Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital I&C Subcommittee

Docket Number: (n/a)

Location: teleconference

Date: Wednesday, February 19, 2025

Work Order No.: NRC-0228 Pages 1-82

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1716 14th Street, N.W.
Washington, D.C. 20009
(202) 234-4433

DISCLAIMER

UNITED STATES NUCLEAR REGULATORY COMMISSION'S ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

The contents of this transcript of the proceeding of the United States Nuclear Regulatory Commission Advisory Committee on Reactor Safeguards, as reported herein, is a record of the discussions recorded at the meeting.

This transcript has not been reviewed, corrected, and edited, and it may contain inaccuracies.

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL I&C SUBCOMMITTEE

+ + + + +

WEDNESDAY

FEBRUARY 19, 2025

+ + + + +

The Subcommittee met via Video/ Teleconference, at 1:00 p.m. EST, Thomas E. Roberts, Chair, presiding.

SUBCOMMITTEE MEMBERS:

THOMAS E. ROBERTS, Chair

RONALD G. BALLINGER

VICKI M. BIER

VESNA B. DIMITRIJEVIC

GREGORY H. HALNON

CRAIG D. HARRINGTON

WALTER L. KIRCHNER

ROBERT P. MARTIN

MATTHEW W. SUNSERI

ACRS CONSULTANTS:

DENNIS C. BLEY

CHARLES H. BROWN, JR.

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

GILBERTO BLAS, NRR/DEX/EICB

CALVIN H. CHEUNG, RES/DE/ICEEB

SAMIR X. DARBALI, NRR/DEX/EICB

TANIA MARTINEZ NAVEDO, NRR/DEX

JASON C. PAIGE, NRR/DEX

WILLIAM A. ROGGENBRODT III, NRR/DEX/EICB

CONTENTS

P-R-O-C-E-E-D-I-N-G-S

1:00 p.m.

CHAIR ROBERTS: This meeting will now come to order. This is a meeting of the Digital I&C Subcommittee of the Advisory Committee on Reactor Safeguards. I am Tom Roberts, chairman of today's subcommittee meeting.

ACRS members in person are Ron Ballinger. Craig Harrington will be back shortly. He was here and will be back. ACRS members in attendance virtually via Teams are Greg Halnon, Vesna Dimitrijevic, Walt Kirchner, Matt Sunseri, and Vicki Bier.

Also in attendance is our consultant, Dennis Bley, who is connected via Teams. And we expect Charlie Brown to be here in person when he finishes getting his new computer set up. Did I miss anybody, either ACRS members or consultants? Please speak up now.

MEMBER MARTIN: Tom, this is Bob. I'm here.

CHAIR ROBERTS: Okay. I'm sorry. And Bob Martin, who is here virtually. Christina Antonescu of the ACRS staff is the Designated Federal Officer for this meeting. No members with a conflict of interest were identified for today's meeting, and we have a

quorum.

During today's meeting, the subcommittee will receive a briefing on the proposed rulemaking to incorporate by reference the requirements of the 2018 version of IEEE Standard 603 into regulation. IEEE Standard 603 is entitled IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations. Title 10 of the Code of Federal Regulations, Part 50, Subsection 55a(h) currently incorporates by reference the 1991 version of IEEE Standard 603, as well as two versions of an earlier IEEE Standard 279. Which of these standards and versions apply to which plants is somewhat complex, as folks will find out during this briefing.

While this rulemaking may seem straightforward, there are several issues important to safety that the staff will address during this meeting. For one, the 2018 version of the IEEE standard includes guidance for mitigating common cause failures within a protection or safety system. In the proposed rulemaking, it has to exclude off of the first sentence of this guidance. I think we'll have a good discussion of why the staff intends to exclude much of the IEEE guidance and the adequacy of the guidance that remains.

Also, there was an earlier attempt in 2015 to incorporate the latest version of IEEE 603 into regulation, and this attempt resulted in several NRC staff non-concurrences, three suggestions from this committee, and disapproval from the Commission to proceed with the rulemaking. The staff will cover that history during this briefing, including how each of the previous issues was resolved in this relatively straightforward proposed rulemaking.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act, or FACA. The NRC implements FACA in accordance with its regulations found in Title 10, Part 7 of the Code of Federal Regulations. Per these regulations and the committee's bylaws, the ACRS speaks only through its published letter reports. All member comments should be regarded as only the opinion of that member, not a committee position.

All relevant information related to ACRS activities, such as letters, rules for meeting participation, and transcripts are located on the NRC's public website and can easily be found by typing about us ACRS in the search field on NRC's homepage.

The ACRS, consistent with the agency's value of public transparency and regulation of nuclear

facilities, provides opportunities for public input and comment during our proceedings. We've received no written statements or requests to make an oral statement from the public. We've set aside time at the end of this meeting for public comments.

The ACRS will gather information, analyze relevant issues and facts, and formulate proposed conclusions and recommendations, as appropriate, for deliberation by the full committee. A transcript of this meeting is being kept and will be posted on our website.

When addressing the subcommittee, the participant should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard. If you're not speaking, please mute your computer on Teams or by pressing *6 if you're on a phone.

Please do not use the Teams chat feature to conduct sidebar discussions related to the presentations. Rather, limit us of the meeting chat function to report IT problems.

Everyone in the room, please put all your electronic devices in silent mode and mute your laptop microphones and speakers. In addition, please keep sidebar discussions to a minimum since the ceiling

microphones are live. For the presenters, your tail microphones are unidirectional, and you'll need to speak into the front of the microphone to be heard.

If you have any feedback for the ACRS about today's meeting, we encourage you to fill out the public meeting feedback form on the NRC's website.

We'll now proceed with the meeting, and I'll ask Ms. Tania Martinez Navedo, the acting Director of the Division of Engineering and External Hazards in the Office of Nuclear Reactor Regulation to make any introductory remarks she'd like to make before we begin the presentations. Tania.

MS. MARTINEZ NAVEDO: Thank you, Member Roberts. And good afternoon, everyone. Our purpose today is to brief the committee on IEEE Standard 603-2018, which will provide stakeholders the regulatory confidence to use the latest version of the standard in the development of safety-related instrumentation and control systems and be applicable to licensing of existing new and advanced reactors. This rulemaking effort would enhance efficiency for the stakeholders without affecting safety. This is in alignment with the ADVANCE Act's requirements and NRC's mission to enable the safe and secure use and deployment of civilian nuclear energy through efficient and reliable

licensing, oversight, and regulation.

At this moment, I will turn it over to Gilberto Blas, who will be starting the presentation for the NRC staff.

MR. BLAS: Good afternoon, everybody. Thank you, Tania. My name is Gilberto Blas. I'm an instrumentation and controls engineer as part of the EICB supporting this rulemaking. And also my colleague Calvin Cheung, also part of I&C doing our rotation and research.

So to start, I'm going to kick it off stating here that the presentation being shown here, being shown today is draft information regarding the proposed rulemaking and accompanying draft regulatory guidance and is subject to change, and we will issue these with an opportunity for comment.

So let's begin with the outline, as you can see, for the presentation. We're going to be going over proposed rulemaking efforts with background information regarding the Commission direction on IEEE 603, leading to the activities done as part of this current rulemaking effort. In addition, we're going to be going over the comparison made between the 1991 and the 2018 version of the standards.

We're going to spend some additional time

on Clause 5.16 on common cause failure, going over the staff evaluation. And, afterwards, we are going to discuss how the proposed rulemaking will handle information that is found in the 2018 version of the standard, including protection and safety systems and reference standards.

So as was pointed out, we're also going to be going over the ACRS letter recommendations from the 2009 previous rulemaking and the NRC staff non-concurrences that have been evaluated as part of this effort. We're going to wrap up with a summary of the proposed incorporation by reference of IEEE 603-2018.

Okay. So some background on where we're at and how we got here. Currently, Chapter 10 of the Code of Federal Regulations in Section 55a(h) has the 1991 version of the IEEE 603 standard for safety systems for nuclear power generating stations that is incorporated into the code. This version of the regulation is not up to date and multiple versions haven't been published since.

Back in 2015, the staff attempted to incorporate by reference the 2009 standard. However, that attempt was disapproved by the Commission, and the reason for that disapproval was due to an imposition of additional conditions and requirements

that were added beyond those in the standard that were inconsistent for new and operating reactors. With its response to the staff in SRM-SECY-15-0106, the Commission directed staff to develop a plan to modernize the NRC's digital instrumentations and controls for regulatory infrastructure, including how to address IEEE 603.

In the response that the staff provided to the Commission in SECY-16-0070, as part of the activities laid out on how to modernize the NRC's digital I&C regulatory infrastructure, they would be coordinating with the IEEE standards committee to address issues related to 603 through the 2018 output.

So moving ahead to 2023, the staff held a public meeting to solicit early feedback on the proposed path forward for IEEE 603-2018. In that meeting, staff discussed various options available on the path forward to utilize the latest standard with initial feedback received from stakeholders supporting incorporation by reference as that approach, as it provides regulatory certainty for licensees and applicants to utilize the latest version of the standard.

CHAIR ROBERTS: On the background, I wonder if you can go back a little before this time

frame. The 55a(h) was at least two versions before the version you're changing now. One was to adopt IEEE 279-1968 and then again for IEEE 279-1971. Can you talk about why that regulation was written at all? Because I've heard an argument that the general design criteria provides sufficient requirements, and what these IEEE standards are is more akin to guidance. Can you talk about why they were added in the regulation?

MR. ROGGENBRODT: Good afternoon. Bill Roggenbrodt, Office of Nuclear Reactor Regulation also in the Division of Engineering and External Hazards.

So in looking over the documentation in 1968 for IEEE 279, those were the proposed criteria for protection systems, and then they were accepted and approved in the 1971 version. Simultaneously with that, you had the general design criteria which went over those criteria, but, again, that was at a plant level or, again, general design criteria.

So the specificity, at least from my reading and research, shows that when you're talking about the details and intricacies of an instrumentation and control safety system that you would have that additional criteria that is system specific rather than plant specific.

CHAIR ROBERTS: Okay. Thank you. That makes sense. So this was actually the same time frame as the GDCs were being provided. So it appeared, at the time, folks thought that the GDCs were great. But for the protection systems, a little bit more was needed than regulation. You have one version, and then, you know, IEEE 603 a couple of decades later. Okay. Thanks. That's very helpful.

MR. ROGGENBRODT: Yes, sir.

MR. BLAS: Thank you, Bill. So as a side note, after we initiated this rulemaking in early 2024, the ADVANCE Act was issued. In response to the ADVANCE Act, NEI did provide a recommendation related to 10 CFR 50.55a, and staff is currently evaluating that recommendation as a separate activity from this rulemaking.

CHAIR ROBERTS: All right. So to clarify, your intent is to proceed with this rulemaking and that evaluation would go on a parallel, and you don't expect, at this point, that that would change the rulemaking finding or is there some potential that it would?

MR. BLAS: Not at this time that we're aware of, no.

CHAIR ROBERTS: Thank you.

MR. BLAS: So next slide. Okay. So moving on from the background to the current rulemaking effort, so in 2024, the staff formed an interoffice working group to formally issue activities on developing a path forward for the industry's use of IEEE 603-2018. Staff evaluated options for the use of the standard in concert with stakeholder input before deciding to proceed with this rulemaking option to incorporate by reference.

As mentioned, staff did a comparative analysis between 603-91, which is currently in regulations, and the standard to be incorporated, which is 2018. In addition, this proposed IBR does not raise significant policy issues and also would not impose additional requirements on the standards. And then, upon its incorporation, the 2018 would be incorporated in a similar fashion to 1991 where the standard would be required for new applicants and it would be optional for current licensees.

CHAIR ROBERTS: Can you clarify what optional for current licensees means? If somebody were to propose a major retrofit of their I&C system, go into digital technology for the first time at their plant, would they be permitted to use IEEE 279 as the basis for that because their plant was licensed under

IEEE 279, or would they be strongly encouraged or required to use the 603-2018?

MR. BLAS: So it depends. It depends on where their licensing basis is at. So if you look at 55a(h), what their licensing basis falls under, whether it be 603 or 279, has a lot to do when either a construction permit or design license was issued. So let's say the example you provided, a 279 plant, wants to use 603-91 or 2018 for an update that they're doing to their nuclear power plant, they have that option available to utilize that standard for that upgrade.

CHAIR ROBERTS: I think I'm asking the opposite question, which is if they said we're going to use 279-1968 because that's what we're licensed to to support a digital I&C retrofit, would you be okay with that or would you have, you know, concerns with that.

MR. BLAS: Let me just make sure I understood the question. So you're saying if a 279 plant wants to use the 279 criteria to do an update, given that it is to their licensing basis, yes, they would be able to do that.

CHAIR ROBERTS: So there are no missing criteria that would, again, concern you in terms of

how they would be designing their retrofit?

MR. DARBALI: This is Samir Darbali, I&C. So Gilberto is right. A plant only has to meet what their licensing basis criteria is. The guidance that we do have, for example, for licensing in ISG-06, it does tie to the 603 requirements right now in 1991, so the staff would have to do an evaluation to ensure that the licensee is meeting their licensing basis but also that the staff is following the Commission policy when it comes to a particular application.

CHAIR ROBERTS: Does that mean, in practice, they would have to follow 603?

MR. DARBALI: What we have found, because, again, sometimes, an applicant will -- an application is going to be supported by a vendor and, typically, vendors support 603 criteria. And so that application package is crafted in a way that meets the 603 criteria.

So what we do when we perform our licensing review is make sure that 603 criteria matches with the licensing basis. So it could be IEEE 279-1971. So, in a way, what we have found in practice is that they do match. Language may be somewhat different, but, in essence, they do meet the criteria.

CHAIR ROBERTS: Okay. Thanks, Samir.

MR. BLAS: Okay. I think we covered everything in this slide, so I'll just move on to the next slide.

Okay. So, in addition to this rulemaking, the staff is planning to develop accompanying draft regulatory guidance with the proposed incorporation by reference with IEEE 603-2018. Right now, the staff is currently evaluating which document would be revised or developed to provide that accompanying draft guidance.

Any questions here? Okay.

MR. BROWN: Yes. What do you mean by that, draft guidance? Is it going to be a new reg guide, is it going to be an existing reg guide, or what?

MR. BLAS: So it would be a regulatory guidance. It would not be staff guidance. And right now, given that we're developing it, it would be draft guidance.

MR. BROWN: We've got reg guides right now that cover a number of items. So this IBR has no clarifications. You're effectively accepting 2018 for the most part. I didn't see anything new in it. It didn't even incorporate stuff that we tried to do back

in 2014. There was a lot of nuances to that one that you all especially left it alone. 2018 is going to be what it is, not a whole lot of differences from the 1993 or 1991, whichever date you're about old enough to remember.

So now the effort is going to be, instead of the panoply of other reg guides like, you know, the computer use and BTPs, et cetera, et cetera, you're going to develop another reg guide that provides clarifying guidance relative to 2018 itself and separate from the IBR, as opposed to melding it into the IBR.

MR. BLAS: Correct, yes.

CHAIR ROBERTS: There was some discussion of the rulemaking document 1.153. It has basically the same title as IEEE 603, and it's relatively old.

MR. BROWN: I thought we had revised that at one time. We revised a lot of the reg guides, and I can remember some of them and I can't remember the rest. All right. Just was curious as to what -- so it will not be a 1.53 plus change?

MR. BLAS: Well, we're still evaluating. We would repurpose Reg Guide 1.53, or it would be a new document.

MR. BROWN: Well, 1.53 still is in play.

I mean, it's still there. If you don't do anything else, it's still there.

MR. BLAS: Correct, yes.

MR. BROWN: Thank you.

MR. BLAS: No problem. Okay. Let's talk about the comparison that was made for IEEE 603-91 and 2018. So for the comparison that was made, the staff came --

MR. BROWN: Let me backtrack for one minute. I'm sorry to interrupt. So the sole real purpose of this IBR, put all the other language and all the other questions aside, is to really do no more than, say, use 2018 vice 1991.

MR. BLAS: Yes.

MR. BROWN: Okay. Make sure I fully understood that. Thank you.

MR. BLAS: We got to make sure that's understood.

MR. BROWN: It's the reg guide type stuff for if you want clarifications.

MR. BLAS: Yes.

MR. BROWN: So if we want to attack, that's where we'd have to attack. If we had comments. Just ask Samir. He'll know. Thank you.

MR. BLAS: Thank you. Okay. In the

comparison that was made, staff developed this approach where clauses and subclauses were divided into items to facilitate a comparison. These items were binned into four categories, as you can see on the screen: identical, which means no changes in the wording between the two; equivalent, which can include items such as formatting changes or updated standard revisions, updated wording, restructured numbering, or something similar to that; enhancements, which would be improved by the clarifications; or an additional text modifying items on existing topics being addressed by existing clauses, and then we're talking brand new added items addressing new topics. So we will present examples in the next following slides on going over the equivalent and enhancement to help demonstrate that categorization.

Also, in the following slides, we're going to be discussing the new clauses added to the document. And something to note, as you can see on the pie chart, for that comparison, the majority of the changes from the revision were mostly categorized into equivalent or identical. That was the majority of the changes. And then the four items that you can see which are new are all associated with Clause 5.16 on common cause failure, which we're going to be

covering in more detail in the next topic section.

So let's present some examples. So here this is what we mean for representing what would be an equivalent clause. Over here, the criterion is identical and provides the clause -- I'm sorry. It's identical. However, the parenthetical examples were changed from using the word example to the Latin exampli gratia, which means for example. And also the generic term regulatory agency, providing specific examples in the updated standard. So for the staff evaluation standpoint, this would be considered an equivalent clause.

So for the enhancement clause here, this clause provides additional improvements and clarifications to an existing clause with the additional text addressing the need to have deterministic behavior for safety functions and, in addition, the refrain back to Clause 4 dealing with topics related to hazard analysis and environmental conditions. For staff, given that this is for an existing topic and clause, this is considered an enhancement.

So here, to summarize, the staff did go through both of the standards. We did that comparative analysis. The results were what was shown

on the pie chart, and we concluded that the only new clause is Clause 5.16 on common cause failure, which we're going to be elaborating in the next following slides.

So for Clause 5.16 on common cause failure, the first sentence states: The safety system design and development shall address common cause failures that create a potential to degrade or defeat the safety-significant function. The NRC staff, as part of their evaluation, is in full agreement with this first sentence.

The remaining statements within Clause 5.16 describe guidance on how the CCF should be addressed with some methods within that are provided. So two things regarding this guidance is that the NRC is not taking a position on the suitability of these methods for addressing common cause failure, as they are described in Clause 5.16; and they may be appropriate for the use by applicants or licensees and would be reviewed by the NRC on a case-by-case basis. In addition, while these methods may be acceptable to address common cause failure in appropriate circumstances, the provided list is not comprehensive and does not include flexibilities that the Commission directed to staff in SRM-SECY-2276.

CHAIR ROBERTS: Now, when I look at this first sentence, which is what you propose to keep in regulation, it does not say digital. The SRM that you cite at the bottom is about digital common cause failures. The proposed draft rulemaking also references BTP 719, which is a staff guidance document that's also specific to common cause failures in the digital portions of the I&C system.

So it occurs to me that first sentence is more general than the guidance that's cited in the rulemaking document, and the guidance that you're not endorsing basically is pretty high level. It says assess the likelihood and consequence of common cause failures and then look at the likelihood and consequence and make a judgment. That's basically what it says in quite a few more words. And so I'm not really seeing how that's contradicted by the SRM that's cited there, although I do agree that there's more options in the SRM but they seem to, you know, fit within that realm of assess likelihood, assess consequences and make a judgment.

So it just seemed to me as an area where, if you don't consider the IEEE guidance to be comprehensive, then you're kind of putting it on yourselves to go write the guidance that would be more

comprehensive. That's why that's what you intended -- or did you intend just to say that the SRM covers it, and so go follow the SRM instead of the IEEE guidance?

MR. BLAS: So, I mean, the thought process was, given that it's not comprehensive, we didn't want to limit the flexibilities the Commission provided. That was the thought process behind this. That was the intent and the reason why we're going this route.

CHAIR ROBERTS: There's a number of areas you can look at there. One is common cause failures in the non-digital portions of the system, things like power supplies, effects of the common environment, design errors, part substitution errors, operator errors, maintenance errors. There's a whole venue that's documented in other IEEE standards that would not fall strictly in the category of digital common cause failures, and the IEEE has guidance and documents like 352 that gives some wisdom of how you might assess those. And I don't know, if they don't consider those complete, that complete, or whether that also needs to be supplemented by some of the flexibilities that's in the SRM.

So it ends up being a rather complex subject in terms of what will constitute an adequate set of guidance. Again, all I was trying to

understand is the rulemaking the intent to start the process of writing that guidance or is the intent to adopt the SRM guidance as sufficient?

MR. DARBALI: This is Samir Darbali again. So you're right. For non-digital common cause failure, it's different. I think, for the most part, a single cause that would affect multiple channels' performative safety in our hardware base. Existing guidance for equipment environment qualification, EMI/RFI, even consideration for flooding or environmental issues that would take multiple channels. There is guidance that applies to covering that.

So you're not expected, typically, for a hardware-based system or hardware component to be affected at the same time, you know, multiple channels at the same time just by random failure. Again, common cause failure would be addressed by existing guidance and, again, EMI/RFI equipment qualification.

The approach here is to provide a way to endorse the criteria as generic, not just for digital I&C. And that's the first step is always looking at ways in which there's a gap in the guidance that we can consider adding. But, at this point, there is no specific plan to start developing non-developed CCF

guidance.

CHAIR ROBERTS: One example is the ATWS rule, 10 CFR 50.62, that predates digital I&C, and that was, you know, probably a decade-plus long evaluation process that ended up with, essentially, a probabilistic risk assessment approach to determining whether or not the risk to ATWS was adequately mitigated. And that analysis used a fixed-point reliability of the reactor protection system based on a large amount of uncertainty and probably a lot of conservatism coming up with the number you would assume.

So it wasn't a matter of, you know, you did the design and, there, you're good enough. It was you did the design, there was the potential for common cause failures. So if the consequence was severe enough, there still was a perceived need to do more. It's not clear to me how that applies today because that rulemaking was done 40-plus years ago, and the rule itself appears deterministic because the conclusion was made to take the results of that risk assessment and put the design changes that would be required into the rule directly. So now, 40-plus years later, exactly how that applies to a plant wasn't considered back then, and that seems like an

area where that's not strictly a digital question, right, because they got the same concerns that had people concerned 20-plus years ago, which is not so much the potential for digital systems to cause problems but for the reliability of the overall system to be very uncertain based on the concern of common cause failures.

So one aspect of this question is so what are folks supposed to do today both from the staff guidance perspective and a regulatory guidance for applicants to assess the ATWS concern from 40 years ago? So when I look at this common cause failure, that's one aspect of it that occurs to me. I don't know the answer to that question. We had some discussion during the NuScale SAR review, and I read a memo that kind of questions whether the diversity within the digital portions of the system is sufficient to meet the intent of the ATWS rule. In their case the consequences weren't that bad, so the ATWS thought process would say there's no need to do anymore because the consequences. If the consequence is considered unacceptable, then you're back into the same question people were looking at 40-plus years ago.

So, again, how this fits in with the 2022

SRM and the focus on digital common cause failures isn't clear to me. That seems like an area that's worth looking at. Am I missing something?

MR. DARBALI: Yes. It does a little bit more than that. I think the first sentence that it's being endorsed is a bit of a clarification of the language in the introduction to the GDCs. That does say that consideration of possible systematic non-random concurrent failures for redundant elements in the design of protection systems and reactivity control systems, that needs to be considered. So I think that just provides some clarification on that existing criteria.

Again, the rest of the language, it's more guidance. Yes. When you look at it for the digital I&C side, it's unclear whether or not there might be a conflict or maybe an over-reliance in that guidance on likelihood over consequence. And so we're trying to ensure that whatever -- I mean, again, from the point of view of this rulemaking effort, that language is not going to be included in the IPR because it's not a criterion.

From the point of view of guidance, again, at this point, what we have is guidance for the staff in the BTP on digital I&C. We are still considering,

as part of the committee's comments on that revision of the BTP, we're looking at the broader regulatory infrastructure and the need for guidance to applicants. That's something we can consider at that point.

CHAIR ROBERTS: Okay. So the question of whether the guidance that you're asking for in this rulemaking would include guidance on common cause failure and how to assess that first sentence of 5.16, that's within the scope of what you're thinking in this rulemaking, as well as the BTP 7-19 comments that we made last year; is that fair?

MR. DARBALI: Could you rephrase the question?

CHAIR ROBERTS: You are looking at the potential for additional guidance on common cause failure mitigation as part of this rulemaking.

MR. DARBALI: Well, not as part of this rulemaking. So the rulemaking is going to be the rulemaking part and then developing accompanying guidance. We'll determine what the appropriate level of guidance can be provided in a timely manner.

But we are considering long-term how this rulemaking, as well as application of existing guidance, so BTP 7-19 Revision 9. We're looking to

see how that is applied by applicants and staff. There's also NEI-2007, which staff is looking to review. So there are a lot of ongoing efforts that, at some point, we do want to harmonize industry guidance that can accommodate all the staff.

CHAIR ROBERTS: To clarify my question, I wasn't asking about the rule itself. I was asking about the accompanying guidance, which, right now, is kind of all TBD in the way the rulemaking is written. If we got a question from the public asking for the scope of the guidance, what their recommendation would be. I was just asking for that guidance that you're still trying to determine the scope of, were you thinking that you would need to add something to explain how to implement that first sentence of Clause 5.16?

MR. DARBALI: So, right now, staff is currently working on that draft guidance. And, you know, when it is complete, we are going to be providing these draft guides and coordinating with the ACRS to schedule another meeting to discuss it.

CHAIR ROBERTS: Okay. I think that answered my question. Before we leave the subject of common cause failure, the other thing that I wanted to talk about is what Samir mentioned, the BTP 7-19 open

comment that we are still interested in understanding what replaced the echelons of defense that were defined in NUREG/CR-6303, which was previously endorsed in the Branch Technical Position until Rev. 9.

And the concern is you have a failure that affects multiple layers of defense-in-depth. And so the single failure, because of integration of the systems that's enabled by digital I&C, you could have, you know, a common cause failure that would cause impact on many layers of defense-in-depth from the prevention of events to the mitigation of AOOs, to the mitigation of accidents, to the mitigation of public consequences.

As you integrate the systems, you get more and more scenarios where you might have that broader impact. And the NUREG/CR-6303 covered that, but now that's not endorsed without something that replaces it. So that's something I know you're still looking at, and that's something we'll visit again. Charlie.

MR. BROWN: I was going to let you finish. I wanted to backtrack to the common cause failure thing, if I can find my notes. I hate computers. You're not making any fundamental clarifications; that's the statement that you confirmed a minute ago.

And independence is one of channels, and divisions is one of the keystones for analog systems, particularly with protecting you from common cause failures. You can do whatever risk-informed analysis you want to do, but it's fairly unlikely that a single chip, a single doohickus from one division do not fail in two or three of the things all at the same time. That's my version of risk analysis.

But that totally changes when you go to digital systems. Right now, when you look at the independence discussion in 603, it's fundamentally established by electrical isolation. You just isolate everything. You don't connect any electrical signals between various divisions. The exception to that is, obviously, when you get to a voting unit. You have to send -- each division has to go to all the voting units. Even there, a failure in one, either a 1 or a 0 not showing up or an average signal would take, you know, it's not going to destroy the voting units. It's just the nature of the 1s and 0s, contact, closures, et cetera.

But with digital systems, that totally disappears. Digital in one particular channel can have a software data transmission that could literally lock up all four voting units. If it will do it to

one, it will do it to all of them more than likely; I'm making that as a declarative statement. And you've added nothing. It doesn't even address -- electrical isolation doesn't even suffice to approach to deal with that particular situation. And, yet, nothing was done in the rulemaking, in your IBR, to try to focus on the difference between analog -- and now we've added another way of having independence destroyed via the software applications.

That was a little bit bothersome. I don't know how having it in the rule, as opposed to in a guidance, gives it more credence and more legal leverage when you're doing system reviews in terms of what you can do. But, now, if you go try to put more explanation to the guidance, oh, but we really don't need that, and they'll go through a dog-and-pony show to tell you why you're wrong if you insist on something other than what they've provided.

So that would disturb me a little bit in terms of how we don't seem to be recognizing in the new IBR that digital systems provide a different concept totally different from analog approaches. And you all didn't do anything, so that's the decision you've made to go, so that's liable to be a subject of considerable discussion once you get to guidance and

how, I don't want to say deterministic it may sound or how non-guidance it may sound, but something is going to have to be done to make sure those distinctions are made from the application of digital systems.

I'm just passing that on. Obviously, you don't have to do anything with that. And you will not argue me out of my consideration since I dealt with this for dozens of years in my own systems back in the naval program, and we did that in all the plant designs that have come up before us to date and there have been no provision made for that.

Anyway, I'm just throwing that on the table for something you to bear in mind that we'll add that into the discussion process if something doesn't show up in the guidance that takes advantage of fixing that or at least addressing it.

MR. DARBALI: Okay. So just to reiterate, you know, the first sentence makes it so that, you know, there's a need to identify and address common cause failure, and it doesn't specify where that is. It's on the licensee to make sure that they address common cause failure, and this would be part of the regulations.

MR. BROWN: I understand that. But there are certain things that stand out in the application

of digital systems that don't even get -- they're totally foreign from what we do with analog systems; that's all. It didn't seem to recognize that there's a different world, and the purpose here was to bring this up into 2018, which also I was very surprised the 2018 did not provide any digital system guidance per se.

MR. CHEUNG: Part of the approach is to support, you know, Commission direction for performance-based technology-inclusive rulemaking. So then, you know, keeping at this high level, it was 8710 but deferring --

MR. BROWN: I understand performance based and technology inclusive. I mean, I ended having designed the first digital systems we used with analog specs and no software standards and a Zilog Z80 2.3 megahertz microprocessor. Try that.

CHAIR ROBERTS: I think I have a slide on this subject, slide 21. So I think we probably --

MR. BROWN: Oh, okay. I forgot that.

(Simultaneous speaking.)

MR. BROWN: My point being is everything we've ever built has been performance-based. Nothing has changed. You can put all the words into the standards you want to, they're meaningless.

Technology inclusive is meaningless. We've always been technology inclusive. But that's good because that's what we have to do politically, but there's specifics that you really need to get away from those words and think about what you're really doing. That's all I'm trying to emphasize. Sorry. I forgot about the slide.

MR. BLAS: All right. Moving on to the next slide, which is related to 5.16. So we are proposing, the staff is proposing to update, you know, proposing to incorporate Clause 5.16, specifically the first sentence containing the shall statement. In the first bullet, this would make Clause 5.16 part of --

(Audio interference.)

MR. BLAS: Given what was discussed, we're proposing to update 50.55a to incorporate by reference IEEE 603-2018 but not require conformance to IEEE 603-2018 Clause 5.16 except that the safety system design and development shall address common cause failure that create a potential to degrade or defeat the safety system function that is described in the first sentence of the clause.

CHAIR ROBERTS: Maybe now I'd ask two questions about the language that's in the direct rulemaking. I recognize that's something that you're

still evolving.

But one thing is the rule says you don't need to comply with the rest of 5.16, but the rationale is you would evaluate it on a case basis whether it's acceptable to comply with the rest of that? That seems to be -- if your rationale is you're not sure you would agree with the design that complies with just the guidance, but then you say you don't require compliance with the guidance. That implies it. So I would go above and beyond your expectations by complying with the guidance. It's not clear. It seems like you're really saying that you're already endorsing the first sentence and the rest of it you're not passing judgment on it at all.

I was just wondering if you look at it that way or whether I was just reading what you wrote. Not required to comply with is different than you're not even sure you'd accept it, somebody that complied with it.

MR. BLAS: So with regards to the portion that's not being incorporated, again, just restating it. It would be evaluated on a case-by-case basis, and it could be an acceptable way of meeting that criterion. Again, just to reiterate, it would have to be evaluated by the NRC staff --

CHAIR ROBERTS: I understand that. That's not what the words say to me. Just something to consider. Take a look at the words. If you think I'm out to lunch, that's fine, too. But, in my opinion, saying you don't need to comply with something kind of implies that, if you did comply with it, you would be better, as opposed to it may not be sufficient, which is what you're really saying.

MR. BLAS: But the intent here on how we are incorporating it into the regulations is the fact that you are required to address the first sentence in the clause, and it's going to be in the regulations. That's the intent, yes.

CHAIR ROBERTS: Okay. Yes. The second point I wanted to make is the preamble due to the roll up, when it talks about common cause failure, it implies that the BTP 7-19 and the SRM are the guidance that the NRC applies. Again, the word the, I might be over-reading, but, when I read the, that implied to me that that was the exclusive guidance that I don't think that's the case. I think, as we talked about at some length earlier in this meeting, there were some evaluation ongoing whether or not there needs to be more guidance for common cause failure.

So you might want to look at the word the

to see if that's really what you meant, as opposed to the guidance includes these documents and not that these are the exclusive guidance. So again, somewhat detail points, worth looking at.

MR. BLAS: Thanks. Any other questions on this slide before we proceed? Okay. Given that, I'm going to pass it over to my colleague, Calvin Cheung, for the rest of the presentation. Thank you for your time.

MR. CHEUNG: Now we're transitioning to the regulatory history to give some additional perspective into the rulemaking. There are four broad topics, the first being the protection and safety systems. Then I'll go into the treatment of referenced standards, which you've also maybe heard referred to as normative references or secondary references. I'll cover that there. Then we'll discuss the ACRS recommendations from the previous rulemaking. And, finally, I'll talk about the non-concurrences from that previous rulemaking effort.

So the term protection system was first defined in IEEE 279-1968, and this standard predates 603 and it was incorporated or is incorporated -- sorry -- into 50.55a(h). And it states in the scope that the protection system encompasses all electric

and mechanical devices and circuitry from sensor to actuation device input terminals involved in generating those signals associated with protective function.

And in IEEE 279-1971, which is also incorporated, the standard clarifies the term to include the actuator system so that it, I quote, consists of the protection signal system and the actuator system.

In IEEE Standard 603-1991, a safety system is defined as a system that is relied upon to remain functional during and following design basis events to ensure: 1) the integrity of the reactor coolant pressure boundary; 2) the capability to shut down a reactor and then keep it in a safe shutdown condition; and 3) the capability to prevent and mitigate the consequences of accidents that could result in potential off-site exposures comparable to the 10 CFR Part 100 guidelines.

Next slide. So in terms of the relationship between these two terms, this first bullet here is from the preamble to the 1991 rulemaking. And it states the NRC recognizes that protection systems are a subset of safety systems. Safety system is a broad-based and all-encompassing

term embracing the protection system, in addition to other electrical systems. Thus, the term protection system is not synonymous with the term safety system, and the final rule is not intended to change the scope of systems covered in the final safety analysis report for current operating nuclear power plants.

With the 2018 rulemaking, we will follow the same approach and utilize the same language in our preamble. And the definition of protection systems and safety systems will be unchanged, and the preamble will be restated consistent with what's showing here.

MR. BROWN: In other words, you're saying they're synonymous? I reread the first slide again after I went through this. Are you saying protection and safety are now to be defined as synonymous with each other or you've got a distinction?

MR. CHEUNG: No.

MR. BROWN: I don't understand the distinction as well as I should have probably.

MR. CHEUNG: This is meant to be a bar term, so that is --

MR. BROWN: I've never done that, that's why I ask. They've always been synonymous to me.

CHAIR ROBERTS: There may be some background useful to explain why they were talking

about protective systems and safety systems.

MR. BROWN: Yes, but I understand the nuance.

CHAIR ROBERTS: The rulemaking applies to protection systems, applies to licenses before? Was it 1999?

MR. BROWN: Yes.

CHAIR ROBERTS: And then the rule applies to safety systems for plants licensed after 1999. It's kind of a head-scratcher because they all can use IEEE 603-2018 or 1991, but they can use them for protection systems for the earlier licensed plants and for safety systems for the later plants. It's a little confusing, and my understanding is it's somewhat historic that you've got, you know -- once you put something in regulation, it's very, very difficult to change it, and so you're kind of stuck with the legacy of this is what the rule language said before 1999, so you're kind of stuck with that, and this is what the rule language was allowed to say once they changed it after 1999.

So you sort of have to recognize when you read that 55a(h) you're reading kind of a mess in terms of parsing. You almost need a Venn diagram or a matrix to figure out exactly what it means. But it

is what it is, so I think it's a good explanation.

CHAIR ROBERTS: I just never worried about it. To me, a safety system is there's a broad category of safety: the reactor protection systems, then there's the fluid systems, there are other systems you use that are also safety systems but they pump water in or whatever.

CHAIR ROBERTS: And I think also it practically ties what Samir was saying earlier: once you do a retrofit and you're into this kind of mess . You've got a IEEE 279-1971 plant developing a digital I&C system that wasn't envisioned for an IEEE 279 if it was written in 1971. There's still a way for the staff to work through the appropriate guidance, so it's, basically, it is what it is, I think, is the simple explanation.

MR. ROGGENBRODT: Chairman Roberts, Bill Roggenbrodt, I&C. Also, in preparing for this meeting, looking over those terms as they were defined, going through starting with IEEE Standard 279-1968 and continuing on into 1971 as was stated, that the protection system was the term that was utilized and include both the protection or the sense of command features, as well as the actuator or the execute features.

What evolved over the years was 279 changed into IEEE 603. It was a trial-use standard in 1977 and then was actually adopted as a regular standard in 1980. In looking at the information when 1991 updated the 1980 standard, it said that, actually, at the request of the NRC, that the safety system term was utilized to align with the term of a safety system in accordance with 10 CFR 50.49 and so that they match each other.

So from that, you're quite correct. Historically, when we define protection system, it includes the entirety of the protection system from and including the sensor all the way through the final actuation device. What changed over the years was actually the definition of the broader term safety system. I believe, in the forward, it says, you know, to accommodate this, we're actually referring to the term safety-related system as is defined in 50.49.

So to your point, it is a head-scratcher until you do the research to see how we got here.

CHAIR ROBERTS: Okay. Thanks.

MR. CHEUNG: Thank you for the addition, Bill. Next slide.

So as previously mentioned, I want to talk about how we are addressing referenced standards. As

you're aware, sometimes they are also called normative references and secondary references; but, regardless, we're going to be treating them the same way and they will not become requirements simply by the fact that they are listed in the standard. So we are incorporating IEEE 603-2018, but that does not encompass or include any other references that may be found in the document.

In some cases, these reference standards can be endorsed by the NRC and have been endorsed through reg guides, so that is still an option available. But those are handled separately and independently. And this treatment of reference standards is consistent with how the 1991 rulemaking handled them.

Any questions?

CHAIR ROBERTS: I mean, there is a precedent for this. The word normative wasn't used in the 1991 version, but their references are pretty integrally involved with the standard. When you read the IEEE standard, I'm just reading from the section two, normative references, it says applying reference documents are indispensable for the application of this document, i.e. it must be understood and used. Each reference document is cited that has a

relationship to this document is explained.

So it kind of leads me to wonder are you really using a consensus standard when the consensus standard says you must use the references? I recognize that the NRC staff typically clarifies references in reg guides. This is a regulation, so you've got kind of a mess with how you would clarify, you know, a regulatory reference in a regulatory guide. It doesn't necessarily make a lot of sense. I understand why you're doing.

I was wondering do you have any perspective on a statement that you're not really using the consensus standard because the standard says you must use references and you're saying you're not adding the references.

DR. BLEY: Tom, this is Dennis. The point you just made I really agree with. It seems to me if you incorporate this standard by reference and it says you must use these others, either you must use them or the staff ought to have their own guidance that replaces them. And the fact that nobody has decided that yet seems like a gap.

CHAIR ROBERTS: So, again, other than the language was strengthened in the IEEE standard, those words were not in the 1991 version, but I think people

are going to argue that's what they meant, which they didn't use those exact words. So I'm not sure there's an answer to that question because it is a historic, you know, it's what you've been doing since at least 1991 and probably before then. But it's just something to think about.

The suggestion from the NEI that IEEE 603 should be a regulatory guidance, as opposed to requirement, that might be a reason to think about that because at least that allows it to be in your regular regulatory guidance structure where you, you know, specifically endorse each reference with whatever caveats you think you need. I'm not a lawyer, I don't know how you would use a regulatory guide to clarify a reference that's in a regulation, so it seems like you're kind of stuck.

Again, it's just a thought. It's not new.

MR. ROGGENBRODT: Bill Roggenbrodt, I&C. So from that vantage point, you've got what's in the incorporate by reference rule itself; and then those other items that are not included, they become a secondary reference. And by being a secondary reference, they may be utilized, but they do not have the same enforcement level as a rule would. So it's not that they won't be examined and evaluated. It's

just that it's referred to as a secondary reference, if I understood your question correctly, sir.

CHAIR ROBERTS: Just one random example. In the standard, Section 5.6, independence test, IEEE Standard 384 provides detailed criteria with the independence of Class I equipment. So you have a reg guide, I believe, IEEE 384, so that's been endorsed by the NRC staff and not as a requirement. But this now says it is a requirement, except you're not endorsing the references, and so the requirement, basically, doesn't exist. Again, it's a bit confusing.

I think, getting back to what Samir said, at the end of the day, you end up assessing independence by that IEEE standard with other parts of your regulatory rules. But it's, you know, it's hard to say it's a requirement of IEEE 603 when the requirement does follow the reference and the reference is not endorsed.

MR. DARBALI: This is Samir. The standard uses past references, it uses sort of different language. So it says provides detailed criteria or see the standard for additional guidance or this standard provides guidance, those sentences are pretty clear that it's not mandatory. So unless there was a clause in the standard that says the DRMs following

this standard shall be implemented or, yes, you shall follow this other IEEE standard, that, I understand, would be problematic, but I believe that's not typical language in the standard.

DR. BLEY: Well, there are several examples of it. If you just search for the word must, you'll find them.

MR. DARBALI: Understood.

CHAIR ROBERTS: Yes, just a random search. Safety systems shall be designed for periodic testing in accordance with IEEE Standard 338 is one example.

MR. DARBALI: I stand corrected.

CHAIR ROBERTS: This may be a longer-term question. I know you had a meeting this morning to talk about the potential of moving this whole regulation into guidance and just something to maybe consider as part of that.

MR. CHEUNG: Next slide. Now we'll move on to the ACRS recommendations from the 2009 rulemaking efforts. And before going to the recommendations, to provide a little background, just to make sure we're all on the same page, in 2014, there was a rulemaking effort to incorporate by reference IEEE 603-2009 version. It was presented to the Commission and it was not approved. The

rulemaking had expanded scope. It created additional conditions and requirements, some of which were specific to operating new reactors beyond what was included in the actual standard language.

With the 2014 rulemaking, the ACRS made several recommendations and there were also several staff non-concurrences that I will also discuss. Before we kick off this 2018 rulemaking effort, one of our primary objectives was to review all these recommendations and non-concurrences to see if they've all been addressed and are still applicable.

So this first recommendation, this was marked as Recommendation 2. I'll add Recommendation 1 was to develop guidance incorporating all of the other recommendations, so, you know, I won't really specifically address that one. But Recommendation 2, this one is dealing with specifying the rule, the use of an independent hardware-based diverse means to produce a diverse trip, the effective redundant portion of the digital safety system if the common processing unit ceases to operate or locks up.

In the staff response to the ACRS letter, the second source shown at the bottom here, the staff concluded that existing regulatory requirements address the scenario described above and some of the

requirements included GDC 20 for protection system functions and GDC 23 for protection system failure modes. And shown in the second bullet, staff is evaluating the development of accompanying guidance and what to include with that in the rulemaking to provide any clarification to go with this rulemaking.

We started this conversation earlier. I don't know if there's more to add to that.

MR. BROWN: My comment earlier was just the fact that we made no illusion that there's a whole different world of development of I&C systems in the digital world than there are in the existing rule guidance, not guidance but the rule effectively focuses on independence with electrical isolation, and that's not the case now. Forget the details. It doesn't say it's not the same, and there are other modes or there are other failures that can result as a result of digital systems, not just electrical connections. I thought that was a mistake. Wrong words. Not a mistake. Something that should have been included to recognize that digital systems provide another venue and world of failure modes that have to be considered, not specifics or specific solutions.

If you really sit back and look at the

most likely one, this is the one if you don't have hardware, as opposed to software. I have never heard in the last 16 years a single comment that had any proposal other than that for solving the lockup of voting units. It's too specific. Nobody ever proposed anything to do the same thing in all of those. In every one of the applicants that came in, three of them resisted it, the committee objected, and they incorporated it into their design. And I'm not saying that's perfect; it's just, for this purpose, I thought the recognition of the difference in independence for software systems is different than that for analog where electrical isolation provides a pretty good basis for having good independence between the channels or divisions of the protection systems.

So that's my point here. I won't elaborate. I just want to differentiate it from the specific to the more general basis.

MR. CHEUNG: Thank you.

CHAIR ROBERTS: Charlie, what I think you're saying is they were looking at in guidance to make sure that people look at that as a potential common cause failure because, clearly, we have a voting unit and that's where all the channels come together. And no matter what the technology is, you

need to look very carefully. It doesn't matter what the technology is –

(Simultaneous speaking.)

MR. BROWN: Well, the hardware, we had decades and decades and decades of multichannel voting units, and all I know is, in my entire career of 35 years, I never saw any report where we had common failure hardware-wise that was separated with the software basis for cause of the nature of the interrupt-driven systems and all the other type stuff you have. You can come up with software failures or data, stream of data, that can lock them all up; and, once it goes to all of them, they're gone. And I just think that fundamental difference ought to be reflected in the rule, not as a specific or how-to but it's different and you need to address that and tell us how, that's all, because we do, from the analog standpoint, we say electrical independence. Here, we say nothing, totally silent; and that's where the IBR, not specifics but addressing the software computer-based issue, to me, was an important thing that you should have included in that particular -- which section was it? 5.16. Yes, 5.16. Yes. So that's why I mentioned it three times now.

I really think you ought to reconsider

that because it doesn't add requirements, it just says it's a different world and you need to address the differences, but 2018 does not cover that. I was totally surprised that the IEEE didn't cover any digital type systems. I mean, that's so current, I can't believe they blew that out their stack. I'm sorry for my strong words and sorry for my strong opinions. No, I'm not sorry. I take that back.

MR. CHEUNG: Thank you. This slide addresses Recommendation No. 3. It relates to 10 CFR 50.55a(h)(4) for the proposed rule. It recommends clarification for both predictable and repeatable, which means processing from the safety data input to safety control device actuation and independent of the redundant portions of the safety system or other external input.

In the 2018 version of 603, Clause 5.5, system integrity, includes the following requirement which we feel meets the intent of the ACRS comment that safety functions shall be designed to have deterministic behavior and timing. And this was something that was an enhancement from the 2009 language.

MR. BROWN: I like the deterministic word you added. That's the only real difference based on

what you've said here. You've added that word in in front of the predictable and repeatable, if I'm comparing the two paragraphs. I don't have it open in front of me, so I'm extrapolating that that's what you're saying.

The problem, even with the earlier recommendation that we made, and I'll only address this back in terms of one specific project we looked at when we asked about the time response, predictable and repeatable, the answers we got back only addressed the controller, the computer-based unit. It did not include sensor to actuation. And what we should have said back in 2014, we should have added in from sensor to actuation device because the computer-based stuff is in the middle and there are other things that it may go through from any particular point before it gets there. So, to me, that's the only other wrinkle I would have thrown into this if I was making a suggestion on this one.

Deterministic is a nice way to phrase that. It's not as fuzzy as just predictable and repeatable. Some people would argue that computer-based systems are predictable and repeatable. Well, it depends on how you program them. If you program them with lots of interrupts, you never have any idea.

When we asked the question on one particular controller that was used -- I forgot, well, I actually know, but I don't want to bring up the name of the project and/or the device, the controller. I asked the question, well, how much application code can you load into your timing cycle? 200 milliseconds. How much of that cycle can you use with application code? They didn't have an answer. They had no clue. Well, they came back on another meeting and, oh, only 70 percent because they couldn't predict whether it would finish or not with all the interrupts. I don't know how they ever got there, but they ran a bunch of testing. Whether it was inclusive, at least it was an answer. And, actually, there was a subsequent project that used that same controller that then did additional testing and said, hey, based on the progress of our software path, we can actually use 75 percent.

So that's a nuance in terms of how these things operate, and that's not deterministic. That's non-deterministic. Deterministic really means very straightforward: this is all you've got, and you can go no farther. But it still ought to be sensor to actuate, through the actuator. That's the only suggestion I would have -- I can't believe I didn't

say that in 2014, but I didn't.

So, anyway, I'm just mentioning that's the thought process on what you can do.

MR. CHEUNG: Thank you. Anymore questions?

This slide addresses Recommendation No. 4. It states that the proposed rule should specify additional condition addressing Section 5.9 for control of access and identifies communications external to the plant should be accomplished using one-way hardware-based devices, and these devices should neither be software configurable nor capable of alteration by external commands or any surreptitious means.

MR. BROWN: Good words.

MR. CHEUNG: End quote. So the staff agrees that this approach is an acceptable approach, but including it as part of the rulemaking would be, I think that I alluded to it before, it would be prescriptive and not meeting the Commission direction to support a performance-based and technology-inclusive approach.

That being said, there's also been revisions to guidance documents in Reg Guide 1.152 and staff guidance BTP 7-19, which addressed

communications, independence, and control of access, and these have been communicated to the Commission in that third letter referenced in the sources back in 2021.

MR. BROWN: I will comment on that, just to give you -- since you weren't here, I don't think. When we started insisting on this, we actually brought this up back in 2010 on another project that I won't mention, along with the watchdog timer issue, a similar type thing. And the applicant strenuously objected to that because it just wasn't a problem. There would not be any problem with the unit directional things, and nobody ever proposed an alternative that would solve the control-of-access issue for external access, how they would fix that if they had bidirectional communications, other than, quote, the standard virus cybersecurity world, which it's been obvious over the last 20 years that that doesn't work.

So that was the reason we then wanted to try to get it -- trying to just put it in the guidance, I can just hear somebody, well, we risk informed and evaluated this and we can handle this in other ways and we're not going to bother to tell you how, but that's okay. And you're stuck. You've got

words that say all you have to do is not have a problem, but nobody ever presented any alternative method other than this, not a single one. No software processes, no other alternatives how you would do it. The only thing you can do is keep the door closed, and that's why we were somewhat specific when we made that proposal.

This still leaves it open-ended, and you will have to fight about it, particularly if they start integrating these systems more, which is another issue which is not really brought up in this. We didn't bring it up in that either. Summed up, one guy did, way back in 2010 or '11, the project went away, so we didn't have to deal with it. They really wanted a more integrated system where they had multiple functions incorporated in their overall system, which was not very good. But it died before we had to say anything.

Anyway, the guidance is squishy. The rulemaking is not law, but it is rule. And nobody in the last 16 years or 18 years has provided any method for ensuring external access. It's easy in the analog world. You just close the doors and put locks on them. This is the worst of the worst, totally hackable if you allow -- I mean, you can communicate

data into a network in the plant, as long as it's one-way hardware. It's not like the whole network and everything else has to be that way, depending on how they're using it. Personally, I would never put it in a network before it went to the main control room. It ought to go directly, but that's another issue in terms of detailed design that we don't specify. Normally, we don't even know what the main control room looks like, other than a couple of network-type configurations, you know, dual, redundant, whatever they want to call them.

So, anyway, this is fuzzy logic on this thing.

CHAIR ROBERTS: And I think the question is whether they have the regulatory toolkit they need to enforce the requirements. There's the security requirements, the cybersecurity requirements, the overarching requirement. And then there's implementation, and it sounds like what you're saying, in 16 years, nobody has ever done it a different way and been successful at, you know, enforcing the standard.

MR. BROWN: Well, when did we finally -- Christina, do you remember when we did 5.71?

MS. ANTONESCU: When we started, I --

MR. BROWN: The final run where we finally got it into an acceptable approach up in the lead-in paragraph of 5.71. They originally were told we could never deal with this because it was a programmatic issue and could only be dealt with five years after the equivalent was designed and installed in the plant. It was a programmatic issue, 73 point, I don't know, one, two, three, or four, one of those.

MS. ANTONESCU: Fifty-four.

MR. BROWN: Fifty-four? Okay. I mean, it was hard for the staff to even recognize that in the cybersecurity reg guide. We did get it into, I think, you know, you mentioned it, 1.152 also. So those were compromises because we couldn't get it into the rule in 2014. We emphasized getting it into the reg guides after the fact, so not as backdoor as we would like but at least it said an acceptable approach is and, if that doesn't send a message to the applicants, I don't know what does.

Anyway, I just wanted to throw that out from an educational standpoint to bear in mind. This is not just an innocuous committee desire to be holier than thou. That's the worst -- I don't know. I mentioned it to somebody. Of all the things that have come on, that's the worst. Any internet connection

anyway is going to be a crusher to attack stuff in the plant where you don't need it, other than going directly to the SCRAM system or the safeguards actuation and/or data up to the main control room. Anyway, I had to have my soliloquy on my soapbox.

CHAIR ROBERTS: Checking the time, we've got three slides to go, so we would think about taking a break around right now, but I think we should plow ahead --

MR. BROWN: For the hard slides.

CHAIR ROBERTS: So let's keep going. We should be able to maybe finish and get into public comments before we take a break. Go ahead.

MR. CHEUNG: Sure. Now we'll move into the non-concurrences from the previous 2009 rulemaking. This first slide summarizes non-concurrence 2014-001 and 2014-003 and concerns the impact having different communication requirements for new and operating reactors.

MR. BROWN: Which communication are we talking about in that one? The one with the digital communication? Software-based? Because data communication, to me, means either an analog voltage signal going to a meter on a panel or a digital signal that initiates from the monitoring systems: pressure,

temperature, flow, level, whatever they are. But the backfit stuff that we looked at reapplied the same rules to them or guidance to them that we applied to the new applicants. If you look at Diablo Canyon, we talked about the same type of an issue in terms of -- I don't understand the difference, I don't see a difference between new reactors and old reactors. Is it the DSRS routine?

MR. CHEUNG: It was accompanying with the 2009 rulemaking in the FRN, there was a subpart C that said, for current reactors, communication signals from an outside safety division during operation must support safety and provide a safety benefit. And then for part D, for new reactors, it goes into a pretty long list of data communications between safety and non-safety: must be one-way, accomplished by a physical mechanism, signals may be shared between redundant portions, safety system may receive signals from non-safety in operation only if the received signal supports diversity and automatic anticipatory reactor trip functions. Applicants for design certs, standard designs, and manufacturing licenses who propose an alternative on this -- paragraph C.

MR. BROWN: So that's an FRN from 2009?

MR. CHEUNG: So it was saying the staff

concerns were with our additions and additional conditions to the 2009 for having different requirements for different types of reactors.

MR. BROWN: Well, we never thought about that when we were doing the backfits, as well as the new applications. I don't remember that. Samir, were you -- no, you're too young for that. That's not a negative, by the way. I'd like to have your age back and a young body to go with it.

We've been through both backfits and all the new applicants, you know, from AP1000 to APR1400 to NuScale and Diablo Canyon, and the only one I know we didn't get to dabble in was Oconee because we never reviewed that one, we never got an opportunity. Whether it's good or bad, the staff decided we didn't need to do it, and they sent it out. Actually, it just arrived. Oh, what's that? It showed me a diagram, and then it was approved. We didn't even have a meeting.

After that, it was obvious and we applied the same rules. There was one other backfit also that we looked at.

MR. CHEUNG: All right. I mean, I think it was, you know, at the time, we were new reactors, operating reactors, so there was a lot of different

perspectives.

MR. BROWN: I didn't realize there was a difference. I apologize for being -- I'm not being obstructive. I just was not aware that it was that explicit between some new reactor, and that's in an FRN you said?

MR. CHEUNG: That was in the proposed rule language with the 2009 rulemaking.

MR. BROWN: Oh, yes, I wasn't here for the 2009 rulemaking. I mean, I was but wasn't aware well enough to handle that at the time. Thank you.

MR. BROWN: Did you want to add a question?

CHAIR ROBERTS: No. I just wanted to clarify what they're explaining is that the rulemaking, the proposed in 2015, was not very clean like the current one is. And there were some different approaches to new reactors and existing reactors, and there was also, you know, several additional requirements were supposed to be added and had led to, I think it was four staff non-concurrences that went up with that rulemaking. And the committee said, basically -- the Commission, rather, basically said go figure this out with the IEEE folks and work amongst yourselves and come up with a more common

position, if you can.

Why they're talking about this now is there are no additional requirements, and there is no non-concurrence this time. So it's just a matter of --

MR. BROWN: Well, it doesn't do anything, though. I mean, it's easy to not have any non-concurrences --

(Simultaneous speaking.)

CHAIR ROBERTS: It's also a perceived desire to add that stuff that's not there anymore, so that's also important. Calvin.

MR. CHEUNG: I guess the point was we were trying to make sure that, whatever the concern was, that it was not still an issue. So our approach is different, like you mentioned. It does not have those additional conditions, so this is no longer an issue.

This slide covers non-concurrence 2014-004 and also 2015-001 and addresses the lack of requirements for an independent and diverse architecture for highly safety-significant digital system support of the implementation of a defense-in-depth approach. So the staff recognizes there's been potential changes in policy -- sorry -- recent policy: in SECY-SRM-2276 which provides digital I&C CCF policy

and allows for the use of risk-informed approaches to demonstrate defense-in-depth and establishes the agency position and IEEE 603-2018 does not include specific diversity requirements and staff did not see it necessary to include or expand on that as part of the rulemaking.

MR. BROWN: Is this the last slide or next to last?

MR. CHEUNG: The summary is after that.

MR. BROWN: What's a risk-informed design? You turn a switch and something may or may not actuate if you've made a risk-informed design? I mean, the software may or may not complete its cycles when it's supposed to maybe? Yes. Samir, you were going to say something. I've never seen a risk-informed design. To me, you can have three channels or four channels; that's risk informed. There's a lot of plants with three channels.

MR. DARBALI: You're referring to the last bullet.

MR. BROWN: Yes.

MR. DARBALI: So that refers to, in SRM --

MR. BROWN: I'm well aware of that SECY.

MR. DARBALI: So before it was a deterministic approach, use your best-estimate

methods, and so we expanded policy to allow the use of risk-informed approaches. But it's not risk-informed, a risk-informed architecture design. It's just the approach to determine that a CCF is addressed or it's out of consideration.

MEMBER KIRCHNER: Charlie, this is Walt. It's rather a misnomer. You're right, and so is Samir. It's more of a consequence analysis using risk, you know, PRA-like techniques than it is a design approach. I mean, they can iterate and improve their design based on the consequence analysis of a common cause failure somewhere in one of the systems or components and so on, but it's really not, it's not, quote, unquote, a risk-informed design. It's more can you live with the consequences of that common cause failure or can you not? And then you go back and redesign, obviously, if you can't, if the consequences are unacceptable.

MR. BROWN: That part of it I can sign up with. It's the generic use in the instrumentation control reg guides, et cetera, et cetera. The electrical instrumentation systems of risk informed does not say that explicitly. It's more generic and, quite frankly, I've never -- oh, that would be nice if I spoke into the microphone. Okay. But the cord is

not long enough.

Anyway, I understand that, Walt. It's just that not explicitly understood in the context of how that SRM was written. It's so generic, it covers the whole panoply of applying digital systems will be considered in a risk-informed design approach, and I've never in 35 years ever had a risk-informed design approach to any piece of equipment we never designed. You can determine whether you need it or not, that's a different issue, but not the design of the equipment. That's why I've always objected to that very overwhelming risk-informed comment that came back in the SRM. We couldn't do anything about it because that's what the Commission wanted to put out. But just bear in mind, somehow, I think you, as the staff, are going to have to figure out how to make sure that does not get misused, and that's going to be difficult because there's going to be people coming in to tell you my software is so good that you never have to worry about it, and I've got a nice bridge I can sell you that's made out of gold and I'll charge you for it.

Anyway, that's it. I'm done.

CHAIR ROBERTS: Yes. And I spent some time earlier talking about common cause failure

mitigation guidance, and the reference to BTP 7-19 and the SRM as the NRC guidance, I think Charlie just gave you another example of where you really need to be careful not to conclude that is a complete set of guidance as to how you design a system that emphatically mitigates common cause failure.

MR. BROWN: In fact, it's pretty good. I mean, staff did a decent job, and I think the committee did a decent job of working on that with you. We were kind of working together. Oh, I'm sorry, I turned it off. We worked together on that pretty well.

CHAIR ROBERTS: Well, we might as well let you go to the summary and then we can --

MR. BROWN: One other point about performance based. You've got to figure what we mean by performance based. I mean, it's got to respond in a certain time. It's got to have a certain accuracy. You've got to meet the ranges of operation that you have to deal with, and you've got to be able to test it. In everything we ever build, and I'm back in the building mode now, okay, is performance based.

So, again, those are fuzzy-logic words that are kind of meaningless in the SRM and every place else, but they're good buzzwords and they sound

good politically. I'm being very unfriendly with that particular comment.

All right. I'm sorry. Anyway, that's good. Thank you. We're finished? Or the summary.

MR. CHEUNG: Next slide is the summary. So, in summary, the staff is preparing rulemaking as an immediate solution to meet industry needs, for providing regulatory confidence, to use the updated standard in parallel. We are evaluating today's recommendation on 50.55a(h) and continuing interactions with industry, along with other ADVANCE Act activities. And based on the preceding evaluations, the staff concluded that IEEE 603-2018 is technically adequate and, therefore, recommends the incorporation by reference of the entirety of the standard into 50.55a(h) with only the first sentence of Clause 5.16. This would align to existing CCF policies and guidance, and IEEE 603-2018 would be applicable to new applicants and current licensees, as we have discussed, should you choose to adopt the new version.

And the regulatory treatment of reference standards or secondary references will remain the same, as well as the scope of systems covered in the FSAR will remain unchanged. Staff is developing

accompanying guidance with the rulemaking to provide additional clarification to industry with this rulemaking.

Questions.

CHAIR ROBERTS: Are there any other questions or comments from the members or consultants?

MR. BROWN: I just have one on the -- just an understanding. 2018 is not very different from the original. But what I forgot when I went through and read it, the reg guides are not referenced in that. Are they referenced in the IEEE standards or not? They're not, are they?

CHAIR ROBERTS: That was the whole point of the normative references discussion that the references -- if the IEEE standard were endorsed to the reg guide and the reg guide would say use the following other reg guide when interpreting the reference, but this is the regulation, which makes it kind of inverted. You can't be referencing regulatory guides in a regulation. That would be --

MR. BROWN: No, I agree with --

CHAIR ROBERTS: So you've got kind of a problem in terms of you think the reference documents are important more than reg guides, you don't have a direct way of putting them in the regulation.

MR. BROWN: I just worry, you know, we've got the points. We're concerned about -- what the committee has been concerned about, in the reg guides and the BTPs and the DSRS is replete with architecture statements, or at least it used to be when I last looked at it, as well as references to the issues we discussed in here. It's just that they're not in a rule anywhere. Staff reviewed documents, DSRS, design specific review standard, et cetera, et cetera, which leaves them open to being argued about and contested. I'm just trying to communicate that, in the four projects that we did, the applicants tried to resist these common-sense approaches to fixing the problems we talked about.

I mean, I'll be dead by then. So will they come around? Maybe. It's just I think the staff has to be willing to look at these on a hard basis when these designs come in -- I'm preaching right now -- in fact that they're guidance. And when they object to some of these ones where there is only one way to go do something and that's deterministic and it's prescriptive, but you have to grow backbone when you get to those. We did in four separate circumstances, and they're trivial. When you look at it from the overall design of the systems, they are

trivial. But a uni-directional communication device. Okay. It's $29.95 wholesale. I'm kidding. I just threw that out there.

So, I mean, you just have to be -- and the watchdog timers, that's so common sense that it can't be built into the software or the processor itself. That's insane. It has to be a separate monitor to ensure that it actually completes its whole cycle.

And what you do with that is another issue. It can either reset or it can issue a trip. It can either SCRAM or it can just be an alarm. There's all types of an indication. With the computer-based systems, if you go reset, when we ask them on this one controller how long, they said, oh, it just resets when this thing happens. Well, how long does that take? Eight minutes. So the operator, he's without any data for eight minutes, that's really great.

I mean, you got to think about it in those terms. That's all I'm trying to get across. Okay. I'm finished with my soapbox now.

CHAIR ROBERTS: Do we have any other comments? If nothing in the room --

DR. BLEY: Yes, it's Dennis.

CHAIR ROBERTS: Go ahead, Dennis.

MEMBER KIRCHNER: Just a clarification, Tom. This is Walt. For Samir or anyone on the staff, so I'm assuming, when this rule is implemented, then the 603-2018 would become under 50.55a(h), the requirement for all new construction permits and operating licenses post the date of the rule. Is that the intent in terms of the formalities of the regulation, or does it remain optional in some sense? I understand it for the existing current fleet that they're accepted and they can choose, but, say we have a new advanced reactor application, then we would go against 603-2018.

MR. BLAS: This is Gilberto Blas. Just to answer that question. So for new applicants, 603-2018 would be a requirement for the new applicant. For current licensees, given that, you know, they're tied to whatever they have in the current licensing basis, it would become optional to do the 2018 standard.

MEMBER KIRCHNER: Right. Okay. Good. Thank you.

CHAIR ROBERTS: Okay. Dennis.

DR. BLEY: Yes. Three things, one of them is a question. The first one, Walt's previous explanation to Charlie about what's a risk-informed system, I would just comment that we haven't, as a

group here, looked at the standards 5.16 and the things after the first sentence. They're pretty benign; and, basically, they say, if the consequence is low, that's probably good enough and, if the consequence is not low, if the likelihood of it occurring is sufficiently low, it might be okay, which is close to what was defined earlier.

But those are pretty benign and pretty wide open, and I still don't understand why it seems like it would be restricting the flexibility of people to work within the rule with the standard without those. It really jumps out at you when you read the rule of we're only going to take the first sentence because the rest of this is troublesome. I don't see the trouble. That's number one.

Number two, a little clarification on Charlie's discussion on the hardware diode for data. We fought that over and over and over again, it's been two or three years now and probably more than that. Some years ago, we wrote a letter, the staff wrote back and said we were wrong. We responded to that, and they came back again saying, well, we can't do anything about it. And we sent a third letter, and that one we sent to the Commission to try to get there. So we've really fought this thing to the

ground many times. In places where the committee has won has been on specific licence applications, and maybe that's where it keeps ending up.

The final thing is on this last slide. I'm a little confused because Tom and, I think, several of the staff members went round and round about are we going to get guidance to explain things a little better, and it kept sounding like maybe and one day we'll look at it. And, here, they're saying gin that last bullet, yes, there will be accompanying draft guidance; so I'm a little confused on that. If anybody would expand on that one, that would be great. If not, we can live with what we got.

MR. BLAS: Hello. This is Gilberto Blas. With regards to the accompanying draft guidance, you know, staff did reconsider their approach and we have decided to move forward with developing draft regulatory guidance with this proposed rulemaking. Right now, again, just to reiterate, we're currently working on that draft guidance, and there will be a public comment period for this and there will be engagements with ACRS to --

DR. BLEY: That makes me much more comfortable because it seemed as if you guys were resisting the idea earlier. So we look forward to

that.

CHAIR ROBERTS: Yes. Dennis, I think the question was whether the draft guidance would include more on common cause failures, and I think we've, and maybe I'd ask Samir, I think we've done versions of that, it will be something we should look at, and pointed out the language in the rulemaking draft needs to be clarified that that is something you'll look at or whether it's interpreted as we think this guidance is sufficient and getting your final 5.16 in there. It conflicts with 5.16, so we're going to take most of 5.16, and I think that also needs to be re-looked because I tend to agree with you. I think, at the end of the day, whatever guidance they write probably will be at least consistent with, maybe in addition to or, you know, tell you more how they assess low likelihood or low consequence, but I think, at the end of the day, it's going to be largely aligned with a fair amount of detail. And that's just a guess on my part but, you know.

I think the outcome of today's subcommittee, the outcome of today's subcommittee is there's a general alignment that this needs more look. You know, given that this is a draft proposed rulemaking that's going to go out for public comment

and come back to a final, you know, draft before it goes back out for final rulemaking, that seems like a pretty good outcome of today's meeting.

So, again, Dennis, I don't think I disagree with you on the 5.16. When I read that text, the thing that jumped out at me was the low likelihood, likelihood, high consequence, and there's a fair amount in the BTP and the SRM on common cause failure. It doesn't exactly estimate on likelihood of a common cause failure, but it says, if you have these design techniques, you're good enough.

(Simultaneous speaking.)

DR. BLEY: It pushes around the edges pretty well on that, I agree with you.

CHAIR ROBERTS: So it sounds like it needs more thought, I think, is probably a fair summary of it. Anybody else have a comment?

MEMBER BALLINGER: I do. This is Ron Ballinger. Do I assume that we will get -- that the draft guidance and the proposed rule will come as a package?

CHAIR ROBERTS: I could ask the staff, but that's my assumption.

MEMBER BALLINGER: It doesn't make any sense to go out, at least to me, with a rule for

public comment without the guidance that goes with it. So what is the schedule for that?

MR. PAIGE: This is Jason Paige, I&C. So the accompanying guidance, we do plan on issuing that for comment with the draft proposal, so they'll both be available. And our schedule for that is to issue those for public comment during the June time frame of summer 2025.

MEMBER BALLINGER: Thank you.

CHAIR ROBERTS: There will be draft guidance with the proposed rule? Because I wasn't aware of that, that the draft that we got just asks the public what they think the scope of the guidance would be, but you're actually going to provide your trial balloon of the guidance in that rulemaking?

MR. PAIGE: That's correct. That is correct.

DR. BLEY: Hey, Tom, this is Dennis. I guess it's a question for the staff. That's really the way it's supposed to work, right? That's the direction is they should come out together for all rules.

CHAIR ROBERTS: Now I'm thinking what is the plan to give this subcommittee a chance to review the draft guidance. Like I said, I was under the

impression until now that that wasn't going to be prepared until you got public feedback.

MR. PAIGE: So that package will be available to everyone to provide comments. I'll discuss internally with Christina in terms of coming in front of the committee again and discussing the draft guidance, if that's desired by the committee.

DR. BLEY: But is it not likely that public comments related to the draft guidance and the rule would kind of interact with one another?

CHAIR ROBERTS: It's kind of the analogy of the draft reg guide, and we'll have a chance to look at it before it goes out for public comment and a chance to look at it after it comes back. Most of the time, we opt to not look at it until after public comment. I guess when we get to the subcommittee deliberations later we can talk about whether or not we want to see this before it goes out or whether, as you point out, the public comments will likely change it significantly and whether we think we've seen enough today to just -- I guess that's something we'll talk about when we get to subcommittee deliberations later.

Thanks for the question. I didn't realize they were planning that in the next three months.

Any other comments or questions from members or consultants? Not hearing any, now is the time to go out for public comments. I guess we'll hear from the room first and then – okay. So nobody in the room wants to make a public comment. Anybody online who would like to make a comment for the record, go ahead and raise your hand or unmute yourself and then state your name and your affiliation, if appropriate, and state your comment. Having given that the requisite ten seconds, nobody made a public comment, so that will end the agenda up until the point of subcommittee deliberations on next actions.

So with that, the court reporter, we won't need your services anymore for the subcommittee meeting. So we'll end the transcribe part.

(Whereupon, the above-entitled matter went off the record at 2:54 p.m.)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2018

10 CFR 50.55a(h), IEEE Std 603

Advisory Committee on Reactor Safeguards

Digital I&C Subcommittee Meeting

February 19, 2025

1:00 PM

Outline

- Overview of Proposed Rulemaking Efforts
  - Background
  - Current Rulemaking Effort
- Comparison of Institute of Electrical and Electronics Engineers (IEEE) Std 603-1991 to IEEE Std 603-2018
  - Examples of requirements that are equivalent or enhanced
- Clause 5.16 “Common-cause failure” (CCF)
- Regulatory History of 10 CFR 50.55a(h)
  - Protection and Safety Systems
  - Referenced Standards
  - ACRS Recommendations from Previous IEEE Std 603-2009 Rulemaking Efforts
  - NRC Staff Non-Concurrences from Previous IEEE Std 603-2009 Rulemaking Efforts
- Summary – Incorporation by Reference (IBR) of IEEE Std 603-2018

Overview of Proposed Rulemaking Efforts

Background

- **10 CFR Part 50, Section 50.55a Clause (h) currently IEEE Std 603-1991 "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations".**
  - Current version is not up to date, multiple versions published since (1998, 2009, 2018).
- **In 2015, the staff attempted to Incorporate by Reference (IBR) IEEE Std 603-2009, but the Commission disapproved it, due to the imposition of additional conditions and requirements beyond those in the standard that were inconsistent for new and operating reactors.**
- **The Commission instead directed staff to develop a plan to modernize the NRC's digital I&C regulatory infrastructure, including how to address IEEE 603.**
  - Staff coordinated with IEEE standards committee to address issues related to 603.
  - To solicit early feedback, staff held a public meeting in September 2023 to discuss the proposed path forward for IEEE 603-2018, discussing various options. Initial feedback supported IBR as it provides regulatory certainty.

Current Rulemaking Effort

- In 2024, staff formed an inter-office working group to formally initiate activities to develop a path forward on industry's use of IEEE 603-2018.
- Staff evaluated options for the use of the latest IEEE standard in concert with stakeholder input, before deciding to proceed with the rulemaking option to IBR.
- Staff performed a comparative analysis between IEEE 603-1991 and IEEE 603-2018.
  - This proposed IBR does not raise significant policy issues, does not impose additional requirements on the standard.
  - The standard would be required for new applicants, and optional for current licensees.

Current Rulemaking Effort (Cont.)

- Staff plans to develop accompanying draft guidance with the proposed IBR of IEEE 603-2018.
- Staff is evaluating which document would be revised or developed to provide the accompanying draft guidance.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comparison of IEEE 603-1991 to IEEE 603-2018

Comparison of IEEE 603-1991 and IEEE 603-2018

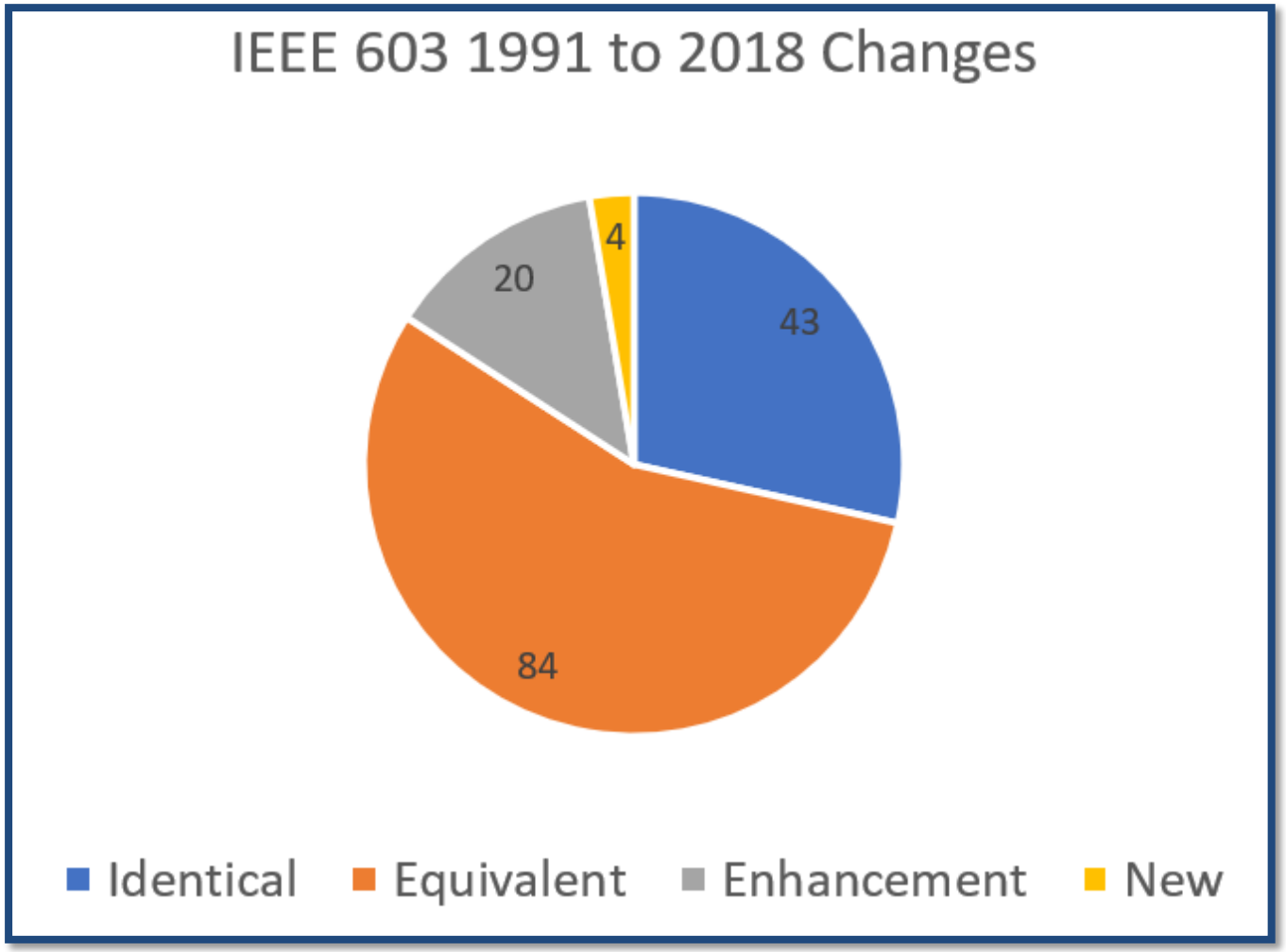
Clauses and subclauses were divided into items (151) to facilitate the comparison.

Identical – No changes in wording between the two standards;

Equivalent – Formatting changes, updated standard revisions, updated wording, restructured numbering or similar;

Enhancement – Improvements, clarifications, additional text modifying items on existing topics; and

New – Added items (clauses, subclauses, or text) addressing new topics.



U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Examples of requirements that are equivalent or enhanced

Example 1 (Equivalent Clause)

- **IEEE 603-1991, Clause 4.12**

Any other special design basis that may be imposed on the system design (example: diversity, interlocks, regulatory agency criteria).

- **IEEE 603-2018, Clause 4.12**

Any other special design basis that may be imposed on the system design (e.g., to address topics such as diversity or interlocks).

Example 2 (Enhancement Clause)

- **IEEE 603-1991, Clause 5.5**

The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis.

- **IEEE 603-2018, Clause 5.5**

The safety systems shall be designed to accomplish their safety functions under the full range of applicable conditions enumerated in the design basis. See items g) and h) of Clause 4.

Safety functions shall be designed to have deterministic (i.e., predictable and repeatable) behavior and timing.

Comparison Between IEEE 603-1991 and IEEE 603-2018 (Cont.)

- The staff completed a comparative analysis of IEEE 603-1991 and IEEE 603-2018.
- The staff concluded that the only new clause is 5.16 “Common-cause failure”.

Clause 5.16 “Common-cause failure”

Clause 5.16 Common Cause Failure (cont.)

- The first sentence of Clause 5.16 states "**The safety system design and development shall address common-cause failures (CCF) that create a potential to degrade or defeat the safety system function**."
- The remaining statements within Clause 5.16 describe guidance regarding how CCF should be addressed.
  - The NRC is not taking a position on the suitability of the methods for addressing CCF described in Clause 5.16, which may be appropriate for use by applicants and would be reviewed by the NRC on a case-by-case basis.
  - While these methods may be acceptable to address CCF in appropriate circumstances, **this list is not comprehensive and does not include flexibilities the Commission directed to staff, in SRM-SECY-22-0076.**

Clause 5.16 Common Cause Failure

- Staff is proposing to update § 50.55a to IBR IEEE Std 603-2018 but not require conformance to IEEE Std 603-2018 Clause 5.16, "Common Cause Failure," except that **the safety system design and development shall address CCF that create a potential to degrade or defeat the safety system function**, as described in the first sentence of this clause.

Regulatory History of 10 CFR 50.55a(h)

Protection and Safety Systems

- 10 CFR 50.55a(h) uses the terms “protection systems” and “safety systems”.
- IEEE Std 279 uses the term “protection systems” to define its scope.
- IEEE Std 603 uses the term “safety systems” to define its scope.

Protection and Safety Systems (Cont.)

- “The NRC recognizes that ‘‘protection systems’’ are a subset of ‘‘safety systems.” Safety system is a broad-based and all-encompassing term, embracing the protection system in addition to other electrical systems. Thus, the term ‘‘protection system’’ is not synonymous with the term ‘‘safety system.’’ The final rule is not intended to change the scope of the systems covered in the final safety analysis report (FSAR) for currently operating nuclear power plants.”(64 FR 17944; April 13, 1999)
- The proposed IEEE Std 603-2018 rule would not change the scope of the systems covered in the final safety analysis report for currently operating nuclear power plants.

Source: Final Rule—Codes and Standards: IEEE National Consensus Standard, dated April 13, 1999, 64 FR 17944

Referenced Standards

- IEEE Std 603-2018 references several industry codes and standards.
- These referenced standards are not proposed for incorporation by reference in this rulemaking.
  - Not mandatory NRC requirements.
  - If a referenced standard has been endorsed in a regulatory guide, the standard constitutes a method acceptable to the NRC for meeting a regulatory requirement.
- This approach is consistent with the Commission statement in the IEEE Std 603-1991 final rulemaking.

Source: Final Rule—Codes and Standards: IEEE National Consensus Standard, dated April 13, 1999, 64 FR 17944

ACRS Recommendations from Previous IEEE Std 603-2009 Rulemaking Efforts

Source: ACRS Letter dated August 5, 2014, https://www.nrc.gov/docs/ML1419/ML14196A137.pdf

ACRS Recommendations (2014)

- ACRS Recommendation: Add requirement in 10 CFR 50.55a(h)(5)i for an independent hardware-based, diverse means that monitors and produces a diverse trip in the affected redundant portion of the digital safety systems if the common processing unit ceases operation or “locks-up”.

- Staff Resolution (2025): Evaluate the potential inclusion of this recommendation in draft guidance as an example of diversity that would provide adequate protection.

Sources: ACRS Letter dated August 5, 2014, https://www.nrc.gov/docs/ML1419/ML14196A137.pdf
NRC Staff letter dated October 16, 2014, https://www.nrc.gov/docs/ML1426/ML14260A342.pdf

ACRS Recommendations (2014; Cont.)

- ACRS Recommendation: Clarify 10 CFR 50.55a(h)(4) to state that “both predictable and repeatable” means processing from sensor data input to safety control device actuation and independent of any redundant portions of the safety system or other external input.

- Staff Resolution (2025): IEEE 603-2018 includes the following requirement: "Safety functions shall be designed to have deterministic (i.e., predictable and repeatable) behavior and timing“.

Sources: ACRS Letter dated August 5, 2014, https://www.nrc.gov/docs/ML1419/ML14196A137.pdf
NRC Staff letter dated October 16, 2014, https://www.nrc.gov/docs/ML1426/ML14260A342.pdf

ACRS Recommendations (2014; Cont.)

- ACRS Recommendation: Add an additional condition regarding "Control of Access" that identifies communications external to the plant should be accomplished using one-way, hardware-based (transmit only) devices.

- Staff Resolution (2025): Recommendation addressed in regulatory (RG 1.152) and staff guidance (BTP 7-19):
  - Use of a hardware-based unidirectional device is one approach the NRC staff would consider acceptable to ensure that safety-related I&C systems do not present an electronic path that could enable unauthorized access to the plant's safety-related systems.

Sources: ACRS Letter dated August 5, 2014, https://www.nrc.gov/docs/ML1419/ML14196A137.pdf
NRC Staff letter dated October 16, 2014, https://www.nrc.gov/docs/ML1426/ML14260A342.pdf
NRC Staff letter dated, July 14, 2021, https://www.nrc.gov/docs/ML2118/ML21187A291.pdf

NRC Staff Non-Concurrences from Previous IEEE Std 603-2009 Rulemaking Efforts

Source: SECY-15-0106: Rulemaking: Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", dated September 10, 2015, https://www.nrc.gov/docs/ML1131/ML113190983.html

NRC Staff Non-Concurrence (2015)

- Staff Position: Concerns about the impact of having different data communication requirements for new reactors and operating reactors.

- Staff Resolution (2025):
  - Data communications implementation is addressed in IEEE 7-4.3.2-2016 (as endorsed by RG 1.152, Rev. 4).
  - A technology-inclusive rule is being pursued via IBR of IEEE 603-2018.

Source: SECY-15-0106: Rulemaking: Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", dated September 10, 2015, https://www.nrc.gov/docs/ML1131/ML113190983.html

NRC Staff Non-Concurrence (2015; Cont.)

- Staff Position: Concerns about the lack of requirements for an independent/diverse architecture for highly safety-significant digital systems in support of the implementation of a defense-in-depth approach.

- Staff Resolution (2025):
  - IEEE 603-2018 does not include diversity requirements.
  - Current policy (e.g., SRM-SECY-22-0076) for Digital I&C CCFs allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth.

Source: SECY-15-0106: Rulemaking: Proposed Rule: Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009, "IEEE Standard Criteria for Safety Systems for Nuclear Power Generating Stations", dated September 10, 2015, https://www.nrc.gov/docs/ML1131/ML113190983.html

Summary – IBR of IEEE Std 603-2018

- Incorporate the entirety of IEEE Std 603-2018 into 50.55a(h), with only the first sentence of Clause 5.16.
  - Aligned with existing CCF policies.
  - Applicable to new applicants, optional for current licensees.
  - Regulatory treatment of referenced standards (i.e. secondary references) would remain unchanged - treated as guidance.
  - "The final rule is not intended to change the scope of the systems covered in the final safety analysis report (FSAR) for currently operating nuclear power plants."
- Accompanying Draft Guidance for IEEE 603-2018.

Source: Final Rule—Codes and Standards: IEEE National Consensus Standard, dated April 13, 1999, 64 FR 17944

Acronyms

- ACRS – Advisory Committee Reactor Safeguards
- BTP – Branch Technical Position
- CCF – Common-cause Failure
- DG – Draft Guidance
- FR – Federal Register
- FSAR – Final Safety Analysis Report
- I&C – Instrumentation and Controls
- IBR – Incorporation by Reference
- IEEE – Institute of Electrical and Electronics Engineer
- NRC - Nuclear Regulatory Commission
- RG – Regulatory Guidance