.

Success is measured by licensees' willingness to invest in modernization of their I&C and other plant equipment selecting technology that is optimal for plant safety and reliability. This selection takes place with a stable and comprehensible regulatory framework providing licensees, OEMs, and regulators a success path with clear NRC review/inspection requirements/guidance as well as clear industry guidance to meet it. Due to the perceived regulatory risk, the current approach is contrary in that licensees find it preferable to invest in reverse engineering of analog technology or maintaining obsolete and no longer supported equipment as a tangible approach that is known to be unsustainable.

3.0 Implications

The Draft DAP regulatory guidance infrastructure modernization effort must take a clean-slate approach when revising the current regulatory framework to address the core issues. While there may be a few critical technical issues and guidance documents that need immediate attention (e.g., CCF, draft NEI 96-07 Appendix D, BTP 7-19, etc.) and should be addressed in the short term, NEI recommends that a a comprehensive assessment of the digital I&C

regulatory framework be performed as a high priority.

As noted previously, the current regulatory framework for DI&C is too complex – too many documents and document types (RIS, ISGs, SRMs, BTP, etc. etc.) containing multiple 'requirements' which often conflict or obfuscate the issue.

An example is in the area of software verification and validation. The comprehensive regulatory framework assessment needs to evaluate the prescriptive nature of the software verification and validation guidance and shift to an approach that is performance-based and technology neutral. The current guidance is fragmented and should be harmonized.

- RG 1.168, Revision 2, endorses IEEE 1012-2004, which defines a very prescriptive microprocessor-based software verification and validation framework, and adds additional requirements.
- RG 1.152, Revision 3, endorses IEEE 7-4.3.2-2003, which has a separate set of software verification and validation requirements.
- BTP 7-14 elaborates on the endorsed IEEE standards with additional review expectations.
- RG 1.28, Revision 4, endorses ASME NQA-1-2008, which has a different set of software verification and validation requirements.

4.0 Priority

Developing a detailed action plan to modernize the current regulatory framework for DI&C is a high priority. While some issues are long in duration, the action plan needs to have short, intermediate, and long term actions.

5.0 Tentative Level 0 Schedule

- Schedule an assessment of the regulatory framework for digital I&C - 3Q2016.
- Develop and implement improvement actions based on the results of the assessment - TBD

Appendix E

Regulatory Infrastructure

1.0 Discussion

DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure – (Draft Digital Action Plan, or DAP), Item #8: The existing process that is used to evaluate proposed alternatives to regulatory guidance and endorsed codes and standards for Digital I&C (DI&C) requires more clarity. Additional clarity would benefit both the NRC review staff and licensee's seeking to pursue an alternative request. The existing process provides generic guidance about what information to include in an alternative request; but is not sufficiently detailed to support preparation of a request which meets the expectations of the NRC staff in an efficient and predictable manner. This can lead to inefficient use of industry and NRC resources and extend the duration of NRC reviews.

An example of an instance requiring an alternative request is an applicant that desires to use IEEE 603-1998 in lieu of IEEE 603-1991, in the design of a DI&C application. As the 1991 standard is explicitly referenced in 10 CFR 50.55a(h)(3), the applicant would need to seek approval of an alternative (in this the 1998 version of the standard), in accordance with 10 CFR 50.55(z).

10 CFR 50.55(z) states:

> *(z) Alternatives to codes and standards requirements. Alternatives to the requirements of paragraphs (b) through (h) of this section or portions thereof may be used when authorized by the Director, Office of Nuclear Reactor Regulation, or Director, Office of New Reactors, as appropriate. A proposed alternative must be submitted and authorized prior to implementation. The applicant or licensee must demonstrate that:*
>
> *(1) Acceptable level of quality and safety. The proposed alternative would provide an acceptable level of quality and safety; or*
>
> *(2) Hardship without a compensating increase in quality and safety. Compliance with the specified requirements of this section would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety.*

As an additional example of current guidance in this area, RG 1.152 contains the following statement (this is typical for many regulatory guides):

> *Applicants and licensees may voluntarily use the guidance in this document to demonstrate compliance with the underlying NRC regulations. Methods or solutions that differ from those described in this regulatory guide may be deemed acceptable if they provide sufficient basis and information for the NRC staff to verify that the proposed alternative demonstrates compliance with the appropriate NRC regulations. Current*

licensees may continue to use guidance the NRC found acceptable for complying with the identified regulations as long as their current licensing basis remains unchanged.

The current requirements and guidance on what is required to be submitted for the basis of a *proposed alternative* is consistently vague and includes immeasurable criteria such as:

- "Sufficient basis and information"
- "Acceptable level of quality and safety"
- "Hardship without a compensating increase in quality and safety"

Draft DAP Item #9: The level of technical detail submitted in license applications, license amendments, and licensing topical reports, as well as the timing and sequence of the technical information expected to be submitted for NRC evaluation during the review cycle should be reassessed and improved.

The level of detail required for DI&C submittals is out of proportion when compared to other types of submittals to the NRC. The current NRC evaluation of digital I&C submittals is based on a detailed review of the design process, the design outputs and partial implementation. Delaying even the first approvals of a digital I&C project until the implementation phase poses too much risk for the licensee, causing regulatory uncertainty and unnecessary delays. A new digital I&C review process should be created and be applicable to changes under 10 CFR 50 and 10 CFR 52. The new process should incorporate some concepts from the existing 10 CFR 52 process where approval (such as a Design Certification) is given long before the implementation and testing phase.

Draft DAP Item #10: Modern nuclear power plant designs typically include a number of I&C systems, with interfaces between them. Often, multiple I&C systems are used in concert, each contributing to the performance of a single function. This means that the overall I&C architecture for a modern plant is a system-of-systems (i.e., it is fully integrated). The integration of I&C systems into a larger architecture is, at the same time, the source of new safety benefits and of new questions regarding potential failure modes and hazards.

The current framework governing regulatory review of nuclear power plant I&C is predicated on a system-by-system review approach which is appropriate for legacy, largely analog, I&C designs with little connectivity between the different I&C systems/entities. It does not acknowledge the overall I&C architecture as a system-of-systems, nor does it address the unique design activities and analyses needed to develop and justify the overall I&C architecture as an entity.

Regulatory requirements and guidance are needed which are developed from the viewpoint of the overall I&C architecture, and address the unique aspects of plant-level I&C design and analysis. This regulatory framework should drive a systematic and coherent approach to documenting the requirements, bases and design decisions that lead to an overall I&C architecture design, as well as specific analyses required to be performed against that architecture design. The availability and evaluation of such documentation will provide

assurance that the chosen I&C architecture design is acceptable in terms of the balance between the benefits gained by integration and the potential hazards introduced.

The NRC began to recognize the importance of I&C architecture with the publishing of the NRC's Design Specific Review Standard (DSRS), written for the mPower design. This DSRS does begin to address the need for regulatory guidance in this area; most specifically in Section 7.0, Appendix B. That appendix identifies some of the important topics related to I&C architecture design, but is lacking in specific guidance for how an applicant can acceptably address those topics (the appendix is only two pages in length).

2.0 Desired Outcome

The industry concurs with the SRM that a modern regulatory framework should apply the following principles:

- Any new or revised requirements addressed in the Draft Digital I&C Integrated Action Plan should be performance-based rather than prescriptive.
- Digital I&C safety requirements should be technology neutral, however, guidance should be tailored if necessary. In addition, the same requirements should apply to operating and new reactors.
- NRC requirements and guidance should be safety focused, support a safety finding based on reasonable assurance of adequate protection, and otherwise not pose an unnecessary impediment to advancement in nuclear applications of digital technology.

Draft DAP Item #8:
A clear and predictable process for proposed alternatives to regulatory guidance with direction for both licensees developing the alternative request and NRC reviewing the alternative request is the desired outcome. The new process should clarify the information required to be submitted for NRC to review and evaluate an alternative request including:

- "Sufficient Basis and Information"
- "Acceptable Level of Quality and Safety"
- "Hardship"

Draft DAP Item #9:
NRC staff review guidance for DI&C submittals which is applicable to both existing plants and new plant designs, and which leverages international standards and best practices is the desired outcome.

The review process should be scalable from single component reviews up to large projects. It is recommended that the review process incorporate phased approvals, consistent with the subject design's lifecycle. The process should include review areas at the overall I&C architecture level (like that detailed below in Item #10 and based on IEC 61513 or similar) as well as at the individual system level using the existing IEEE 603.

I&C reviews should focus on the system level requirements and process, to ensure the change is consistent with the high level requirements designed to evaluate that the change meets the basic requirements. The review should ensure that all hazards have been properly mitigated or prevented. I&C Hardware/Platform reviews and approvals should leverage third party certifications such as Safety Integrity Level as defined in IEC 61508.

The review process should be a phased approach that allows for NRC approval at each stage to provide regulatory certainty. The following is a recommended process.

- The first phase should concentrate on the proposed design requirements and the design process that serves to bound the approval process with NRC approval of the plan.
- The second phase should be a review of the detailed design in accordance with the requirements and plan from phase 1, and end with an SER (with appropriate limitations and conditions as needed).
- The final phase would be the design implementation/test/install phase and could include the inspection by the inspection and enforcement division, within the context of the SER (this should tie to NRC action plan for NRC Action plan item 11 and NEI plan F). There could be ITAAC (Inspections, Tests, Analyses, and Acceptance Criteria) - like or other limitations and conditions in the SER to ensure implementation and testing were performed as described in the license submittal.
- The process should include a provision, similar to the 10 CFR 52 process for departures to address the possibility of changes that impact NRC approvals given at earlier phases in the process.

A re-packaging of the existing process will be unacceptable since it is not in keeping with the requirements of the SRM which called for a process that was less prescriptive and applicable to both operating and new reactors, and the current ISG-06 is very prescriptive, cumbersome, and only applicable to operating plants.

Draft DAP Item #10

The desired outcome is a set of regulatory requirements and guidance which address the following topics for the design of an overall I&C architecture.

- A lifecycle model to govern development and implementation of an overall I&C architecture, which interfaces appropriately to the I&C system software lifecycle models already endorsed by the NRC.
- The derivation of overall I&C requirements from the plant safety and operational bases which include sources such as:
    - Plant accident analyses
    - Plant defense-in-depth concept
    - Design and operational concept of each plant process system
    - Plant maintenance concept and availability targets
    - Human Factors analyses
    - Constraints arising from designated locations of I&C equipment

- The design of the overall I&C architecture including topics such as:
  - Bases for the definition of the systems comprising the architecture
  - Organization of the I&C systems according to lines of defense
  - Allocation of functions to the I&C systems
  - Identification and justification of interfaces
- The identification and assignment of requirements based on the overall I&C architecture design:
  - To the individual I&C systems
  - To the identified interfaces
- The analyses to be performed at the level of the overall I&C architecture, such as:
  - Defense-in-Depth analyses
  - Diversity analyses
  - Independence / Separation analyses

A successful regulatory framework could be similar to (or incorporate portions of) that found in the international standard IEC 61513, which explicitly acknowledges and guides the development of an overall I&C architecture as a predecessor to design of the individual I&C systems For system level changes IEEE 603 may still be appropriate, but since IEEE 603 does not address the overall I&C architecture, furthermore the NRC should make use of the MDEP common position papers, DICWG-09 Common Position on Safety Design Principles and Supporting information for the Overall I&C Architecture.

3.0 Implications

Providing clarification on the "alternative approval" process for DI&C will improve the quality of submittals, the consistency of reviews, and reduce the burden on applicant and NRC. This will also improve the predictability of NRC reviews of DI&C upgrades.

Without a consistent and predictable licensing review process, with agreed upon level of rigor prior to submittal for NRC approval, the industry will continue to make only those changes that can be made within the rules of 10 CFR 50.59 without taking advantage of the improvements available from implementing digital technology for protection systems within the current operating fleet.

A successful regulatory framework could be similar to (or incorporate portions of) that found in the international standard IEC 61513, which explicitly acknowledges and guides the development of an overall I&C architecture as a predecessor to design of the individual I&C systems.

4.0 Priority

This is a medium to high priority for issues 9 and 10 however low priority at this time for issue 8, as alternative requests are not viewed as a major blocking point in the licensing process at this time.

5.0 Tentative Level 0 Schedule

To be developed and integrated into the overall DAP schedule.

Appendix F

Consistency from Licensing to Inspection

1.0 Discussion

The NRC acknowledges industry stakeholder's concern with regulatory positions not always consistent between the NRC Headquarters staff, which performs licensing actions, and the Regional Offices, which perform inspections. This can result in delays and uncertainty for licensees and increases the chance that needed upgrades are not pursued. More upfront agreement and communication on generic Digital I&C (DI&C) technical matters between licensing staff and the regional office inspection staff is required.

The DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure – (Draft Digital Action Plan, or DAP) identified five areas where the staff is considering for short term action. It is industry consensus that inspection inconsistency should have a higher priority and a short term action plan is developed that addresses this issue. This issue has near term impact on new plants inspections and any ongoing digital upgrades under NRC review.

For example, DI&C-ISG-04 was created to address communication independence concerns that supported ongoing projects and new builds. The ISG-04 framework was structured to enable highly integrated control rooms planned for the new build plants. However, the paths taken by NRR and NRO for the same AREVA technology were different. Certain features found acceptable for the Oconee RPS/ES project, were not accepted for EPR project. Furthermore, ISGs were seen as conservative guidance that would enable fast track approvals for those that wanted quicker decisions. However, as the ISGs were revised or incorporated into other guidance documents, the guidance became more conservative, applied in a broader way, and lacked flexibility. In the end, the successes of the Oconee project were never repeated and highly integrated controls rooms have not been accepted. As a result, ongoing design certification reviews and rulemaking proposed to the Commission would have prevented the very things that the original DI&C-ISG-04 effort was designed to enable.

It is industry consensus, that management oversight efforts must continue after any guidance documents are revised to ensure they are implemented as intended. Staff should develop metrics that capture the implementation success that is envisioned by the upgrade project.

2.0 Desired Outcome

The desired outcome is to increase regulatory consistency within the NRC, create an efficient review cycle and prevent inconsistencies in the application of regulation. It is suggested to include actions in near-term action list and develop necessary regulatory guidance and training to ensure there is consistency between various regulatory organizations and branches during the reviews and audits.

DI&C inspection guidance in Inspection Procedure (IP) 52003 should be revised to better define

roles and responsibilities for inspectors. For example IP 52003 states: review the documentation required to gain a working knowledge of the digital I&C modification. The intent is for inspectors to be familiar with the system; not to duplicate previous NRR review efforts.

3.0 Implications

In the absence of clear guidance with respect to consistency of audits and inspections, the regulatory uncertainty will exist that would preclude the digital projects to be initiated and to complete in timely manner. This also precludes in time closure of ITAAC (Inspections, Tests, Analyses, and Acceptance Criteria) for new plants and level of inspection by Vendor Branch and Region.

4.0 Priority

Industry recommends placing this as a near-term priority with a detailed working group action plan.

5.0 Tentative Level 0 Schedule

NRC develop action plan – 2Q2016

NRC implement action plan – TBD

Appendix G

Topical Report Process Improvement

1.0 Discussion

The DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (Draft Digital Action Plan, or DAP) acknowledges that the expenditure of NRC resources for the review of DI&C platform topical reports has not gained the efficiencies in performing licensing evaluations as was originally envisioned. This issue is applicable to both digital upgrades and the new plants. The NRC indicated that during the Oconee RPS/ESF upgrade they encountered a large amount of changes to the platform which required extensive reviews. In general, many of the changes were very minor, and non-technical with the majority not requiring NRC approval if they occurred as a change after the installation. For many topical reports, many years may pass between initial approval of the topical report and the first implementation at a nuclear power plant. Many design and technology changes typically occur during that time due to process revisions, enhancements, and product upgrades. Under current regulatory environment, NRC expects complete review and approval of any changes by the staff. This approach requires significant expenditure of resources by the NRC, vendors and the licensees resulting in the expected efficiency gains by prior topical report approval being lost.

2.0 Desired Outcome

The DAP Item 12 states that a process is needed to effectively and efficiently address updates to topical reports, and to address design changes made to platforms following issuance of the topical report safety evaluation. The desired outcome is to have the NRC recognize that a vendor can use a screening and evaluation procedure to document the assessment to changes in a platform to maintain its original topical report qualification. This will help focus the NRC review on changes that could impact safety. For changes that do not impact safety, reviewing the assessment conducted rather than the platform changes themselves will reduce the staff review time and scope when licensing reviews reference a topical report. In addition, the NRC should integrate the concepts related to SIL certification as discussed in Appendix C to streamline the topical report process and improved the sustainability of issued topical reports.

NRC considers this as a longer term effort to be worked in conjunction with the regulatory infrastructure improvements discussed in Appendix E. NEI agrees with the plan; however, we recommend that the action plan be developed in the near term to bring more regulatory certainty to the issue and to have the plan implemented prior to next major safety digital upgrade.

3.0 Implications

In the absence of clear guidance with respect to regulatory certainty in topical reports changes and maintenance, safety digital projects continue to be delayed due to the perceived risk from

the unclear regulatory expectations and additional cost and schedule impacts from lengthy NRC reviews.

4.0 Priority

The Industry does not believe this is a high priority item given other priorities and limited resources. NEI recommends this issue remain in the action plan but at a lower priority compared to the issue of commercial dedication and SIL certification (see Appendix C), which has an impact on this issue.

5.0 Tentative Level 0 Schedule

- Develop the the action plan to result in more regulatory certainty – 3Q2016
- Implement the plan - TBD

Appendix H

Incorporation of Industry Standards in Regulation

1.0 Discussion

The NRC activities to incorporate IEEE standards into the regulations or to endorse future versions by Regulatory Guides should conform to the Commission direction in SRM-SECY-15-0106 that future requirements be performance-based and technology neutral. The 1991 version of IEEE 603 and the alternative IEEE 279 have worked because they set fairly high level performance-based requirements for safety systems. Those requirements are technology neutral, universal, and have remained static for the nuclear industry. The trend with the revisions to IEEE 7-4.3.2 has been to incorporate more prescriptive requirements that are technology focused (i.e., more detailed mandatory requirements based on specific programmable technologies).

The NRC DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (Draft Digital Action Plan, or DAP), item 3 addresses rulemaking activities to incorporate a future revision of IEEE 603 (e.g., 2018) in place of IEEE 603-1991. NRC DAP item 4 addresses activities for NRC to endorse a future revision of IEEE 7-4.3.2. The detailed action plans for these two items also identifies staff actions to pursue the incorporation of additional requirements into these standards (i.e., the addition conditions proposed for the endorsement of IEEE 603-2009 in SECY-15-0106).

The trend with the revisions to IEEE 603 and IEEE 7-4.3.2 that makes them more prescriptive should be reversed by eliminating requirements that do not add value with respect to ensuring quality and safety in a modernized regulatory infrastructure.

2.0 Desired Outcome

Industry desires a clean endorsement of any revision to IEEE 603 that is appropriately performance-based, technology neutral, and effectively integrated into a modernized digital I&C regulatory framework.

IEEE 7-4.3.2 should be harmonized as much as possible with the international technical standards developed for specific digital technologies used in safety-critical applications.

NRC actions to pursue the incorporation of the additional conditions on IEEE 603-2009 and IEEE 7-4.3.2 proposed in SECY-15-0106 with the IEEE Standards Committee as a high priority would be counter-productive, since it was these conditions that drove the industry reaction to the proposed rulemaking.

Any future rulemaking regarding incorporation of a later version of IEEE 603 needs to be well structured to avoid unintended consequences, since the licensing basis for most operating plants is that only the protection system is designed to IEEE 279. Scope expansion of IEEE 603 to other systems must be avoided. Furthermore, the applicability of new requirements must be

narrowly focused on the digital components of the system to avoid confusion with regard to the regulatory basis for the other aspects of the system design (e.g., sensors, cables, separation, etc.).

3.0 Implications

Addressing newer versions of IEEE 603 and IEEE 7-4.3.2 is one small element of the modernization needed for the digital I&C regulatory infrastructure and must be coordinated and integrated with the broader effort related to DAP item 7.

Specific issues with IEEE 603-2009:

1. Revision of IEEE 603 will not solve the digital I&C issues. IEEE 603 is a system-based standard. Digital aspects are addressed in IEEE 7-4.3.2. Keeping the 1991 version of IEEE 603 or referencing a newer version will have little technical impact; however, if not structured properly, it could cause inconsistencies in design basis documents with respect to the versions cited for compliance.
2. IEEE 603-2009 added a section on common cause failure (CCF) by referring to IEEE 7-4.3.2 only. This approach perpetuates the unbalanced focus on software CCF. IEEE 603 needs to be revised to address all CCFs and should reference IEEE 379 as the standard for addressing CCFs.
3. The current rule structure separates *protection systems and other safety systems*. That distinction needs to be retained in any future rulemaking to ensure that the system-related requirements from IEEE 603 are not unintentionally changed for the portions of systems not affected by digital equipment retrofits. The proposed rulemaking to incorporated IEEE 603-2009 significantly expanded the scope to all safety related systems.

Specific issues with IEEE 7-4-3.2:

1. The 2010 version (which has not been endorsed) both changed the nature of the guidance from DI&C-ISG-04 and increased prescriptiveness of the standard. The DI&C-ISG-04 guidance was developed and touted as a 'fast-track' approach to addressing communication independence. It was clearly communicated that it was conservative guidance that would support an easier and quicker NRC review and not requirements. The effort to move the DI&C-ISG-04 guidance into the standard made the conservative guidance (e.g., ISG 'should' statements) became mandatory requirements (i.e., standard 'shall' statements) in the process. Other process guidance from other NRC documents related to development lifecycles, common cause failure analysis, and commercial grade dedication were added, which increased the complexity and prescriptiveness of the standard (i.e., the number of mandatory requirements increased from 73 in the 2003 version to 336 in the 2010 version). The 'single repository' approach to capture everything digital created duplication with other NRC-approved or endorsed guidance documents. NRC endorsement of IEEE 7-4.3.2-2010 (or the 2016 version with the same requirements) would exacerbate the current problems with overly prescriptive requirements rather than solve them.

2. The IEEE 7-4.3.2-2016 version addresses software CCF. These CCF-related requirements will need to be harmonized with the results of DI&C Improvement Plan item 1 in any subsequent revision prior to any NRC endorsement.
3. IEEE 7-4-3.2-2010 moved the non-mandatory guidance from Annex C into the main body as mandatory requirements. The commercial grade dedication guidance for digital I&C requirements in IEEE 7-4.3.2-2010 need to be harmonized with RG 1.209 (which recognizes EPRI TR-107330), RG 1.152, Revision 3 (which recognizes EPRI TR-106439 while also noting that IEEE 7-4.3.2-2003 Annex C, is not endorsed because it provides inadequate guidance), and RG 1.28, Revision 4 (which endorses NQA-1-2008).
4. The software verification and validation requirements IEEE 7-4.3.2 need to be harmonized with RG 1.168, Revision 2, (which endorses IEEE 1012-2004) and RG 1.28, Revision 4 (which endorses ASME Standard NQA-1-2008) and shift to an approach that is performance-based and technology neutral.

The role of the IEEE-related appendices in Standard Review Plan Section 7.1 should be re-evaluated to ensure that the review guidance is made consistent with the changes coming from DAP activities to ensure consistent and effective implementation as part of DAP Item 11.

4.0 Priority

The industry perspective is that the IEEE 603 rulemaking effort is low priority and provides little benefit.

The detailed action plan item to separately pursue the additional conditions on IEEE 603-2009 and IEEE 7-4.3.2 proposed in SECY-15-0106 with the IEEE Standards Committee should not be pursued at this time, since it will duplicate the collaborative regulatory improvement activities with the nuclear industry on the DAP being conducted through NEI. The work on these tasks should be deferred until the broader direction setting aspects of actions described in Appendices A, C, D, and E are completed.

5.0 Tentative Level 0 Schedule

The following DAP items are prerequisites for the efforts to update IEEE 603 and IEEE 7-4.3.2:

- Appendix A - Potential Common Cause Failures
- Appendix C – Procurement issues including Embedded Digital Devices
- Appendix D - Regulatory Document Infrastructure Improvements
- Appendix E - Regulatory Infrastructure

Harmonize IEEE 603-2009 in the context of performance-based and technology neutral to the extent practical consistent with the integrated regulatory framework modernization decisions - 2017.

Harmonize IEEE 7-4.3.2-2016 in the context of performance-based and necessary technology-based requirements to the extent practical consistent with the integrated regulatory framework modernization decisions - 2017.

Appendix I

Cyber Security

1.0 Discussion

The DRAFT Integrated Action Plan to Modernize Digital Instrumentation and Controls Regulatory Infrastructure (Draft Digital Action Plan, or DAP), Item 5 proposes to provide guidance to the staff of the NRC to support their review of voluntarily submitted cyber security design information. The Action Plan describes this topic as having been identified through significant engagement with stakeholders and staff analysis of the regulatory infrastructure. Further, this item is characterized as a near-term priority; and an associated working group action plan is described.

2.0 Desired Outcome

This item should be eliminated from the DAP. Further, NEI recommends that the NRC suspend all work on this item, halt the development of any guidance, and reallocate those resources to support more pressing DI&C needs. The current regulatory framework is more than adequate to address safety and security issues associated with DI&C systems. There is no clear evidence that implementation of this item will substantially improve the licensing process, improve regulatory clarity, or will enhance safety and security. A requirement to implement specific technologies for communications isolation within the design of DI&C systems is unnecessary and would likely have many unintended adverse consequences. NEI's members, including new plant and SMR communities are unified on this point.

3.0 Implications

As described in the working group Action Plan, this item encompasses two substantive elements:

a) The review of cyber security elements during the licensing review of DI&C systems; and,

b) The recommendations of the ACRS to require communication flow enforcement device designs within the regulations.

A more fulsome discussion of NEI's position on both elements is warranted.

3.1 Cyber Security Design Reviews

The Action Plan describes that the current regulatory framework increases the regulatory uncertainty for COL holders and operating reactor licensees, who are ultimately responsible for ensuring their systems comply with the NRC's cyber security regulations (e.g., 10 CFR 73.54), and may have to address vulnerabilities in system's design after the design has been completed. The Action Plan provides no substantive discussion on how the staff proposal would resolve this apparent issue.

The industry has been uniform in its position on this topic throughout the record of activity. The industry has clearly established our views to the NRC and the DI&C Subcommittee of the Advisory Committee on Reactor Safeguards (ACRS). Notably, at the February 23, 2011 ACRS DI&C Subcommittee meeting to review draft Regulatory Guide (RG) 1.152, Revision 3, the industry provided two detailed presentation describing how the design requirements under 10 CFR 50 and the security requirements under 10 CFR 73 provide a stable framework to address both design and security issues. The transcript and presentations can be found at ADAMS Accession Number ML111080650.

While the incorporation of specific cyber security features into the design of a digital system may be attractive, NEI urges extreme caution in this area. First, simplicity is an attribute of both safe systems and secure systems. Increasing the complexity of a safety system to address cyber security concerns may have the unintended effect of diminishing both safety and security. Second, the design basis used to establish the safety basis of a system are likely to remain static for long periods of time, however, the cyber security features implemented to secure a digital system are likely to change over time to reflect the advancing nature of the cyber threat. Incorporating cyber security features into the design of the DI&C system will necessarily complicate cyber security upgrades.

NEI continues to believe that the clear separation between 10 CFR 50 and 10 CFR 73, as articulated in final RG 1.152, Revision 3, is the appropriate regulatory structure, and that no change is warranted. As noted in the presentations to the ACRS, industry supported the proposed revisions as:

Keeping the focus of Regulatory Guide 1.152 on security from a safety design stand point ensures protection of digital safety systems against non-malicious events;

- The licensee's cyber security programs will address malicious actions or attacks while ensuring preservation of the safety functions associated with the SR CDAs to meet the requirements of 10 CFR 73.54; and,
- The combination of proposed RG 1.152, Rev. 3 and the programmatic provisions under 10 CFR 73.54 {RG 5.71 or NEI 08-09 R6} seamlessly address the secure design, development, and operation of digital safety systems.

RG 1.152, Revision 3 provides appropriate separation between 10 CFR 50 and 10 CFR 73. The industry has developed guidance to aide licensees in how to consider cyber security during the design of digital systems.

Several EPRI reports provide effective technical guidance for integrating cyber security into the design and procurement processes. These include:

- Technical Guideline for Cyber Security Requirements and Life Cycle Implementation Guidelines for Nuclear Plant Digital Systems-1019187
- Cyber Security Procurement Methodology, Rev. 1- 3002001824

These resources are able to aide industry personnel in the technical decisions required to establish effective cyber security while achieving safe and effective Digital I&C designs under the current regulation. In addition, this approach allows the industry to utilize technically sound cyber security approaches that adapt to rapidly changing technology and threat landscapes. NEI is aware that licensees are making use of these EPRI reports.

3.2 Communications Flow Enforcement Requirements

The Action Plan describes that the ACRS has raised concerns associated with the control of access to plant equipment and networks. ACRS has indicated that such a review should consist of evaluating the design of the communication flow enforcement devices to verify this device maintains unidirectional flow from higher security levels to lower security levels. NEI also understands that the ACRS has promoted specific design elements for communications isolation be incorporated as a requirement.

The industry has followed the discussions between the ACRS and the NRC very closely, and we are not convinced that there is a compelling safety basis for requiring additional reviews of communications flow enforcement mechanisms beyond the current regulatory framework. Further we see no compelling basis for including a specific type of communications isolation mechanism within the regulations.

Current 10 CFR 50 related guidance to prevent inadvertent access for DI&C equipment is adequate to provide reasonable assurance. Current 10 CFR 50 related guidance to protect against the design basis threat of radiological sabotage cyber attacks is adequate to provide high assurance of adequate protection. NEI sees no compelling discussion in the record that indicates the current framework is inadequately protective.

A requirement to implement a specific technology for communications isolation within the design of DI&C systems is unnecessary and could have many unintended adverse consequences. Notably, the requirements could provide a considerable hurdle to the development of highly integrated control rooms.

4.0 Priority

The Industry does not believe this topic warrants further development, and recommends that the NRC suspend all work on this item. Associated resources should be reallocated to support more pressing needs.

5.0 Tentative Level 0 Schedule

N/A