

U.S. Nuclear Regulatory Commission Public Meeting Summary

August 7, 2015

Title: Public Meeting to Discuss a Proposed Rule to Incorporate by Reference Institute of Electrical and Electronics Engineers Standard 603-2009 into the U.S. Nuclear Regulatory Commission Regulations

Meeting Identifier: 20151142

Date of Meeting: August 4, 2015

Location: Teleconference and webinar only

Type of Meeting: Category 3

Purpose of the Meeting:

The purpose of the meeting was to provide information and receive feedback about an upcoming proposed rule to incorporate by reference Institute of Electrical and Electronics Engineers Standard (IEEE Std) 603-2009 into the U.S. Nuclear Regulatory Commission (NRC) regulations. The NRC did not accept formal comments during the meeting.

General Details:

The meeting was in a webinar format, and audio was provided by teleconference. The meeting was attended by 63 individuals including 24 NRC staff and 39 members of the public. A list of attendees is provided as an enclosure to this meeting summary.

Summary of Presentations:

The meeting started with welcoming remarks, introductions, and meeting ground rules. Next, the NRC staff gave a presentation. The staff's presentation slides and a handout are available in the NRC's Agencywide Documents Access and Management System (ADAMS) package under Accession No. ML15216A636.

In the presentation, the staff:

- Described the purpose of the rulemaking activity
- Identified changes to IEEE 603 between the 1991 and 2009 versions of the standard
- Explained how the draft proposed rule addresses changes to the standard
- Discussed the relationship between Draft NRC Regulatory Guide 1.153 and the new rule
- Presented questions that are included in the draft notice for the proposed rule
- Discussed the safety case for the new reactor independence conditions in the draft proposed rule

The draft proposed rule establishes a series of new conditions for the use of IEEE 603 in the following areas:

- System integrity
- Independence between safety and non-safety systems
- Independence between safety divisions
- Documentation requirements

Following a short break, there was a question and answer period in which the NRC staff and members of the public discussed various aspects of the subject matter.

Public Participation Themes:

During the public question and answer portion of the meeting, NRC staff addressed questions on the following topics:

- A representative from the Nuclear Energy Institute (NEI), Gordon Cleifton, wanted to confirm that the NRC would maintain an interface with the industry as the rulemaking goes forward, including a workshop during the public comment period. He also asked whether the staff planned to allow for an extended public comment period. The staff confirmed that the NRC would maintain such an interface and intends to have a workshop during the public comment period. The staff also confirmed its intent to have an extended public comment period. A typical rulemaking comment period is 75 days, and the staff is recommending 120 days for this rulemaking. Mr. Cleifton stated that he could act as the point of contact for the industry as the draft rule goes forward.
- Ted Quinn (consultant) asked if there would be any changes for the interface to cyber security from the draft rule. Also, would there be any differences between what was done for the Diablo Canyon digital upgrade and the draft rule? The staff explained that there would not be changes to the interface with NRC Regulatory Guide 5.71, "Cyber Security Programs for Nuclear Facilities," except that if applicants for new reactor licenses or design certifications pursued an alternative to the data communication criteria, they would need to identify all direct and indirect data communication paths to the safety instrumentation and control (I&C) system. This would enable a licensee to establish a sufficient cyber security program. The NRC held a public meeting on this topic on April 29, 2015. A summary of the meeting is available under ADAMS Accession No. ML15119A289. The NRC plans to hold a second public workshop on August 18, 2015, to discuss a separate initiative on whether to include cyber security design features within an I&C licensing review. This is the subject of a draft Commission Paper (SECY Paper) where the staff is proposing options to the Commission on this matter. Regarding the question about the Diablo Canyon license amendment, the staff pointed out that this application references two previously approved platforms: the Tricon and the Westinghouse ALS systems. Though each of these systems was evaluated against IEEE 603-1991 criteria, newer versions of the IEEE standard were used in the development of these systems. The staff also noted that the Diablo Canyon plant protection system design has not been evaluated for compliance with the proposed conditions included in the draft rule. The Diablo Canyon plants are currently operating, so they would not be required to comply with the new reactor conditions being proposed in the draft rule.

- Paul Hunton (Duke Energy) noted that definitions for certain terms were being identified in the statement of considerations of the proposed rule, and they might supersede other definitions in other regulatory documents. (The statement of considerations is the portion of the *Federal Register* notice before the rule text. This is sometimes referred to as the preamble.) The staff responded that the intent was to have clear meaning and intent within the statement of considerations, not to do a global revision of definitions. Mr. Hunton recommended that the staff verify consistency of definitions in other regulatory documents and standards, and if the intent is to supersede previous definitions, to be aware of the potential for unintended consequences. The staff stated that inconsistencies identified within these definitions should be corrected before the rule is made final. There will be an opportunity to make such corrections during the public comment resolution period.
- Ken Scarola (consultant) noted that it appears in the rule that the NRC Office of Nuclear Reactor Regulation is comfortable with accepting data communications as outlined in NRC Digital I&C Interim Staff Guidance 04 (ISG-04), but the NRC Office of New Reactors has established more restrictive data communication criteria. Why is there this difference? The staff responded that new reactor designs are more integrated and complex and involve a higher level of data communications as compared to recent operating reactor digital upgrades. Based on experience licensing new reactors, it has been difficult for applicants to provide the requisite level of design information and analysis to justify independence of certain data communication techniques as outlined in ISG-04. Third, the Commission policy on advanced reactors states that new reactors should have enhanced safety and be more simple in design and operation as compared to current operating reactors. The staff also noted that an applicant can propose alternatives to the new reactor portion of the independence requirements under 10 CFR 50.55a(z). However, the staff acknowledged Mr. Scarola's recommendation that there be a provision in the draft rule that would allow new reactor applicants the option to provide detailed design information and analysis to support a wider range of data communication techniques instead of having to use the alternative route.
- Troy Martel (Safe Operating Systems) asked about the applicability of the new rule to diesel controls and load sequencers. The staff referred to the stated purpose and scope of both the IEEE 603 standard and of the existing rule which include safety-related control and protection systems. The rulemaking effort will not change the intended scope and diesel controls and load sequencers will continue to be within the scope of the rule.
- Frank Novak (General Electric Hitachi) noted that in a previous public version of the draft rule there were criteria addressing common-cause failure (ADAMS Accession No. ML14136A089). However, in the current draft rule, the criteria were taken out. Why? The staff provided an explanation as to why the common-cause failure criteria were taken out. The staff noted that its basis and current guidance for treating common-cause failures in digital safety systems has been largely based on a policy statement (Item II.Q of the Staff Requirements Memorandum for SECY 93-087; ADAMS Accession No. ML003708056) developed in the early 1990s and put into effect within branch technical positions of the Standard Review Plan (NUREG-0800). The previous draft rule had provided no additional criteria or changes to the SRM criteria. The staff believes

that the codification of a requirement for performing defense-in-depth and diversity analyses and possible inclusion of additional diverse means of accomplishing required safety functions warranted development of additional technical bases supporting the regulatory basis for such a rule and, therefore, the criteria were removed from the draft rule. The staff has initiated research into the bases for the current SECY policy statement and is documenting and evaluating the improvements in digital safety and control system development processes that have evolved since the policy was initiated. The outcome of this research will enable the NRC to either affirm or revise its policy as the evidence is evaluated. If appropriate, a separate rule and accompanying guidance could be developed to codify requirements for defense-in-depth and diversity analyses to be performed and additional diversity to be included in the design of digital safety systems. Alternatively, existing guidance for coping with the potential for common-cause failures could be enhanced.

- Ken Scarola (consultant) made a comment about the draft rule criteria for addressing signal faults. Normally, erroneous signals are considered a class of signal faults. Is it the intent of the staff that industry be able to detect and mitigate erroneous signals? For example, if a valve has a safety function of both open and close, and it receives a close signal when it should be open, this would be an erroneous signal, but this would be difficult to detect and mitigate. The staff noted that the intent was to address detectable signal faults. The staff agreed that some clarification on the term signal fault could be considered to address this concern.
- Ken Scarola (consultant) stated that it appears that the NRC has made up its mind that enhanced human-machine interfaces (HMIs) using multi-divisional displays are not safe. Mr. Scarola asked if the staff has seen operator performance on simulators using multi-divisional displays and the increased safety margin that is obtained. For example, on the US-APWR simulator, operators were able to mitigate a steam generator tube rupture event with about 30 minutes of margin using the non-safety HMI controlling safety-related plant equipment compared to 2 or 3 minutes of margin if they could only operate such equipment from safety-related displays. The staff noted that it has not closed its mind on multi-divisional displays, but based on licensing experience with new reactors, applicants had difficulty demonstrating the safety benefits (from a human factors and I&C perspective) of such multi-divisional displays. The staff has not seen research or a technical basis that evaluates the safety benefits and hazards of such multi-divisional displays. If the industry desires to continue to pursue such a design, it should develop the requisite technical basis. Furthermore, some arguments for using non-safety-related multi-divisional HMIs to control safety-related plant equipment appear problematic. For example, applicants have stated one reason for using the non-safety multi-divisional HMIs over the safety-related HMIs (which operators will depend upon if the non-safety HMIs fail) is the lower capability and human reliability of the safety-related HMIs. As another example, one applicant incorporated the capability of non-safety HMIs to place safety-related plant equipment in operational or maintenance bypass, which is not needed for abnormal or emergency operation and for which adequate independence has not been demonstrated. The staff noted that the benefits of using non-safety HMIs during emergency operation should be weighed against the risk of a permanent connection of a non-safety HMI to safety systems. Based on such experience and lack of technical basis, the NRC staff did not see it prudent to allow non-safety control of

safety-related plant equipment at this time. If a new reactor applicant believes they do have the necessary design information and analysis to support such a design technique, the draft rule would allow them to pursue an alternative.

- Ken Scarola (consultant) noted that the rule would apply to all design certification applicants, regardless of their submittal date, unless they already received design certification. This could be challenging for design certification applicants who have already submitted their application and may be close to receiving design certification, but then the IEEE 603-2009 rule is finalized before receiving design certification. This could result in significant rework for that applicant. The NRC staff noted that the timing of applicability for design certification applicants was considered during the development of the rulemaking. If received as a public comment, the NRC would take this concern into further consideration.

Action Items/Next Steps:

- The NRC staff intends to seek Commission approval to publish a proposed rule on IEEE Std. 603-2009 in the *Federal Register*.
- If the Commission approves the publication of the proposed rule, then the *Federal Register* notice of proposed rulemaking will provide an opportunity for the public to submit formal comments. The NRC will provide formal comment responses to timely-filed comments on the proposed rule.

Additional Information:

- Meeting notice and agenda: ML15204A103
- NRC staff presentation slides: ML15209A953
- Handout with preliminary draft proposed rule language: ML15204A643
- Meeting summary: ML15216A637
- Docket folder: <http://www.regulations.gov/#!docketDetail;D=NRC-2011-0089>

safety-related plant equipment at this time. If a new reactor applicant believes they do have the necessary design information and analysis to support such a design technique, the draft rule would allow them to pursue an alternative.

- Ken Scarola (consultant) noted that the rule would apply to all design certification applicants, regardless of their submittal date, unless they already received design certification. This could be challenging for design certification applicants who have already submitted their application and may be close to receiving design certification, but then the IEEE 603-2009 rule is finalized before receiving design certification. This could result in significant rework for that applicant. The NRC staff noted that the timing of applicability for design certification applicants was considered during the development of the rulemaking. If received as a public comment, the NRC would take this concern into further consideration.

Action Items/Next Steps:

- The NRC staff intends to seek Commission approval to publish a proposed rule on IEEE Std. 603-2009 in the *Federal Register*.
- If the Commission approves the publication of the proposed rule, then the *Federal Register* notice of proposed rulemaking will provide an opportunity for the public to submit formal comments. The NRC will provide formal comment responses to timely-filed comments on the proposed rule.

Additional Information:

- Meeting notice and agenda: ML15204A103
- NRC staff presentation slides: ML15209A953
- Handout with preliminary draft proposed rule language: ML15204A643
- Meeting summary: ML15216A637
- Docket folder: <http://www.regulations.gov/#!docketDetail;D=NRC-2011-0089>

DISTRIBUTION:

PUBLIC RidsNrrDpr DDoyle TInverso GLappert

ADAMS Accession Nos.: Pkg. ML15216A636; Notice ML15204A103; Summary ML15216A637; Presentation Slides ML15209A953; Preliminary Draft Proposed Rule Language ML15204A643
NRC-001

OFFICE	NRR/DPR/PRMB	NRR/DPR/PRMB*	NRR/DPR/PRMB	NRR/DPR/PRMB
NAME	DDoyle	GLappert	TInverso	DDoyle
DATE	8/6/2015	8/7/2015	8/7/2015	8/7/2015

OFFICIAL RECORD COPY



NRC Public Meeting
List of IEEE 603-2009 Proposed Rule Public Meeting Attendees
August 4, 2015

Name	Organization
Rossnyev Alvarado	NRC
Christina Antonescu	NRC
Joseph Ashcraft	NRC
Royce Beacom	NRC
Jennifer Borges	NRC
Samir Darbali	NRC
Bernard Dittman	NRC
Cliff Doust	NRC
Daniel Doyle	NRC
Antonio Gomez	NRC
Tara Inverso	NRC
Terry Jackson	NRC
Glenna Lappert	NRC
John Lubinski	NRC
Aby Mohseni	NRC
David Rahn	NRC
Mo Sadollah	NRC
Aaron Sanders	NRC
Fred Schofer	NRC
Richard Stattel	NRC
Russell Sydnor	NRC
John Tappert	NRC
Michael Waterman	NRC
Deanna Zhang	NRC
Jack Adkins	GE
Douglas Chapin	MPR Associates
Gregg Clarkson	NuScale Power
Gordon Clefton	NEI
Darrell Cooksey	Hurst Technologies
Chris Earls	NEI
Dan Grundman	Areva
Brian Haynes	Schneider Electric
Raymond Herb	Southern Nuclear
Nathan Hottel	Areva
James Howard	GE Hitachi
Paul Hunton	Duke Energy
Steve Hutchins	NEI
Troy Martel	Safe Operating Systems
Jerry Mauck	TR Resources
Randy Newton	NuScale
Francis Novak	General Electric Hitachi
Warren Odess-Gillett	Westinghouse

Ken Pigg	Duke Energy
Jason Pottorf	NuScale
Ted Quinn	Technology Resources
Deann Raleigh	Curtiss Wright
Jack Rosentel	Lockheed Martin
Ken Scarola	Nuclear Automation Engineering
Clayton Scott	Schneider Electric
Jimmy Seawright	Luminant Power
Shelby Small	GE Hitachi
Mark Stofko	Westinghouse
Bryan Thomas	PSEG Nuclear
Patrick Troy	Lockheed Martin
Masafumi Utsumi	Mitsubishi Heavy Industries
Wesley Vaughn	Southern Nuclear
Charles Waite	Process Design Consultants
Hughes Wike	NuScale
Jonathan Witter	BWXT mPower
Roger Wyatt	Areva
Peter Yandow	GE Hitachi
Gyota Yasoda	Mitsubishi Electric Power Products
Camille Zozula	Westinghouse Electric