Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards
Digital Instrumentation and Control Systems

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Tuesday, May 20, 2014

Work Order No.: NRC-800 Pages 1-323

NEAL R. GROSS AND CO., INC.
Court Reporters and Transcribers
1323 Rhode Island Avenue, N.W.
Washington, D.C. 20005
(202) 234-4433

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

SUBCOMMITTEE

+ + + + +

TUESDAY

MAY 20, 2014

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., Charles H. Brown, Jr., Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR., Chairman

DENNIS C. BLEY, Member-at-Large

JOHN W. STETKAR, Member

STEPHEN P. SCHULTZ, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

NRC STAFF:

STEVEN ARNDT, NRR

JOE ASHCRAFT, NRO

ROYCE BEACOM, NRR

SUSHIL BIRLA, RES

DANIEL DOYLE, NRR

CLIFF DOVIT, NRR

MAURICIO GUTIERREZ, RES

PAT HILAND, NRR

TERRY INVERSO, NRR

TERRY JACKSON, NRO

HYUNG JE, NRO

IAN JUNG, NRO

DAWNMATHEWS KALATHIVEETTIL, NRO

WENDEL MORTON, NRO

TIM MOSSMAN, NRO

WILLIAM ROGGENBRODT, OCHCO

DANIEL SANTOS, NRO

RICHARD STATTEL, NRR

JOHN THORP, NRR

DINESH TUNEJA, RES

MICHAEL WATERMAN, RES

DEANNA ZHANG, NRO

JACK ZHAO, NRO

ALSO PRESENT:

TRICIA BOLIAN, AREVA*

GORDON CLEFTON, NEI

DAVID HERRELL, MPR Associates

STEVEN HUTCHIN, NEI

YON HO KIM, KHN

TROY MARTEL, Safe Operating Systems*

WARREN ODESS-GILLETT, Westinghouse

KEN SCOROLA, Nuclear Automation Engineering*

BOB SEELMAN, Westinghouse

RYAN SPRENGEL, Mitsubishi Nuclear Energy Systems*

RUTH THOMPSON, Environmental Inc.*

ROGER WYATT, AREVA*

*Present via telephone

A G E N D A

P R O C E E D I N G S

8:34 a.m.

CHAIRMAN BROWN: This meeting will come to order. This is a meeting of the Digital Instrumentation and Control System Subcommittee. I am Charles Brown, Chairman of the Subcommittee.

ACRS members in attendance are Stephen Schultz, Dennis Bley, John Stetkar, myself, our consultant, Myron Hecht, and Christina Antonescu of the ACRS Staff as our Designated Federal Official for this meeting.

The purpose of this meeting is for the Staff to brief the ACRS on 10 CFR 50.55a Rule to incorporate by reference the IEEE Standard 603-2009 Standard Criteria for Safety Systems for Nuclear Power Generating Stations.

Specifically during the meeting, the Subcommittee will consider the Staff's reasons for this rulemaking activity, changes made to IEEE 603, differences between the 1991 version and the 2009 version, changes to regulations being made to incorporate the new version by reference, and to 10 CFR 50.55a, discuss in particular new conditions being added to the proposed rule to address independence criteria, and an overview of Draft Guide 12525 which

has been issued or being prepared or proposed to update Reg Guide 1.153.

The Subcommittee will gather information, analyze relevant issues and facts, formulate proposed positions and actions, as appropriate, for deliberation by the full Committee.

Rules for participation in today's meeting have been announced as part of the notice for this meeting which was published in the Federal Register on April 29th, 2014.

We have received no written comments or requests for time to make oral statements from members of the public regarding today's meeting. Also, we have some people on the bridge line listening to the discussions. Those that we know about are Troy Martel from Safe Operating Systems, Ruth Thompson from Environmental Incorporated, Ken Scarola, Nuclear Automation Engineering, Patricia Bolian and Roger Wyatt from Areva.

To avoid interruption of the meeting the phone line will be placed on a listen-in mode only during the discussions, presentations, and Committee discussions. The bridge line will be opened at the end of the meeting to see if anyone listening would like to make any comments. At that time, those who want to

make comments should identify themselves by name.

A transcript of the meeting is being kept and will be made available as stated in the Federal Register notice. Therefore, we request that participants in this meeting use the microphones located throughout the meeting room when addressing the Subcommittee. The participants should first identify themselves and speak with sufficient clarity and volume so that they may be readily heard.

We will now proceed with the meeting, and I will call upon Mr. John Thorp, the I&C Branch Chief, Division of Engineering and Nuclear Reactor Regulation Office to make an opening statement.

MR. THORP: Thank you.

CHAIRMAN BROWN: I didn't say anything about Mr. Hiland. I presume you all will coordinate whatever you all want to B-

MR. THORP: Thank you, Member Brown. We do have my Division Director, Pat Hiland, here today, as well as our senior-level advisor. In fact, senior-level advisors I think from a couple of the offices, all the offices from Research; Steven Arndt from NRR, Dan Santos from Office of New Reactors, and Sushil Birla from the Office of Nuclear Regulatory Research. Appreciate their presence here, as well as all other

members of Staff and Management that are here this morning.

Members of the Subcommittee, my name is John Thorp. I'm the Chief of the Instrumentation & Controls Branch in the Division of Engineering, in the Office of Nuclear Reactor Regulation.

The Staff was requested to provide an informational briefing to you all on several topics related to 50.55a, and information contained in the preliminary draft proposed rule text and its associated Statements of Consideration.

We have several presenters this morning who essentially are also representatives of the Working Group. This is not the complete Working Group, but these are the members who will be presenting today. We have Michael Waterman from Research who will speak to the work on the Draft Regulatory Guide and the changes to 1.153. We have Ms. Deanna Zhang from Office of New Reactors who will speak to the independence criteria. We have Rich Stattel who will speak to the overall preliminary draft proposed rule text, and then at the end, providing there's time, I would hope that there would be some time, we'll have one of my staff, as well, who's a former member of the Office of New Reactors, Mr. Royce Beacom, who is the Chair of the IEEE 603 Impact

Working Group, and is associated with that Nuclear Power Engineering Committee working with this particular standard. He'll talk about the path forward for the next revision to the actual standard.

So, all these folks will present the results of what I think all of us acknowledge is an extensive effort by the Working Group over the last four years to develop new regulations, new draft regulations for safety-related instrumentation and control systems.

The preliminary draft proposed rule text is, of course, currently in draft form, and it's undergoing concurrence reviews by the various offices. So, the information you'll hear today is, in essence, the content of the preliminary draft proposed rule text and Statements of Considerations.

We're prepared to present the contents of the proposed draft rule text, and to discuss the rationale used by the Working Group in its development. The proposed rule text includes a discussion section, which includes many Statements of Consideration. And a lot of the speaker notes and the words that you will hear will be coming directly from those Statements of Consideration, so we're trying to stay very consistent with our effort to present to you what is actually in

this preliminary draft proposed rule text.

These statements provide an explanation of matters considered during the development of the proposed rule text, and they also provide clarification of what is intended for each clause of the proposed rule, so those statements I'm referring to are the Statements of Consideration.

Now, once the concurrence process is completed, the proposed rule will be made public and will undergo a public comment period, after which the Working Group will reconvene to address any comments received. So, without further ado, I'll turn the mic over to Rich Stattel.

MR. STATTEL: Thank you, John. I will begin B- this slide here is the agenda for today's presentation.

This proposed rule would incorporate a Voluntary Consensus Standard, IEEE 603, 2009 version into the NRC regulations to establish functional and design requirements for power, instrumentation, and control systems for nuclear power plants.

This action is consistent with the provisions of National Technology Transfer and Advancement Act of 1995, which encourages federal regulatory agencies to consider adopting voluntary

consensus standards as an alternative to de novo agency development of standards.

This action would also be consistent with the NRC policy of evaluating the latest version of consensus standards in terms of their suitability for endorsement by regulations or Regulatory Guides.

Okay. I'm going to start out by talking about the reasons for changing this rule. Okay. One of the main driving forces for this rulemaking activity is the fact that the current incorporate by reference standard has become outdated. The state of I&C system technology has changed a great deal since that standard was issued back in 1991.

There are several design concepts that are being incorporated into digital I&C systems today that were not being considered in 1991. The industry has matured and has gained a great deal of experience with the use of digital I&C systems, particularly in the balance of plant applications non-safety related systems such as digital feedwater controls.

The NRC has raised concerns in this interim time period over the different failure modes that digital systems can introduce, particularly for highly integrated systems.

The NRC has raised concerns, also, for the

potential of software common cause failures or errors that can occur with systems using multiple instances of software or logic implementation.

In actuality, very few I&C systems being proposed to the NRC today were developed to the 1991 standard to which we are evaluating them, and we're trying to correct that situation. Additionally, the Working Group identified a need for clarification of applicability requirements based on the experience we have had recently with the existing regulation.

As I stated, the primary objective is to update the incorporate by reference standard to the more recent IEEE 603 2009 version of the standard. This standard establishes the minimum functional and design requirements for power instrumentation and control systems for nuclear power plants. There was an intermediate version of this standard that was published in 1998; however, the NRC chose not to incorporate that version at that time because the changes to the standard were not considered substantial at the time of issuance, and the safety benefits of the new standard were not considered significant enough to warrant the resources that would have been required to incorporate that standard into regulation.

Additionally, the proposed rule defines

conditions which would allow existing licensees to replace plant equipment while maintaining their existing licensing basis. It also defines the conditions for which existing permit license certificate standard design and standard design approvals would be required to address the new standard.

And, finally, the rule imposes conditions upon the use of IEEE 603 2009 in the areas of system integrity, diversity, defense-in-depth or D3, independence, maintenance bypass, and maintenance of records.

So, we start out with discussing what exactly changed in the standard, so this is a list, this is basically a summarized list of what has changed in the standards between 1991 and 2009. I'll just point out that some of these changes were made in the 1998 version, and then they carried through to the 2009 version, and some of the changes were just introduced in 2009.

The Working Group evaluated and compared the new 2009 version of the standard with both the 1991 and 1998 versions. And, again, this is the list that summarizes those changes that we identified. I'll now explain each of those changes in detail.

Okay. The first change was included to address the introduction of digital computers or digital components such as field programmable gate arrays, FPGAs or computer programmable logic controller, PLC technologies into instrumentation and control systems in nuclear power plants.

Back when computers were first being introduced to the industry, the IEEE decided to develop a separate IEEE 7-4.3.2. Standard as a companion standard to IEEE 603 to provide guidance for digital computer-based systems. This was done instead of including the technology-specific guidance within IEEE 603 itself.

In 1991, IEEE's 7-4.3.2, the version at the time was 1982 version, was generally referenced within IEEE 603; however, no specific topical references were included in IEEE 603. So, in the 1998 version of IEEE 603, specific sectional references were added to the standard. And on this slide it points to the specific references that were added in.

MEMBER BLEY: Now, with the new revisions to 603 does the other one you had up here, that's still a cross-reference. That one still exists? They didn't incorporate that?

CHAIRMAN BROWN: You mean 7-4.3.2?

MEMBER BLEY: Thank you, Charlie. Yes.

MR. STATTEL: Okay, a little explanation. When I say it's a companion standard, so IEEE did kind of a unique thing. They matched the sections to the section numbers of IEEE 603, so in sections where there was no additional guidance required, basically, the section still exists. It just says no guidance in addition to what's in 603 is necessary. So, in areas where there was guidance required and it needed to be elaborated on, the IEEE basically added that guidance in there. So, we take into account both.

Now, the difference being IEEE 603 is actually B- we consider the criteria within that to be regulation because of this incorporate by reference. IEEE 7-4.3.2 was never incorporated by reference. Now, however, it is endorsed by the NRC, a version of it is endorsed by the NRC under a separate Regulatory Guide, which is 1.152, which is really not within the scope of what we're talking about today, but we do endorse the version of that standard. But it's considered guidance, not regulation.

MS. ZHANG: And the 2009 version of IEEE 603 points to the 2003 version of IEEE Standard 7-4.3.2.

MEMBER BLEY: So, they continue to exist.

MS. ZHANG: Yes.

MR. STATTEL: Yes, it's a little confusing when you get into the versions because it's IEEE standard practice to update the references to the current versions of their standards. This is understandable; however, when we -- the timing is such that when we endorse a particular standard the version that's being referenced by the new IEEE standard may not be the version that's actually endorsed by the NRC.

CHAIRMAN BROWN: When we did 1.152 and that does endorse, like you said, 7-4.3.2, was that -- my memory fails me. Wasn't that 2003 version when we just did the most recent revisions?

MR. STATTEL: Yes, it is.

CHAIRMAN BROWN: Okay.

MR. STATTEL: So they are actually in --

(Simultaneous speech.)

MR. STATTEL: That's not an exception, but they are in sync right now.

MS. ZHANG: But we are working on --

MR. STATTEL: Or they will be.

MS. ZHANG: Yes, we are working on endorsing the 2010 version of the standard because that's been out for four years right now.

CHAIRMAN BROWN: Have they made any substantive changes?

MS. ZHANG: Yes. They incorporated a lot of the guidance from the NRC ISGs, ISG-1, or ISG-2 and ISG-4.

CHAIRMAN BROWN: Yes. When I looked at 7-4.3.2, blah, blah, blah, whatever --

(Simultaneous speech.)

CHAIRMAN BROWN: -- questioned some of the value. I mean, yes, they pointed out some stuff but they really didn't attack the new technology anywhere as close as you all did in this incorporation by reference of 2009 in the rule. I mean, you all really went after looking at where we had -- that's my impression from reading the rule and the Reg Guide, accompanying Reg Guide that you all got drafted, as well, that you really looked at the lessons learned out of the last few design cycles we've had and tried to bring those lessons into this being talked about and held up by the rule. So, 7-4.3.2 was far more generic the way I looked at it.

MR. STATTEL: And a lot of the efforts are going on in parallel. The Reg Guide 1.152, the effort to update that has actually been put on hold weighing the outcome of this rule, what we're talking about today. So, unfortunately, a lot of the new things --because I am on the Working Group for IEEE 7-4.3.2,

as well, so a lot of the things the Working Group has done and has published in 2010, and we're actually currently working on a new version that we intended being published next year. A lot of those things really aren't visible in the regulatory structure right now.

CHAIRMAN BROWN: Okay.

MR. STATTEL: But the goal is --

CHAIRMAN BROWN: I didn't look at 2010, I looked at the 2003 version.

MR. STATTEL: Right. That's understandable.

CHAIRMAN BROWN: Far more prescriptive.

MR. STATTEL: It is actually a very substantive change we made from 2010.

CHAIRMAN BROWN: Yes.

MR. STATTEL: That's correct, yes. Now, I don't want to imply that there's gaps, because a lot of what we incorporated in the 2010 version of IEEE 7-4.3.2 is covered under the interim Staff Guidance that we have in place. So, when we perform our safety evaluations we consider all of those aspects.

CHAIRMAN BROWN: Okay, thank you.

MR. STATTEL: Okay? Now, a little word on the reference standards from within the IEEE 603. Since reference standards are not considered by the NRC to

be incorporated by reference into regulation, these changes were not really considered by the Staff to be technically relevant to the IBR rulemaking process and incorporate by reference the rulemaking process.

Instead, as we mentioned, the NRC endorses many of these other standards through its Regulatory Guidance process. The difference between the incorporate by reference and an endorsement of a standard is that the criteria of an IBR standard are essentially elevated to the level of regulation, and while the criteria of an endorsed standard are considered to be a guidance and accepted ways to meet the underlying regulatory criteria; just to make that clarification. So that's number two here. Right? So, IEEE, like I said, they updated all of their referenced standard from within IEEE 603, and there are several.

Okay. The next change that was made to the IEEE 603 standard, during the 1998 revision of the standard a new Informative Annex that's titled "Electromagnetic Capability," or "Compatibility," sorry, was added. The NRC does not endorse this Informative Annex. Instead, Electromagnetic Compatibility or EMC has been addressed by a separate Reg Guide, Regulatory Guide. The Reg Guide that does address this is Reg Guide 1.180. It's titled,

"Guidelines for Evaluating Electromagnetic and Radio Frequency Interference in Safety-Related I&C systems." And that endorses a military standard, Standard 461a, and IEC Standard 61000. So, basically, that Informative Annex, that change we didn't consider really relevant to the rulemaking process.

CHAIRMAN BROWN: And did you all make a comment on that relative in the rule or did you not? I remember seeing references to that, you all not endorsing the annex, but I've lost it as opposed to the B-

MR. STATTEL: I believe there is a discussion.

CHAIRMAN BROWN: In the Reg Guide?

MR. STATTEL: There is a discussion in the Statements of Consideration within the proposed rule document, the text.

CHAIRMAN BROWN: Okay. No, just one thing for my own information. When I read through the entire Statements of Consideration it looks like those were reflected on those very heavily in the Reg Guide. Is that B- proposed Reg Guide?

MS. ZHANG: Yes.

CHAIRMAN BROWN: So, that information is being carried out so it will be available B-

MS. ZHANG: Yes.

CHAIRMAN BROWN: B- so people will understand what you're talking about.

MR. STATTEL: That's correct. That was the intent.

CHAIRMAN BROWN: Okay.

MS. ZHANG: And Mike will explain in detail how that was done.

CHAIRMAN BROWN: Okay. Yes, I know that's coming up later. Thank you. All right. Appreciate that.

MR. WATERMAN: Just one other comment. The annexes in IEEE Standard 603 1991 are Informative Annexes and, therefore, not considered by the IEEE to be binding upon the standards.

CHAIRMAN BROWN: Okay, thank you.

MR. STATTEL: Okay, on to the fourth change. In 1998 a new section was added to the standard, 5.16, and this was done in an attempt to address criteria for software common cause failure.

In actuality, when we reviewed this clause we determined that the added clause does not introduce any criteria at all. Instead, it simply refers to IEEE 7-4.3.2.

CHAIRMAN BROWN: I lost the bubble. Would you go back and start that over again? I was looking

for one of my notes.

MR. STATTEL: They added a section. Now, Section 5 has several subsections within it.

CHAIRMAN BROWN: Okay.

MR. STATTEL: They added a new one. If you look at the 1991 version there is no 5.16.

CHAIRMAN BROWN: Right.

MR. STATTEL: So, they added a version. It's titled "Common Cause Failure Criteria." Right? So, we're like okay, what's the criteria? Well, when we look in there it really doesn't provide any criteria. It simply refers to IEEE 7-4.3.2, so there's really nothing for us to really evaluate.

So, basically, our position is though we do endorse IEEE 7-4.3.2 via Reg Guide 1.152, the NRC does not consider the guidance criteria within 7-4.3.2 to be complete or adequate for addressing software common cause failure criteria. Instead, the NRC refers back to Staff Requirements Memorandum, the SECY 93-087 paper via our standard review guidance and Branch Technical Position 719 when we perform those evaluations for susceptibility to common cause failure.

So, basically, we endorse the 7-4.3.2 guidance; however, in the area of software common cause

failure or addressing common cause failure criteria we have other methods that we use for our safety evaluations.

MEMBER STETKAR: Rich?

MR. STATTEL: Yes?

MEMBER STETKAR: Why do we only care about software common cause failure?

MR. STATTEL: Well, I don't think that's a true statement.

MEMBER STETKAR: I can't find anything that tells me I need to worry about hardware common cause failure, so I'm led to believe that we care only about software common cause failure.

MR. WATERMAN: Rich, I can take that.

MEMBER STETKAR: I need something to tell me where we tell people to do an analysis of hardware common cause failure. I'd like to see where that is.

MR. WATERMAN: John, the hardware common cause failure is actually addressed over in the single failure clause of IEEE Standard 603.

MEMBER STETKAR: I'm sorry. A common cause failure will negate any single failure.

MR. WATERMAN: No, no, no, no. But in IEEE Standard 603 in the section on single failure criteria, it attempted to address hardware common cause failure

by providing a lot of exclusions for why common cause failure of hardware need not be considered, such as manufacturing process, and there's a B-

(Simultaneous speech.)

MR. WATERMAN: B- maintenance and things like that.

MEMBER STETKAR: See maintenance.

MR. WATERMAN: Keep going. Well, I don't have the standard in front of me but B-

MEMBER STETKAR: I have it.

MR. WATERMAN: Oh, good. As a matter of fact, all of those exclusions for why common cause failures need not be considered sort of were the basis for adding in Clause 516 on common cause failure because we wanted the point that software didn't seem to rise to that level where you could say well, they had a high quality manufacturing process. Well, you still get common cause failures of software.

MEMBER STETKAR: Let me approach it from a different question. Have we seen hardware common cause failures? Have they occurred? That's a question.

MR. STATTEL: In digital I&C B

MEMBER STETKAR: The answer B- no. I didn't say digital I&C devices. I said have we seen hardware common cause failures?

MR. WATERMAN: Yes, we have.

MR. STATTEL: Yes, we have.

MEMBER STETKAR: Have we seen hardware common cause failures in instrumentation and control systems?

MR. STATTEL: Yes, we have.

MEMBER STETKAR: And safety systems? Yes, we have. Why are we not interested in evaluation of hardware common cause failures going forward?

MR. STATTEL: Okay. I think we'll have a greater discussion on the NRC's position. Right now what I'm explaining is what changed in the IEEE standard. This clause, 5.16, only addresses software common cause failure.

MEMBER STETKAR: That's correct.

MR. STATTEL: That was its only intent, so all I'm explaining to you now is what changed in IEEE 603 with the addition of this clause.

MEMBER STETKAR: Right. And it's titled generically "Common Cause Failure Criteria," so I got really interested in it because it was going to tell me how I think about common cause failures in these systems. And, you're right, all it does B-

MR. WATERMAN: It fails B-

MEMBER STETKAR: B- it fails miserably.

MR. WATERMAN: Yes.

MEMBER STETKAR: Completely.

MR. STATTEL: Yes. I agree with you. We do endorse a separate IEEE standard for common cause failure. It's 3.7.9. Is that correct, Mike?

MR. WATERMAN: Yes, IEEE 3.7.9 is B-

MR. STATTEL: Yes. Which is also referenced from within IEEE 603. I believe B- I'm not going to try to guess at the reference.

MEMBER STETKAR: No, that's okay. We can dig it up. Thanks.

MR. STATTEL: To answer your question, though; yes, the NRC cares about a lot more than just software common cause failure, and we evaluate systems for common cause failure generally.

MEMBER STETKAR: How is that B- the reason I'm digging on this is that people are spending a lot of effort, and I'm not saying they shouldn't spend a lot of effort to examine software common cause failure, and to provide diverse means of actuating safety functions in the eventuality of software common cause failures and so forth. There's a lot of effort being placed on that particular topic. I don't see that effort being placed on hardware common cause failures, which we've accepted their existence for the life of the

industry and we seem to mainly observe them, for example, reactor trip breakers. We put in, you know, focused specific fixes to supposedly address that particular issue.

Going forward does it seem reasonable to focus that amount of energy specifically on the area of software? And, again, I'm not saying that some energy shouldn't be focused on software, but not with an integrated perspective of hardware common cause. In other words, the software, we still have reactor trip breakers. They can fail mechanically. Perhaps someone believes that the mechanical failure of a reactor trip breaker is not credible. I'll get to the term of "credible," or that it's adequately reliable. I'll get to reliable later. Maybe software common cause failures is so unlikely we ought not to worry about them because we're dominated by hardware common cause failures that we don't address.

MR. STATTEL: That's a very good comment. I agree.

MEMBER STETKAR: So, you know, if we're rewriting regulations going forward or guidance, in particular, ought we not to think about that?

MS. ZHANG: I think we agree. It's something that we had discussed a lot in the Working Group in terms

of the types of common cause failures that should be addressed. I think we limited the scope of this incorporation by reference rule so that we can explore other items, you know, topics in a more holistic manner later on. I think there are other efforts that we are undertaking to address all these other issues, and part of it is common cause failure, what types of common cause failure? How do you address common cause failure?

MEMBER STETKAR: Terry Jackson has a couple of comments.

MR. JACKSON: Just a comment about the common cause failure. I'm not sure this microphone is working or not.

MEMBER STETKAR: Put it up a little higher.

MR. JACKSON: All right. So, basically, when the Staff discussed the issue about common cause failures, both hardware and software, and to really address B- I think the I&C area is really taking the same approach that the Agency takes in other areas, whether it be mechanical or structural area. And from a deterministic standpoint, there's not a specific analysis for common cause failures. Although we may treat it in certain areas like with ATWS Rule, or maybe insertion systems like auxiliary feedwater pumps and stuff that may have required diversity in the past. But,

overall, the Agency uses programmatic means to address common cause failure from the hardware stance. So, for example, it will be through the Corrective Action Program, Part 21 Rule, or the operating experience B-

MEMBER STETKAR: So, when common cause failures happen we try to fix them up.

MR. JACKSON: Well, I'm saying that the Agency's approach is to address them through programmatic means, so there are certain programs. And like Mike had mentioned, there's the Quality Assurance Program and things like that that are there to help address them, not that they, necessarily, could not happen. And we have seen them happen, as the folks up in front have mentioned. We have seen them happen in I&C systems, but those same programs also help to address those common cause failures.

MEMBER STETKAR: This standard applies, by the way, to analog, digital?

MR. STATTEL: It does, yes.

MEMBER STETKAR: Electro mechanical, knife switches.

MR. STATTEL: Absolutely, yes.

MEMBER STETKAR: You name the way of getting things to work.

MR. STATTEL: Yes, we pick up this standard

for evaluations no matter what technology they use.

MEMBER STETKAR: So, this standard applies to any traditional electro mechanical relay-driven logic also.

MR. STATTEL: I will say I've been in the industry for quite a while, and in the early days I think it was a lot more prevalent, the common cause failure on the hardware systems, or on the analog systems. For example, at the combustion engineering plants there was a common cause failure mode that had to do with the relays that were used for the actuation logic, and it turned out to be B- well, really the solution was they changed the model of the relays and they replaced the relays, so it was addressed.

They're a lot less frequent nowadays. When a common cause failure occurs, we review those events and it's the first thing we pick up on, is did this affect more than one channel? Why did this cause a plant trip? Why, you know -- what is the commonality of this? And we'll initiate generic communications, as necessary.

MEMBER STETKAR: Rich, but that's my point. It's a reactive approach B-

MR. STATTEL: That's true.

MEMBER STETKAR: B- to common cause

failures. When they occur, you will examine them and try to fix that particular problem. In the area of software common cause failures the guidance and the regulations now address, that's a B- I hate the word "proactive," but it's a forward-looking B- says you have to do an analysis. You have to examine the likelihood of having common cause failures, and install in your design defensive mechanisms against those common cause failures.

CHAIRMAN BROWN: Software.

MEMBER STETKAR: Software.

MR. STATTEL: What I will say even in the area of hardware B-

MEMBER STETKAR: But that's a different approach. It isn't sitting back and waiting until the software common cause failure happens and say oh, my God, you know, let's trace this back and find out where it happened B-

MR. STATTEL: It's more like a matter of dealing what you're aware of. Now, it's not entirely true that hardware common cause failures and completely reactionary. For example, environmental qualification, this is recognized widely as being a source of a common cause failure, whether it's digital technology, or analog technology, or whatnot. So,

therefore, we do require analysis for all environmental conditions that are relevant for these systems. So, I don't think it's fair to say that we really treat them that much differently.

Software is a little bit unique in that there is a potential there that there is a common cause or a common error that's duplicated among divisions or redundancies without an awareness of that. And that's a potential that is a little bit more self-evident in the analog technologies.

MEMBER STETKAR: Okay.

MR. STATTEL: All right. Now, I do have a place keeper here. We will be discussing a little bit more on the topic of D3 and software common cause failure later on when we talk about the conditions that are being imposed on the use of the new standard.

Okay. The fifth change, this section of the standard B-

CHAIRMAN BROWN: Rich, excuse me.

MR. STATTEL: Sorry?

CHAIRMAN BROWN: Before you go on, back to John's B- I was looking at your rule changes just to refresh my memory a little bit on it. You do have a reference, a specific modification I should say, and that's to 6H, page whatever it is. It's the fifth B-

MR. STATTEL: What page are you on?

CHAIRMAN BROWN: I'm on page 140 of the overall document, but it's the B- Item 6 addresses under H, 55A-H, and then you've got your modifications 1, 2, 3, 4, 5, and then 6. And I guess when I first read that, just thinking along John's lines, I didn't really focus on the second sentence under that where it said, "The following requirement must be met when addressing digital system common cause failures." I mean, I kind of read that more generically, that it would apply at any time. It didn't really dawn on me until you made your comment, because this is a document that applies to all technologies, whether your relays, or meg amps, or whatever, vacuum tubes if you really wanted to go back that far. So, it just seems to me there's an opportunity here to make B- you made that point in your Reg Guide about other technologies. And I notice the DSRS for mPower also made these points that similar things apply to other technologies. This is just not for, you know, computer-based or microprocessor-based type digital technologies. So, that was just a thought to B- and I'm not saying, you know, throw in all these. It doesn't talk about B- it just says you've got to evaluate the potential for these things, that's all.

MR. STATTEL: Well, it's really viewed by

the industry as an above and beyond requirement to perform a D3 analysis that's focused on the potential for software or digital system-related common cause failures. We don't require that in the area of hardware.

CHAIRMAN BROWN: Yes, but you are for the digital B- I mean, the rule B-

MR. STATTEL: Right.

(Simultaneous speech.)

CHAIRMAN BROWN: B- digital type systems, whether they're FBGAs.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: Whether microprocessors, or whatever, you're going to be requiring it.

MR. STATTEL: Right. And that's the direction that the Staff received from the Commission for the SECY paper.

CHAIRMAN BROWN: Okay.

MR. STATTEL: Is to consider the potential for common cause failure of digital systems, software common cause failures.

CHAIRMAN BROWN: I don't B- I understand.

(Simultaneous speech.)

MR. STATTEL: B- of responding to that. We did not receive direction from the Commission to require an additional analysis to address the concerns

of hardware common cause failure beyond what we're already doing in regulations.

MR. THORP: That are non-digital items.

MR. STATTEL: Right.

MR. THORP: It shines a specific spotlight to add on that expectation.

MR. STATTEL: So, kind of the B- if you look at the source of that, it really comes from the Commission paper we received in 1993.

MR. THORP: And D3 for anyone in the audience who perhaps is not familiar with it, is diversity and defense-in-depth. Trying not to use acronyms without explaining them here.

CHAIRMAN BROWN: Yes. It's interesting B- thank you, by the way. I think most B- I knew what it was, I wasn't going to say anything. You said it was a SECY paper of 1993. But, I mean, when you really get down to it how much experience in 1993 did the industry really have with the newer technologies and applications? It was not vast, and the vulnerabilities that digital-type systems bring to the utilization that we have in protection and safeguard systems have really become much more apparent as people have started looking at them more deeply. That's my personal opinion. As I mentioned in May, this is a design-type

meeting, so they bring a lot more vulnerabilities, so I can understand why we do it. But the details, we didn't really know as much about what we were talking about as much in '93. So, that's B- I would still think there's some consideration that we ought to think about hey, should we B- and I'm not advocating B- I agree with Rich. I mean, if we tried to go back and do a detailed hardware common cause failure analysis for all the little piece parts, it would be extensive to be able to do that.

Personally, not speaking for anybody but myself, we typically tried to use redundancy to ameliorate common cause failures and for critical systems to put in diverse systems, not necessarily with absolute thought of common cause, but it's a single failure-type thing that could spread through whatever. So, I mean B- but we don't want to lose the bubble on hardware common cause failures because we've actually B- John's right, we've had plenty of experience with those, and it's hard to really pinpoint a software common cause failure.

MR. STATTEL: I will note here we received the paper from the Commission in 1993. No rulemaking effort was done subsequent to that. And, therefore, this is no regulatory requirement B- there's currently

no regulatory requirement for a licensee or an applicant to perform this above and beyond analysis. Right? Most do. When we receive applications from plants who want to upgrade their systems, typically they will do a D3 analysis. However, it's not a regulatory requirement. It's really more or less guidance.

CHAIRMAN BROWN: Well, you're making it a regulatory requirement.

MR. STATTEL: And that's one of the B-

(Simultaneous speech.)

MR. STATTEL: B- and that's why we're imposing that condition.

CHAIRMAN BROWN: We're not disagreeing.

MR. STATTEL: Now, in addition to that, we're doing it here in the incorporate by reference rule, but in addition to that we've initiated a separate rulemaking effort to -- basically, a common cause failure or a D3 rule, to initiate a new rule to specifically address common cause failures. I initiated that effort about a year ago, and that is in the process.

MEMBER STETKAR: Okay.

MR. STATTEL: Because we feel that B- we agree with you that common cause failures should be

addressed in regulation, not just as guidance. And we feel that it's appropriate to have a separate 50 dot something rule that would have requirement language in that.

MEMBER STETKAR: And that would apply whether I'm looking B-

MR. STATTEL: All I&C.

MEMBER STETKAR: B- at, you know, some valve, motor-operated valve. I'm trying to get away from anything that has anything to do with I&C, or is it just I&C?

MR. STATTEL: Of course, we just think I&C, so B-

MEMBER STETKAR: I understand that. That's why I'm trying to understand what B-

MR. STATTEL: This could potentially be expanded.

MEMBER STETKAR: The reason I ask is you mention new rulemaking to address common cause failures. And I guess I see the rationale in that if it's going to be a comprehensive rule that addresses common cause failures, pump, and pipes, and valves, and the little electronic widgets, and all that kind of stuff. If it's solely addressing I&C, why can't it be done in the context of, you know, the current update

to the rules? Why do we need separate rulemaking?

MR. STATTEL: Well, because B- the reasoning is incorporate by reference was really not intended to introduce new regulation.

MEMBER STETKAR: I understand that.

MR. STATTEL: It was intended to endorse a guide or bring it into the fold of regulation. We don't have a standard that really covers this topic, so at this point in time our only option is to develop a separate rule. And the appropriate place to do that would be not within the incorporate by reference B-

MEMBER STETKAR: Certainly not within the incorporate B- I wasn't trying to imply B-

MR. STATTEL: Okay.

MEMBER STETKAR: B- that the incorporate by reference would cover it.

MR. STATTEL: Right.

MS. ZHANG: I think we B- it's just because of B-

MR. STATTEL: I mean, if there were a standard out there that adequately addressed it and we could endorse that, then I think there could be a possibility for incorporate by reference, but we're not aware of any.

MS. ZHANG: I think, you know B-

MEMBER STETKAR: And to locate it here would make it sort of a confusing and potentially obscure place to put it. We think some attention should be focused on it.

CHAIRMAN BROWN: All right. We're B- as John noted, we've probably beat this one to death, and we probably ought to move on in the interest of B-

MR. STATTEL: Very good. Very good. Okay. The next section that was affected by the change to the IEEE standard was 5.6.3.1, Interconnected Equipment. This section of the standard was enhanced to provide additional guidance for maintaining independence between safety systems and support systems, including those which are classified as non-safety related. This revised section expands on the concept of associated circuits and provides guidance criteria for establishing necessary independence between these systems.

Right now I'm really just explaining what changed in the IEEE standard. We don't take any exception to this enhanced guidance that was provided in this standard, but in addition to that we're going to be providing criteria that we'll talk about later. Okay?

Change number six, okay. This is an

interesting one. It's actually pretty simple. The standard requires system surveillance testing to be performed periodically to insure safety functionality during plant operations, so it is necessary for licensees to be able to bypass or prevent safety system actuation during these maintenance activities.

The purpose of this clause, this is Clause 6.7 of the standard, is to establish performance criteria for situations requiring systems or portions of systems to be in a bypass state. It requires safety systems to retain capability of performing safety functions while the surveillance or maintenance activities are being conducted.

In the 1991 version of the standard, this requirement was stated and it was immediately followed by an exception clause. I'm going to show that on the next slide. The exception clause identified conditions where certain portions of the safety system could be tested or placed into maintenance bypass without satisfying the criteria of the preceding clause. So, if you look at the next slide, this is the actual language from the 1991 version of the standard. Okay?

So, when IEEE revised the standard, okay, this exception was determined to be contrary to the IEEE policy. The IEEE policy is that the requirement is not

truly a requirement if there can be allowable exceptions. To address this policy, the IEEE 603 Working Group changed a "shall" to a "should," as I'll show you in a second which effectively changed the requirement into a recommendation. The exception clause was also reworded and retitled as a note. And if you look, I'm going to go back and forth between this and the next slide so you can see the difference. So, you can see the "shall" changed to a "should" right there on the top paragraph. And you can see the clause below changed into a note.

The NRC does not agree. We had a lot of discussion about this particular change. We ended up with a position where we don't agree with the softening of the requirement; therefore, the rule states that the criteria from the 1991 standard should be used in lieu of the new Clause 6.7. Okay? And I'm going to reference that when we get to that as we go through the actual changes to the rule, so store that in your memory that this is the reason we're proposing that. So, basically, this version of this clause is what becomes regulation.

MEMBER BLEY: And it keeps the exception.

MR. STATTEL: Exactly.

MEMBER BLEY: Right.

MR. THORP: It would otherwise be

impossible on a two-channel system like that to be able to do maintenance.

MR. STATTEL: It's necessary to have it. We've always been using that.

MEMBER STETKAR: You're keeping the "should."

MR. STATTEL: No, we're B

CHAIRMAN BROWN: Are we going back to the whole thing. I'm back B-

MR. THORP: We are retaining the tougher requirement. We don't want to soften it.

CHAIRMAN BROWN: See, I'm back reading the rule language. All right. Yes, okay, I guess I'll see. My initial impression was that it was only the B- that it was just the exception and the note that you were taking issue, but now B-

MR. STATTEL: Rather than try to add a new condition onto the existing clause requirements, we simply refer back to the '91 version for this particular clause.

MEMBER STETKAR: Rich?

MR. STATTEL: Yes?

MEMBER STETKAR: Are we B- I didn't want to interrupt. Are you done with this topic?

MR. STATTEL: Sure.

MEMBER STETKAR: Okay. I'd like to ask you a couple of things about bypasses. Let me go back to Section 5.8.3 which addresses indications of bypasses. I want some clarification because a couple of phrases in that section I have questions about.

In one area it says, "If the protective actions of some part of a safety system have been bypassed or deliberately rendered inoperative for any purpose other than an operating bypass continued indication of this fact for each affected safety group shall be provided in the control room." That seems to tell me that I do not need continuous indication of an operating bypass. Is that correct? And if so, why not?

MR. STATTEL: Well, that is correct. There is a separate criteria that deals with the requirements for operating bypass. And, essentially, for operations of the plant we typically don't want to have alarms, you know, indication of an abnormal status when that is the normal status. So, if you have, for instance, low pressure safety injection bypassed because you're operating in a low pressure C-- you're operating the plant B- I guess "operating" is not the right word, but B-

MEMBER STETKAR: Yes, no. You're in a low pressure.

MR. STATTEL: Right. You're operating the plant and you have a low pressure condition by design. Now, there is a requirement, so if the pressure were to increase that that safety function would automatically enable itself. Right? But there's not a requirement to have this like this locked in alarm status, abnormal B- telling the operator something is abnormal when, in fact, that's not an abnormal status. That's the normal condition for this state of the plant.

MR. THORP: In that example, they would have gone into that bypass condition through the course of the execution of their procedures, and it'll be a perfectly normal condition.

Another concept within the control room is the concept of a dark bus such that the presence of activated alarms, if they were continued to allowed to occur or grow would present a distraction to the operator, so in cases where an alarm or other feature is bypassed to minimize the repeat instances of alarms it's tracked in an alarm control program or manual of some kind, and a sticker is placed on that indicator. The indication is thereby rendered dark so that when a new alarm comes in it's something that presents itself to the operators and allows them to deal with the situation. So, that's just another little piece of

philosophy on that issue of bypass.

MEMBER STETKAR: Let me make a couple of notes here because I'm a slow writer.

MR. STATTEL: Plants will have a temp alt program or whatever to govern that.

CHAIRMAN BROWN: But based on your comment, though, there is some B- I mean, say there's an indicator, an alarm module or whatever it is, you would expect if it was being bypassed and it's out, that there's something on it that the operator would see, although it's not projecting itself in terms of confusing with other things that may come out B-

MR. STATTEL: Yes, will be monitored under a controlled process of some kind, procedures and other programmatic controls.

MR. THORP: I mean, there are several examples we can discuss, but it's really more of a human factors consideration. We don't want B- I mean, in an ideal world there will B- if there is no abnormal situation we should be able to take the plant from one state to another without having alarms. Right? Because, basically, this is a normal operation of the plant.

I guess another one would be the automatic isolation of residual heat removal systems. That would be another operational-type bypass.

MEMBER STETKAR: There's a number of them, and if everything works perfectly and the operator B-

MR. STATTEL: Turn the right switches at the right times.

MEMBER STETKAR: B- is 18 days into an outage really remember that that's bypassed in the heat of the battle? That's fine. If, for example, the automatic system that resets the actuation doesn't work, the operators probably wouldn't recognize that.

MR. STATTEL: But those are regulatory requirements, as well, for those operational bypasses, and those are checked for operability per the surveillance test, as well.

MEMBER STETKAR: If everything always works perfectly the operators don't even need to be there.

MR. STATTEL: I mean, it's the same requirement. The requirement to trip the reactor on high pressure, basically, that is confirmed to be operable through the surveillance programs. The same surveillance programs are used to verify the removal of bypass for these types of functions, so operational bypasses removal is treated in the same respect.

MEMBER STETKAR: Let me ask another question about B- and I B- unfortunately, I'm not multitasking here fast enough. There's another part of

that section about indication bypasses that says, "This indication shall be automatically actuated if the bypass were in operative condition is expected to occur more frequently than once a year, and is expected to occur when the affected system is required to be operable."

Why do I care whether it's more frequently than once a year? In fact, the less frequently it happens in alert, I would seem to like to be alerted to a condition. If it happens every day, you know, I'm pretty well used to it. Now, it's Section 5.8.3., and I wouldn't pull B-

MR. STATTEL: Item D.

MEMBER STETKAR: Is it Item D?

MR. STATTEL: It's a short section.

CHAIRMAN BROWN: It's on page 14 of 2009, or at least my printed out copy.

MR. STATTEL: I think it's more of a question for the IEEE Working Group. This was not something that changed.

(Simultaneous speech.)

MEMBER STETKAR: That's fine. But when I read these things, I read what's becoming law now, and I don't particularly care what was law in the past.

MR. STATTEL: Okay.

MEMBER STETKAR: Perpetuating situations C-

(Simultaneous speech.)

MR. THORP: This is already incorporated by reference via 1991. I think it was in there, as well.

MEMBER STETKAR: The world used to be flat. We learned it's not flat. That's what they tell me, anyway. Anyway, I was just B-

MR. STATTEL: I don't have a response to that. That is not something that was addressed in our conditions or in the incorporate by reference.

MS. ZHANG: I think it's another type of those human factors you don't want them to continuously be B-

MR. THORP: The idea is B- yes, my gut reaction as a former SRO license holder is that that's an issue of trying to insure operators don't get desensitized to the alarms coming in.

MEMBER STETKAR: This says B- no, this is backwards. This is exactly backwards. It says that it's automatically actuated if it occurs frequently. It is not automatically actuated if it does not occur very frequently, which is not consistent with that sort of approach. As I said, I B- if something happens every day and it always has and always will, I don't need to

be reminded of it.

MR. STATTEL: I honestly don't know of any significant bypass functions that would be operated C-- that would be exercised less frequently than once a year.

MEMBER STETKAR: Oh, the two or three that you mentioned, if I have an 18 or 24-month refueling interval.

CHAIRMAN BROWN: And no scrams.

MEMBER STETKAR: And no scrams.

CHAIRMAN BROWN: A lot of people do that now.

MEMBER STETKAR: Yes, fueling breaker to breaker for two years, many of those bypasses are only instituted once every year and a half to two years.

MR. STATTEL: Well, I have not seen an application where someone wanted to not cause an annunciation when they're bypassing a trip function like that.

MEMBER BLEY: But this is the rule they're going to live by.

MR. STATTEL: I understand. I understand.

MS. ZHANG: We'll look into it.

MR. STATTEL: That's a good point.

MEMBER STETKAR: Now, and this is B- I

waited until here, but I thought I'd bring it up. In the standard, the standard addresses sense and command, executed functions, and whatever they call C-- power supplies in Section 6, 7, and 8 of the standard. And it addresses maintenance bypass in each of those sections. And each of those sections has a clause that essentially says that when you have a maintenance bypass condition, that reduces the available redundancy to zero. In other words, you are now B- whether you're at three out of three, two out of two, one out of one, whatever the coincidence logic is, but you must demonstrate acceptable reliability. How does one determine that the reliability is acceptable, and where is the Staff Guidance if I'm reviewing a design to determine what is acceptable reliability? And what is acceptable reliability B- is acceptable reliability applied in isolation to each of those three separation functions, or is it applied in some sort of integrated sense?

So, for example, if I have a piece of equipment that has B- if I'm down to a one out of one, let's say, just take a simple two-train plant. And I'm down to B- and I have a digital instrumentation and control system that is ostensibly more reliable than an analog relay-driven system. The end user, that end

piece of equipment that has to start and operate might have a reliability of something on the order of two or three failures in 100 demands, if it's a big complicated piece of equipment.

The intermediate B- and that might be governing for a power supply if it's a diesel generator, for example. Other pieces of equipment might have a reliability of a couple of failures in 1,000 demands. The I&C portion of it might have a failure and one in 10,000 demands. So, what is an acceptable reliability now if I'm down to a one out of one? Is it 95 percent reliability for the integrated system, is it one failure in 10,000 demands if I only focus on the I&C portion of it? And how does a reviewer determine whether B- what's acceptable?

MR. STATTEL: Okay. I can tell you how we address that during our safety evaluations. As you know, we rely on, basically, a risk-informed approach to regulation, so typically the licensing basis establishes what's acceptable for reliability. So, if we have a plant that's upgrading a system or making a change to their design, the tech specs, the limiting conditions for operation kind of establish it. So, if we have a reduction in redundancy, if one channel is out of service, there might be a two-hour limiting

condition, LCO associated with that condition. So, that's established. Right? That's the licensing basis that we work off of. So, if they're upgrading to a system, and they can show that the replacement is as reliable as the system that they are replacing, then staying with that number might be acceptable, as an example.

It is case by case, though. We do evaluate this. If they want to extend that from one to two hours based on an increase in reliability of the replacement system, then we have to factor that in, as well. And, typically, we'll get the reliability analysis group involved with that evaluation.

MEMBER STETKAR: Okay. Wipe the slate clean now and let's say I come in with a brand new design.

MR. STATTEL: Correct. Yes. Yes, and that is B-

(Simultaneous speech.)

MEMBER STETKAR: I don't have 30 years of tech specs that have been grandfathered in, you know, somebody said sometime said oh, a couple of hours sounds good, and we've always used a couple of hours.

MR. STATTEL: Actually, I'm going to let Deanna speak a little bit to this because it is more of a new reactors issue. Typically, when we're

evaluating B-

MEMBER STETKAR: But this does apply for C-

MR. STATTEL: I agree. I agree, but typically for NRR when we're working with an operating reactor we use that existing licensing basis as kind of an anchor point from which to compare the changes. And we do consider the reliability.

Reliability analysis, by the way, is a required document. We look for that in the safety evaluation, so oftentimes they'll come up with a required B- a reliability analysis, and it'll put these very objective numbers that the system is this reliable. What does that mean to us? All right. If we don't have anything to compare that to or any criteria, you know, we have to evaluate that. So, we always revert back to what the current licensing basis is. But I'll let Deanna talk about the new reactor situation.

MS. ZHANG: For new reactors B- well, first of all, for new reactors we tend to have more redundancy than existing reactors for the most part. In other cases similarly to what existing reactors do we do look at the tech spec surveillance requirements and the LCO conditions that are B- that's been established B- that's being established for the new plant design.

MEMBER STETKAR: Deanna, let me interrupt

you just to get something on the record. Yes, we do have more redundancy, but we also have in general more relaxed tech specs. So, for example, in a B- just to get it on the record, in a four-train redundant plant, typically what you'll see is you're allowed by tech specs to have one train inoperable indefinitely. That can be covered under maintenance rule or things, but by law you can have one train inoperable indefinitely. You can have a second train out of service for some time period, which does get you down to this zero redundancy, because it then becomes a two out of two actuation logic, so the licensee or the applicants and the regulations have accounted for that larger redundancy with more relaxed criteria in terms of allowing people to do online maintenance and things. So, just because I have a four-train redundancy doesn't mean that I can't get down to a two out of two required.

MS. ZHANG: Again, as you have mentioned, the conditions in which we get to the two out of two train, you know, to have a second train out of service, that is a very limited time, and there are additional requirements, tech spec requirements imposed during that period of time.

MR. STATTEL: Now, we also receive applications where tech spec changes, for example,

where a plant wants to be able to perform a maintenance activity to deal with a failed component and they don't want to go through like a temp alt type situation in order to maintain operability, so they'll actually make a PRA argument that it's safer to just extend the LCO time and maintain operations, as opposed to either shutting the plant down or installing temp alt jumpers and things like that for those activities. And, again, we evaluate those on a case by case basis, and there have been cases where we've approved the changes they propose to the tech specs.

MS. ZHANG: Also, in addition, I think this is where some of the benefits of digital technology comes into play in that there is continuous self-testing going on so that if there's any errors or anything, you know, that are detected it will be announced B-

MEMBER STETKAR: My whole point, though, is that B- if you go back to my original example where I have sort of three levels. One is the I&C, and I specifically said digital I&C for a reason. The other is the execute function which I can think of pumps, and pipes, and valves. And the third is power supply; those are 6, 7, and 8 of the standard. Power supply includes things like the diesel generator. The relative

reliability of each of those piece parts given a condition where I'm down to one out of one, or two out of two, or three out of three regardless of what my design looks like. The relative reliability of each of those piece parts is much different, and yet I'm now asked to demonstrate that I have acceptable reliability when I am in that minimal operating configuration.

My question originally was how do I demonstrate that, number one. And number two, do I demonstrate that in an integrated fashion where I may be limited B- I'm back to what am I am limited by? I may be limited by the fact that the diesel won't start. I don't care about demonstrating that it's one times ten to the minus four, or two times ten to the minus four, or three times ten to the minus three in the context of the I&C system because that's irrelevant. So, I'm not sure how people would apply these. Do they apply them in isolation? Oh, I have to demonstrate acceptable reliability of my digital I&C which is ten to the minus four per demand. Well, that doesn't seem to make sense if I'm limited to ten to the minus two.

MS. ZHANG: From a reliability perspective that's definitely true. If you look at reliability of the system as a whole, oftentimes your I&C system is not the limiting factor.

MEMBER STETKAR: Right.

MS. ZHANG: You know, you have to look at the sensor to the final actuating device, as well as the support systems. And, again, you know, even when you do look at reliability numbers, you know, you take into account, you know, maintenance, how often is it? What types of failures that can occur, detected, those that can be detected, those that cannot be detected, and those drive your reliability numbers as a whole.

I'm B- of course, for the nuclear industry I don't know if there's a specific requirement that C-- how they calculate the overall reliability number, but I've seen other process industries, you know, how they calculate reliability numbers. And as you said, you know, from a B- from the sensor to the final actuator device there are different factors that go into how reliability is calculated, including common cause failure.

MR. WATERMAN: The other thing is that licensees are required to do a configuration analysis of the plant before they start reducing beyond the minimum required redundancy. For example, the example well, maybe my diesel generator won't start. You have to confirm that equipment is available before they go into two channels out of service.

MEMBER STETKAR: But that's a determine B- in a sense that's a logic matrix deterministic, you know, I can't have X and Y out of service at the same time B-

MR. WATERMAN: That's right.

MEMBER STETKAR: B- because I violate the law. It's not B-

(Simultaneous speech.)

MEMBER STETKAR: Or I now have to impose, you know, a four-hour time limit rather than a two-day time limit or something like that.

MR. STATTEL: And I would presume B-

MEMBER STETKAR: It's not reliability.

MR. STATTEL: I would presume that the operating plants provide a precedent or a basis for what we, what the NRC considers to be an acceptable reliability. And I would think some of that could be used for comparison purposes to determine what's acceptable in the new plants. But I'm not in the new reactor side, so B-

MEMBER BLEY: Well, on either side I think this whole discussion is really important because it says you can't look at these things in isolation. Whatever you come up with as acceptable reliability has to include all of the pieces that can cause failure.

You have to look at that in total.

MR. THORP: Without going too far off the path here one observation just from working at the power plant, that I think the nuclear industry over the decades has come quite a long way in sort of assessing, you know, what are these little contributions from all the various things that we're doing to the plant in any given condition, whether they're doing online maintenance or maintenance during shutdown conditions. And they're actually applying logically-based computer programs and PRA calculating software that looks at the actual sort of specific change in core damage frequency, et cetera, based on the removal or the effect to any given piece of equipment and how that fits within the overall picture, and actually conduct a daily calculation of that value based on the plant maintenance for the day and for the week, et cetera, to assess does this make sense for us to do this? And I witnessed many times the reshuffling of proposed maintenance and repair activities in order to achieve a reduced value in that delta core damage frequency number. So, in essence, I think it strikes me that they seem to be sensitive to that type of concern and what I see this being executed in is a very sort of practical day to day approach, so it remains within their

consciousness.

MR. STATTEL: I certainly can't speak for all the licensees; however, when I was at the plant it's a very dynamic process, so if we're performing maintenance on a system and something changes, we find something wrong or we have to change the scope of that maintenance, basically, at Calvert Cliffs, at least, we would stop the maintenance at that point and they would, basically, recalculate what B- how does this affect core damage frequency? It really came down to that level. And they would B- and the operators would have to perform an assessment before we continued on to that maintenance so we weren't going down a path where we were reducing reliability without being aware of the impact that would have on plant safety.

CHAIRMAN BROWN: I'm going to regain control of our meeting B-

MR. STATTEL: Thank you.

CHAIRMAN BROWN: B- for at least hopefully for a second, more than a second. Why don't we move on to B-

MR. STATTEL: This is the last change to the standard. I know we're running a little bit behind schedule.

CHAIRMAN BROWN: Yes, we're about 10 or 15

minutes.

MR. STATTEL: Right.

CHAIRMAN BROWN: I'm not actually running actual B-

MR. STATTEL: This is number 7. This is the last actual change to the standard, and then the next section will be what we're changing in the rule, so that will be a good breaking point.

This last change was added to the standard. This clause was added to the standard 5.6.3.1. This has to do with interconnected equipment. It introduces technology-specific guidance for communication independence which is a departure from the earlier IEEE decision to place such guidance into the companion standard of 7-4.3.2. And we're going to discuss this a little bit later when we get into the criteria that we're imposing on independence. I refer to a future slide, but we will get to that, I mean, unless there's any discussion on this point.

MEMBER BLEY: I'm just a little curious about since some of you guys were involved with the standard itself. What drives a decision to change from a technology independent standard to one that's at least a little bit technology-specific?

MR. STATTEL: It has been a struggle because

oftentimes, you know, we're trying to incorporate into the standards as we're having these Working Group meetings lessons that we've learned over the past five years. That's a typical discussion that we have at the Working Group. And most of the lessons we're learning are from using digital B- you know, incorporating digital technology. Those are the aspects, that's what we're learning, so the topic comes up.

Now, 603, they really B- a lot of the situations when you step back and think about it, they're applicable not only to digital systems. Yes, you recognized it in the process of incorporating a digital system, but in reality common cause failure, it could happen in an analog system, you know. We recognize that, so the idea of the IEEE Working Group, I believe, was let's keep it as technology neutral as we can possibly make it. But then when we get down into communications independence you just can't do it. Right? Because there are just no analogies or there's no equivalent processes that are occurring in the analog system.

So, one approach is to spill all that guidance over into the 7-4.3.2 standard. And another approach is to okay, it's just a simple clause. Let's go ahead and put it into the standard because we don't

have any way of making it applicable to all technology.

Now, another note I'll make regarding technology, 7-4.3.2 standard, the title of it is "Digital Computer Systems." Right? And there's been a lot of debate over the years over well, does that include field programmable gate array, does it include other technologies that are being introduced? And the Working Group right now in the current revision we're working on, is we are rescoping and retitling that standard. And we intend for it to apply to all digital systems no matter what the technology.

MEMBER BLEY: First up here, electrical isolation applies to everything.

MR. STATTEL: Correct, that's correct.

MEMBER BLEY: Was that in the old version of the standard?

MR. STATTEL: Yes.

MEMBER BLEY: Okay.

CHAIRMAN BROWN: Well, it was less specific.

MR. STATTEL: Right.

CHAIRMAN BROWN: The real B- let me just finish this thought before I lose it.

MR. STATTEL: Go ahead.

CHAIRMAN BROWN: If you look B- the

division definition in the old standard said you had to have electrical independence which is effectively electrical isolation. I mean, that's the way I always read it. That worked well for analog systems. I mean, once you met electrical isolation or independence you really couldn't compromise downstream systems, and you could not feed it back. Relay contact, diodes that blocked signals to even solid state voting systems really isolated you. When you go to microprocessor-based, computer-based B- those type software-based systems doesn't work. And that's what B- the argument was made in some of these early design projects that came in here, was that you would have a fiber optic link to forward electrically isolated with our serial data communication. Well, that doesn't do anything for you.

MR. STATTEL: That is exactly correct, and that's what the IEEE, the Working Group was attempting to address with this particular clause. What they recognized is that yes, you can have separation, you can use fiber optics for your communications lines, you can have electrical isolation. You know, they're completely independent but if you're not having some sort of control over the data that's being transferred across that line then you can compromise the functional

independence, and you can actually have a situation where you meet all the regulatory requirements, or all the requirements in the standard and really not meet the intent of maintaining the integrity of the safety function.

CHAIRMAN BROWN: The key metric for all of these systems is independence.

MR. STATTEL: That's right.

CHAIRMAN BROWN: No matter how you slice it. You can talk about redundancy, talk about B- well, redundancy and independence are B- they go together.

MR. STATTEL: Right. And for that reason, the Standards Working Group decided that they were going to deviate, depart from their position of keeping this technology neutral because they felt that this communications aspect was so important that they wanted to include it in the independence. That's my read on this.

CHAIRMAN BROWN: This still B- but, I mean, the words digital communication independence is a very generic term.

MR. STATTEL: Right. And later on when we talk about what's going into the rule we'll discuss how we're B-

CHAIRMAN BROWN: Yes, I'm not going to go

into that right now. I'm sure we'll have a more animated discussion later.

MR. STATTEL: Okay.

MEMBER STETKAR: Rich, I have one more on the standard. This is a generic question but it's somewhat pervasive throughout the standard. What is a credible failure? Let me read you a quote from the single failure section to put it in perspective.

"The performance of a probabilistic assessment of the safety systems may be used to demonstrate that certain postulated failures need not be considered in the application of the criterion. A probabilistic assessment is intended to eliminate consideration of events and failures that are not credible. It shall not be used in lieu of the single failure criterion."

There are other statements regarding credible failures. What is a credible failure? Is Godzilla credible, get the plug in for Hollywood.

MR. STATTEL: That's a very loaded question. I'll try to answer that.

MR. THORP: Well, while you're thinking about it, I'd like to make sure that the availability of an answer is certainly open to our senior level advisors who I certainly have a lot of faith in on a

discussion like this.

MR. STATTEL: It's certainly the subject of a lot of discussion that we have with the licensees. We particularly run into this when we review the failure modes and effects analysis reports that are provided to us. We have these discussions with regional inspectors because, you know, if you think --if you interpret that as anything I can think of is a credible failure; well, you know, we have some pretty smart people in the room and they can think if some pretty wild failures that in reality the probability of them occurring is just so minuscule that we don't consider B- we don't necessarily consider them as B-

MEMBER STETKAR: How minuscule is minuscule? That's what I'm getting to.

MR. STATTEL: Now, on the other hand there's a discussion of if it's a known failure versus an unknown failure, or if it's a failure that has occurred versus a failure that they, we've been using digital systems for 20 years and we've never seen this failure. Does that mean it's not credible?

We don't agree with that. We see in the failure modes and effects analysis, we see a lot of failures that there's no precedent for them. They haven't actually occurred. We don't have a high

instance rate of them. We have high probability numbers of these failures, but the B- you know, the analysis identified them as being credible. Right?

It is subjective, it's a subjective determination. Now, on the other hand, we B- I mean, again, this is not limited to digital technologies. If you consider the accident scenarios, I mean, there are certain accident scenarios that we don't require to be addressed in the safety analysis. So, for instance, a meteor strike on a plant site, it's not something that's in the safety analysis of a plant. So, for whatever reason from the perspective of meeting regulation we don't consider that to be a credible failure mode for that site.

MEMBER STETKAR: But if that meteorite strike is more likely than other things that we're asking people to spend a heck of a lot of effort to evaluate, is the expenditure of that heck of a lot of effort justified? That's part of this point of what is credible? Credible is, indeed, a metric. We pay a lot of lip service to the notion of risk-informed regulation. Risk is frequency and consequences, and uncertainty.

MR. STATTEL: Yes.

MEMBER STETKAR: And credibility is simply

a word. Anything, you know B- I don't know what brought down the Malaysian Airline. It is a credible event because it happened, if we can ever figure out what it was. We also had the meteorite streak across Siberia. There have been flies in lube oil, for example, that have disabled pieces of equipment. Things that we haven't B- you know, can you think about them? Yes, you can think about them. What is the likelihood? That's a different question.

So, the question is moving forward, we're now in 2014, we're not in 1971. And we pay a lot of lip service to risk-informed regulation, and yet we tend to use these very subjective ill-defined terms like credible throughout our regulations.

MEMBER BLEY: If I'm somebody new that's just shown up and I B-

(Simultaneous speech.)

MEMBER STETKAR: I'm sorry. This is incorporated by reference in our regulation, and credible is pervasive through it, so it is in our regulation.

CHAIRMAN BROWN: Are we the only ones that do that? I don't think so.

MEMBER STETKAR: No, that's okay, but that, you know B-

CHAIRMAN BROWN: I'm trying to regain control of my meeting here.

(Laughter.)

MEMBER STETKAR: I'm not sure if anyone else uses the term "credible."

MEMBER BLEY: Well, I would just like to make a comment to go back to where John was a long time ago, and where Mike started in responding to him. 5.1 just smells like somebody trying to tell me common cause failures of equipment are so unlikely we don't need to think about them if we've thought about the big connecting things like support systems and that sort of thing. And, yet, the last time I look at the failure histories and I haven't looked at this stuff for a few years, problems on cards, hardware problems on cards popped up, a number of cards, four or five out of a rack of ten and things like that are still happening, so it seems like almost wishful thinking use of the word "credible" and the thing John just brought up. We're real interested in how you tell people to deal with that.

MR. STATTEL: Well, it is case by case. And in the case of common cause failure we have established a position, so we do get arguments that oh, this is not credible to have a common cause failure across

divisions. That doesn't matter from our regulatory perspective. It still needs to be considered. We still consider it credible no matter the probability is, so we don't let people B- we don't allow licensees to use a risk argument to dispel the credibility of that B-

MEMBER STETKAR: But why not?

MR. STATTEL: Well B-

PARTICIPANT: Because we're not risk-based.

MEMBER STETKAR: No, you're not even risk-informed.

MR. THORP: Okay. We do have a contribution to the discussion from our senior level advisor.

(Simultaneous speech.)

MEMBER STETKAR: We finally provoked him out of the B-

MR. ARNDT: Steve Arndt at NRC. Two points, and I don't want to belabor this. But to John's original point about credible and level of definition of that, things like that. One of the rationales, of course, is when we don't have enough information to provide very specific guidance, or we choose not to provide specific guidance, the primary reason for that is to allow the Staff to exercise engineering judgment. And as Rich highlighted, we give the Staff and the licensees in Reg

Guides and in Staff Guidance in the SRP criteria for evaluating and using that engineering judgment, the kinds of things that should be in the failure modes and effects analysis, the kinds of things we need to look at, where we get sources of information such as previous failures and previous analysis.

So, really it is somewhat challenging, as you pointed out, that we're not completely consistent across technologies in terms of what is credible and what's not, but the primary purpose there is to allow the Staff to exercise engineering judgment based on their technical capability and the industry submittals.

To go to your second point on common cause failure, the particular reason that we don't exercise the option of allowing certain software common cause failures to be credible is because the guidance we got from the Commission specifically did not allow us to do that. It said you will do this particular thing, so in that particular case that's the guidance we got. And until we decide that we need to go back to the Commission and get a different read on that, that's where we are.

MR. STATTEL: In truth to make an argument for credibility or not credibility of any particular failure mode you have to identify it first. Right? I

mean, there have been cases where I've reviewed failure modes and effects analysis where the licensee or the applicant has identified a failure and I look at that, wow, I would not have thought of that. And it's not entirely surprising because they are the experts on the systems that they're designing. Right? But it also leads me to the question of well, what other failures might there be out there that I haven't thought of. Right?

So, there's no definitive answer to that. But I will say when we're performing these evaluations and we're reviewing these analysis reports that are required to be performed by the licensees, if they identify a failure mode and they make an argument that it's not credible, we do key in on that argument, and we do challenge that. I mean, that's just common sense for us to do that. So, we'll typically B- we'll perform audits, and we'll how they're addressing, or how they're confirming that, in fact, that is not a credible failure mode if they make that argument.

CHAIRMAN BROWN: Can I go on, please?

MR. STATTEL: I think it's a good break point now.

CHAIRMAN BROWN: Well, I was going B- we're going to do one or the other. I was going B- I was

noticing in the schedule that we were due to start on the independence part, which is about page 23 of the slides.

MR. STATTEL: Okay.

CHAIRMAN BROWN: And there are about three slides to get to that point, then we were going to break at 10:15. And I looked B- they didn't seem to be overly complex, although that might happen on the 5.1.5 since I may have some comments on that, but the rest of it looked like it was kind of how you were calibrating the integration of the new rule in with all the various age gaps that exist for the older B-

MEMBER STETKAR: We should take a break now.

(Laughter.)

CHAIRMAN BROWN: My astute and wonderful Staff over here on my Subcommittee says we will take a break now.

MEMBER STETKAR: Staff?

CHAIRMAN BROWN: Well, I'm calling you Staff in this case. Okay. Good suggestion, thank you, Rich, prod me a little bit. We will break now for 15 minutes until 10:25, and then we'll resume the meeting. Recess.

(Whereupon, the proceedings went off the record at 10:08 a.m., and went back on the record at

10:29 a.m.)

CHAIRMAN BROWN: Okay. The meeting will come back to order, and we will proceed where we left off with the summary, or that's not a summary, I guess that's where B- is that where you're going next?

MR. STATTEL: That's where I'm going next, yes.

CHAIRMAN BROWN: Yes.

MR. STATTEL: Thank you. So, basically, what we discussed in the first session is just what was changed in the IEEE standard. Now what we're going to be doing is getting into the meat of the presentation, and that's how the NRC is reacting to that, and how we are incorporating that standard into the regulation. So, basically what is changing in the regulations, and we're taking a little bit different approach here.

Now, I'll point out in the proposed rule package that was sent to you, and I hope that you figured this out, the actual rule language that's being proposed doesn't start until page 136. All right?

MEMBER STETKAR: Yes.

MR. STATTEL: Okay?

MEMBER STETKAR: Oh, darn.

MR. STATTEL: Yes. I won't speak to why it took 135 pages to get to that point. I'll let Dan answer

that, if that question comes up. But that's where B- I just want to point you to that. That's where the actual rule language is that I'll be referring to. Okay? So, this slide shows what's changing in the regulations, and I'll cover each of those in detail.

Okay. I'll start out with definitions. Okay. For the context of this rule these are the terms, what you see on the slide. These terms are defined in the Federal Register Notice document which is the proposed rule. It's within that 135 pages I mentioned. This was done to provide a common understanding for each of these terms as they are being applied to the different standards being referenced in the Code of Federal Regulations.

It is intended that these definitions be applied by the NRC for underlying basis of 50.55a(h)(2) through (h)(8), which cover all of the conditions that we are imposing on this rule. Some of these terms are being introduced by the rule. They're new. These are the terms that on the slide are colored in blue. Okay. The rest of the terms used within the B- are used within the reference standards or Reg Guides; however, the definitions in these standards are not necessarily consistent with each other, so the Working Group decided to provide a common definition to avoid

ambiguity in these cases. Now, another note, these definitions can be found between page 11 and page 17 of the FRN document.

Now, I apologize to the members of the public that don't have access to this document. I believe it will be made public shortly after this meeting.

CHAIRMAN BROWN: Well, they're also included in the glossary for Reg Guide 1.1.5.3.

MR. STATTEL: Right. Those definitions are also included in the Reg Guide. That's correct. And Mike will talk a little bit about why that is when he gets to his part of the presentation here. Are there any questions on the definitions while I'm on this slide?

I'm not going to B- I wasn't planning on discussing each of the individual definitions. We will be referring back to them when we get to B-

CHAIRMAN BROWN: Can I ask a question on them then?

MR. STATTEL: Certainly.

CHAIRMAN BROWN: Okay. On the definition for hardwired connections.

MR. STATTEL: Okay.

CHAIRMAN BROWN: Which reads, "Hardwired connections in the context of 50.55a(h) is defined as

a permanent physical point-to-point connection that is used to transmit signals. Hardwired connections can be implemented using various physical media, copper wire, fiber optic, for example."

Now, is this to imply or mean that those are not software-based signals being transmitted on those hardwired connections?

MS. ZHANG: No, there's other B- so, we had a discussion B-

CHAIRMAN BROWN: There's another part about data communications.

MS. ZHANG: Yes.

CHAIRMAN BROWN: That's very clear, it says what that means. "Information encoded in a specific format." But a hardwired connection can transmit B-

MS. ZHANG: Data.

CHAIRMAN BROWN: B- data communication.

MS. ZHANG: And I'll kind of explain why that's the case. So, originally, we had, you know B- we thought of hardwired connections as just, you know, transmitting, you know, a zero B- you know, like an on/off B-

(Simultaneous speech.)

MS. ZHANG: And like it wouldn't be data communications. It's like, you know B- I thought that

was well understood, but when we discussed it among different members and, you know, people in the Staff, that wasn't the case how they understood hardwired connections to mean. So, we generated this hardwired connections based on a common understanding that we kind of agreed on, but we added a definition for data communications, and in the rule language specified which cases would B- you know, you could use data communications, and which case you couldn't use data communications.

CHAIRMAN BROWN: Very specific in a few places where you said don't use data-type, and it defines those. Those are obviously serial data links or whatever B-

MS. ZHANG: Yes.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: Those types of links.

MS. ZHANG: Yes.

CHAIRMAN BROWN: But a hardwired connection does not B-

MR. STATTEL: A relay B-

CHAIRMAN BROWN: B- data communications going because, obviously, a fiber optic link can do serial data.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Coax cable, can do serial data, et cetera.

MS. ZHANG: Exactly.

CHAIRMAN BROWN: So, I was wrong in parenthesizing non-software based.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Okay.

MS. ZHANG: There were certain reasons why we had to B-

CHAIRMAN BROWN: So, it can be hardware, it can be software-based or regular old analog signals.

MS. ZHANG: Yes. So, in this case it just talks about the type of connection it is.

CHAIRMAN BROWN: Okay. The second one was physical mechanism where you said in the context of the rule, it's defined as a means to enforce one-way communication from safety systems to non-safety systems through a hardware-based method such that no software is used to maintain the direction of data flow. So, there are two questions here. One is, why just safety to non-safety? Why not safety to safety, as well? And why not B- when it says no software is to maintain the direction of flow, the software should not select the B- be used to select the direction of flow. In other words, there's not some software-based component of

that physical mechanism that can switch it from unidirectional to bidirectional.

MR. STATTEL: Well, the idea is that there is no reliance on any software component.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Well, but I'm just saying the words say only to maintain the data flow, not to B- the basic selection. That's a nuance.

MS. ZHANG: I think the intent of it was not for it to use software to select the direction of data flow.

CHAIRMAN BROWN: Well, I'm stumbling on the intention, what it's supposed B-

MS. ZHANG: Yes. The reason we used that to maintain the direction of data flow is that we don't want the software used, so we want a hardware-based device. We don't want software used to prevent data communication going back the other way. So, that was the intent.

Now, about the switching of, you know, directionality, I think that's why we said only, you know B- data communication can only be from safety to non-safety.

CHAIRMAN BROWN: That's not true, though, because you send safety signals from one division to

the voting unit of another division, and that's a safety to safety interdivisional transmission, and you do not want B- I mean, if I had my way, which I don't, okay, that right now is done with B- it can be serial data into another computer-based unit as we've seen in a number of the new design projects.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Which brings up one of the vulnerabilities that we discussed ad nauseam in many of the meetings.

MS. ZHANG: And in this case we were only specific to data communications between safety and non-safety. For data communications between safety divisions we have other criteria that we have added to establish what types of data we're allowing to communicate between redundant portions of safety systems.

MR. STATTEL: I mean, we'll get into the discussions on the criteria.

CHAIRMAN BROWN: Okay.

MR. STATTEL: This particular term is only used in the clause that we're introducing for safety to non-safety communication. The terms is not used in the regulation.

CHAIRMAN BROWN: Okay. Back to my nuance is

what is it B- is it a manual B- I mean, the way I would view this if I was thinking my irrational way would be I have to go to the device, I have to take out a little thing, and I have to switch a wire or a plug from one point to another if I wanted to change the hardware-based directionality. A lot of these devices hardware come bidirectional. It just depends on whether you don't connect B-

MS. ZHANG: Well B-

CHAIRMAN BROWN: Or you ground it, or whatever.

MS. ZHANG: There are several ways you can implement this type of communication. One is to use fiber optics, and you only have a transmit on the safety side. Right? Another way is to have an actual, you know, kind of like a data diode type of device, you know, where there's just going B- nothing physically going back. So, we didn't want there to be like a specific technology that we're specifying here, you know. But the way we B-

CHAIRMAN BROWN: I'm not asking for a specific, I'm just worried about the B- how is it determined what B- that it's only going to be unidirectional, that there's not a little card invoked in the thing which now switches something, you can

switch and actuate remotely that would change the direction of flow from uni to bidirectional? That's my only point.

I'll get away from the safety to non-safety. I'll look for the other discussion, but it's still B- you can still have a hardware device which has a software component that says how is it going to operate, and it can be told to do that remotely. So, that's my point. And my suggestion would have been to select or maintain B-

MR. STATTEL: Well, what I recommend is we defer this conversation until we get to where the actual term is used in context.

CHAIRMAN BROWN: That's fine.

MR. STATTEL: And then we'll continue this discussion.

CHAIRMAN BROWN: Is it in the rule, or is it some other place?

MR. STATTEL: It is in the rule, yes.

CHAIRMAN BROWN: Okay. I just don't remember that.

MR. STATTEL: Yes, it is in the actual rule language, so it will be in the CFR.

CHAIRMAN BROWN: All right.

MR. STATTEL: Okay? Any other terms?

CHAIRMAN BROWN: No, that was it.

MEMBER STETKAR: You didn't define credible.

(Laughter.)

MR. STATTEL: I noted that when B-

MEMBER STETKAR: And I'm not sure credible is used in the rule actually.

CHAIRMAN BROWN: I don't remember seeing it in the rule myself.

MR. STATTEL: And we can refer back to these at any time as we see the terms. Okay?

So, a backfit analysis was performed and it determined that the application of the new criteria was not mandatory for current license holders. Instead, the new criteria will be applied to new applications and selectively to license amendments depending on several factors that are identified in the proposed rule, such as the introduction of digital technology to I&C systems.

The previous date-based applicability in the current regulation, those clauses were left in place in order to maintain the existing design basis for the currently licensed operating facility. These conditions are based on the issuance date of the plant's construction permit, standard design cert, or

manufacturing license.

A new set of criteria was then added to define the applicability for the IEEE 603 2009 version standard criteria including conditions implemented by this rule. The rule also allows voluntary application of the new standard and conditions for previously licensed facilities. So, basically, an applicant can always choose to use the new version of the standard in lieu of their license-basis standard on a voluntary basis. But there are conditions where they would be required to use the new standard.

Okay. The table that's on this slide can also be found on page 22 of the proposed rule document that you have.

MEMBER STETKAR: Okay. Rich?

MR. STATTEL: Yes?

MEMBER STETKAR: Are you going to spend any more time on the table?

MR. STATTEL: Unless you want to.

MEMBER STETKAR: I do.

MR. STATTEL: Okay.

(Laughter.)

MEMBER STETKAR: Sorry. I was trying to understand how this works, and I think I do. So, I'd like to explore a couple of examples. As I understand

it the GE ABWR certified design, if I were going to actually build one of those sometime in whatever future would be required to comply with IEEE Standard 279-1971. Is that correct?

MR. WATERMAN: Yes.

MEMBER STETKAR: Does that make any sense?

MR. WATERMAN: Yes, it does, because it was design certified at the time when 279-1971 was the regulation.

MEMBER STETKAR: To what extent did the GE ABWR employ DAC in the nondescript design of its digital I&C systems?

MR. STATTEL: I don't know, but I assume that any B- okay.

MR. JUNG: Let me answer that question. It's a B- at the time, the design details at the time addressed a lot of the safety issues at the same time specific digital system implementation. I just want to emphasize that specific implementation of the life cycle development process, the whole life cycle process themselves is DAC.

MEMBER STETKAR: Where I'm getting at is, does it make sense that I could have an ABWR whose licensing COL process does not begin until at least 2015 because I haven't seen any of those on the radar yet

that you certify design. Constructed somewhere in the 2020s and be held accountable to 1971 standards? Does that make any sense at all?

MR. JUNG: Let me B-

MEMBER STETKAR: Given the fact that there's no details about the design of that system whatsoever, so we're not talking about something that has been built and is operating. I'll get to AP1000 in a moment because you'll see where this is leading.

MR. JUNG: Let me answer that in two ways. One is a legal answer which you may not like.

MEMBER STETKAR: Fortunately, we are not attorneys, we're simply B-

MR. JUNG: Right. I still have to answer that in a way because B-

MEMBER STETKAR: Yes, I understand.

MR. JUNG: B- there's a specific regulation in Part 52 associated with the finality. You know, once B- it's by rule the Commission approved the design to be safe. So, anybody who reference that design we are not revisiting that safety issue because it's a B- unless there's a specific backfit of a concern that rise to a very high level.

Second, the other answer is related to the reality of what happened in South Texas. Hopefully, you

can remember for South Texas when they came in with a COL for using ABWR. Staff had significant interactions, and if you remember Subcommittee, there was a pilot for DAC implementation.

MEMBER STETKAR: Right.

MR. JUNG: In that what South Texas and Staff agreed to is that South Texas would B- actually made a departure to come in with the later standards. That was the direction we are heading.

MEMBER STETKAR: But South Texas isn't literally using the GE-certified ABWR design. They're using a modification of that certified design.

MR. JUNG: Modification to that B-

MEMBER STETKAR: So, I'm talking about a GE cert. Suppose I have an applicant come in next year and say I want to take the GE-certified design and build a plant at my site some time in the 2020s. That applicant would only be required to meet the 1971 version of the standard for the design that they would eventually try to develop, because there is no developed designs.

MR. JUNG: That's B- the answer is yes. However, remember they B- both Toshiba and GE came in for renewal of the ABWR designs, and during that interaction with GE and Toshiba the Staff specifically identified that issue as a recommendation for GE to

address, but it's not legally required to do so. It is more of a recommendation at this point, so the finality rule still applies. And that's the answer we have at this point.

MS. ZHANG: But the design certifications, they have a limit on them. Their certification is a 15-year limit.

MEMBER STETKAR: But we just heard that when they came in for renewal the design B- the finality apparently applies for the renewal, so that you can't, apparently, say well, when you renew you should meet the most recent standards. Is that correct?

CONSULTANT HECHT: Can I offer something here?

MEMBER STETKAR: Hold on a second. We're dealing in NRC B-

MR. JUNG: That is B- I understand that is true because it's a rule that it requires essentially a rule change to allow B- to force that. The rule change means backfit strict, backfit criteria. But I fully understand your concern, and Staff understands the whole issue of obsolescence. For South Texas, obsolescence was the real issue, the technology they have chosen at the time of certification was a completely different protocol, and building that

design would be a challenge. But from a Staff perspective obsolescence by itself is not a specific safety reason by itself to apply backfits.

CONSULTANT HECHT: I was going to expand on that point by saying it's highly unlikely that a plant that was to be built in I guess 2018 or 2019 would utilize 1990s technology.

MEMBER STETKAR: It isn't the technology, it's the requirements in the standard and the rule. For example, hardware-based communication, one-way communications. I don't know whether that's in 1971. I doubt that it is since it was included in 2009.

It's not the B- I don't care the widgets that they're going to install, it's the requirements that they must satisfy in terms of independence, diversity, defense-in-depth, you know, one-way communication, all that other stuff.

CONSULTANT HECHT: But doesn't this B- but doesn't the B-

MEMBER STETKAR: No.

CONSULTANT HECHT: B- new rule here imply that B-

MEMBER STETKAR: No, no. I can build a plant in 2050 using the certified ABWR design and not meet the requirements of IEEE 603-2009.

MR. WATERMAN: Paragraph 3 deals with trigger points at which 2009 must be used.

MEMBER STETKAR: Yes.

MR. WATERMAN: And in there is when you make extensive changes to your systems that involve diversity and defense-in-depth and things like that you've got to go to 2009.

MEMBER STETKAR: But couldn't I build a plant in, pick a year, 2050, five-zero, and reference the GE certified ABWR design and not need to comply with the requirements in IEEE Standard 603-2009 provided that I don't do anything B- I don't care about B- because as long as I can demonstrate that whatever widgets I put in there perform the same function as the functions that are in the certified design, whether they're relays or whatever.

MR. WATERMAN: Wouldn't it be safe enough?

MEMBER STETKAR: Well, that's B- haven't we learned in the last 28 years things that we would like people to do? That's my whole point. If it was safe enough in 1971, why is the IEEE in all of their wisdom, and the NRC in all of their wisdom said that oh, we should actually require new plants to meet this enhanced standard?

MR. WATERMAN: Because people are using

newer technology that was B-

MEMBER STETKAR: No, no, no, no, not widgets, not widgets.

MR. WATERMAN: It is widgets.

MEMBER STETKAR: The diversity and defense-in-depth, one-way communications, independence, determinism, all the stuff that Charlie has been preaching is not widget-dependent. It's a philosophy. 603-2009 is more philosophy than widgets, that's why it applies to relays, it applies to digital I&C, it applies to software, it applies to everything.

MR. STATTEL: But it's really not B- I mean, what is the relevance of the data construction because we have plants that were built in 1971 that are held to that same standard, but we allow them B-

MEMBER STETKAR: I understand backfits B-

MR. STATTEL: B- to continue operating.

MEMBER STETKAR: That's fine. I understand currently operating plants for which designs exist.

MR. STATTEL: Okay.

MEMBER STETKAR: I'm not at all challenging that.

MR. STATTEL: Okay.

MEMBER STETKAR: I'm challenging a new plant whose design was not specified in any clarity

whatsoever in the certification documents. And, indeed, I'm not challenging Vogtle and Summer because they are being built, they have real designs. So, saying that 203-1991 applies to them makes perfect sense, they should not, unless they make going forward substantive changes.

MR. STATTEL: That's correct.

MEMBER STETKAR: That's fine.

MR. STATTEL: All right. The next slide will talk about those triggers.

MEMBER STETKAR: Yes. But ESBWR is now held to 1991, ABWR is held to 1971.

MR. WATERMAN: System 80 Plus is B-

MEMBER STETKAR: Yes, but who is going to build a System 80 Plus?

MR. WATERMAN: Korea builds a lot of them.

MEMBER STETKAR: We don't regulate Korea, so B-

CHAIRMAN BROWN: That's true. The other point is 271, or if you look at how that ABWR, the GE one was certified, you probably could not define the level of functionality independence within its design because it wasn't specified. It was devoid of information, so the trigger points you're talking about would B- there were none. You couldn't point to a

trigger point to say hey, you have to comply with the new standards because if you look through all the trigger points you talk about they're not there. They weren't defined as part of their certified design.

MEMBER STETKAR: But if somebody were going to build that plant they would say I only need to comply with B-

MEMBER SCHULTZ: Legally that's what it would say.

MEMBER STETKAR: That's what they would say.

MEMBER SCHULTZ: There is no regulatory trigger point that overrules the B-

CHAIRMAN BROWN: Yes, unless somebody can find one. I'm just talking from a technology B- if you look at the level of detail specified in that ABWR, and that's only based on discussions we've already B-

MEMBER STETKAR: Where I'm getting to is DAC cuts both ways. DAC was established to allow applicants a lot of flexibility without specifying much detail in the certified design. Okay, that's fine. That helps the applicant. On the other hand, when you finally build a new plant ought they not be required to comply with our current state of knowledge regarding the way you ought to finalize that design?

That's the other side of that. Had they come in with a lot of details in that certified design I wouldn't be saying this. I'd say yes, indeed, they had a real design that provided extensive detail that you could review and was reviewed, wasn't pushed off to inspections after the plant was built. And, indeed, in that sense design B- you know, licensing finality would apply. But they didn't, they chose to not provide the detail. And now when they actually design and build the thing, ought they not to comply with our current knowledge of how things ought to work?

I just raise it up. Again, I'm not an attorney. I'm a poor technical guy.

MS. ZHANG: I think it is B-

MEMBER STETKAR: That's enough. I, you knowB-

MS. ZHANG: B- kind of bound by the legalistic portions of it.

CONSULTANT HECHT: Is the answer that the NRC shouldn't do a standard design approval without a more specific definition of the technology B-

MEMBER STETKAR: That's where Charlie has been trying to point people. And I think for some of the newer it's like the DSRS. But we are in a limbo situation.

CHAIRMAN BROWN: AP1000 we ended up with C-- they finally provided a functional diagram as well as more clarity on the communications, more clarity on watchdog timers in terms of the corruption of the voting CPUs. And the same thing has proceeded on the APWRs to some extent where, you know, we've headed down that path.

MEMBER STETKAR: Well, APWRs at least B- APWR will need to meet 2009.

CHAIRMAN BROWN: Yes, I understand that, but we've still been talking B- we've been going down that B-

MEMBER STETKAR: We're talking specifically about ABWR, System 80 Plus, if we're ever going to build any of those. In some sense, AP-600, if we're ever going to build any of those, ESPWR which is also heavily DAC. And then in principle future implementation of AP-1000, although that's a B- I'll admit the AP-1000 is a real gray area.

CHAIRMAN BROWN: But we did get some B-

MEMBER STETKAR: We did B-

CHAIRMAN BROWN: In our area we got definitions of B-

MEMBER STETKAR: Design certification on the AP-1000s had more detail than the others. And

they're building them now.

CHAIRMAN BROWN: And the STP, the ABWR applications for STP had much more B-

MEMBER STETKAR: Yes.

CHAIRMAN BROWN: B- detail in it.

MEMBER STETKAR: But that was STP's ABWR, not B-

CHAIRMAN BROWN: Not the old one.

MEMBER STETKAR: Not the old one.

CHAIRMAN BROWN: Yes.

MS. ZHANG: We understand.

MEMBER STETKAR: Okay.

CHAIRMAN BROWN: Should we roll on here?

MR. STATTEL: I think these are very good points, and certainly not something that we're addressing within the incorporate by reference rule. However, I mean, I think philosophically it's a larger issue that has to do with the design certification process.

MEMBER STETKAR: In some sense, but digital I&C, and digital I&C DAC, in particular, has been an anomaly throughout the whole process. I mean, it B- you know, so saying is it globally applicable to the design certification process, in principle, perhaps. But, in particular, digital I&C DAC would be B- the lack of

specificity of the design information, at least for a number of those certified designs at the design certification and COL stage is unique.

MEMBER SCHULTZ: And if you think about it, why is it unique? It's because the designer said well, the technology is changing so much in that particular field, I can't provide you the specifications at this point in time.

MEMBER STETKAR: Right.

MEMBER SCHULTZ: We'll do that later.

MEMBER STETKAR: Yes.

MEMBER SCHULTZ: Well, doesn't that impose upon them the expectation that they ought to be following the now current standards associated with application and design?

MEMBER STETKAR: Or the standards that are current at least when you build the first one.

MEMBER SCHULTZ: Exactly, yes. I think it's a whole B-

MEMBER STETKAR: The reference COL, in effect, is what I'm talking about.

CHAIRMAN BROWN: Well, the first answers we got on AP-1000 were along that line.

MR. STATTEL: Yes.

CHAIRMAN BROWN: Changing so fast, which is

just baloney. You can define these architectures without the technology being involved just like putting your belt and suspenders on. Anyway, we ought to B- I've been given permission to move on.

(Laughter.)

MEMBER STETKAR: By B-

CHAIRMAN BROWN: By my Staff.

MEMBER STETKAR: By your lowlife Staff.

(Laughter.)

MR. STATTEL: Next we'll discuss some of the criteria that are established in the rule for using the new standard. The table on this slide provides some examples of I&C system modifications to aid in the determination of applicability of the new standard. This table can be found on page 28 of the proposed rule document that you have.

CHAIRMAN BROWN: Now, is this B- let me ask you one question on this, Rich, the way you B- if I go back. This is the paragraph B- this is number 3, isn't it, the modifications B-

MS. ZHANG: Yes.

CHAIRMAN BROWN: B- and replacements?

MR. STATTEL: Yes.

CHAIRMAN BROWN: Effectively for existing plants. Well, it applies to existing plants. If an

existing plant changes, they come in to -B use Watts Bar, for instance, if they didn't do their thing identical where they're just rebuilding old transistors B- I'm kidding a little bit, but from the old days B-

MR. STATTEL: It's not quite as farfetched as you might think.

CHAIRMAN BROWN: No, I know, based on the meeting we had it was kind of interesting.

MR. STATTEL: Yes.

CHAIRMAN BROWN: Essentially, replicating the old design, the Eagle Field 21 design, whatever. But if they make any changes that fall into this category, then they have to follow the new rule. So, that's B- I wanted to make sure I understood. This is not B- just not a new reactor type, this is old B- this is existing plant B-

MR. STATTEL: Well, we don't specify. However B-

CHAIRMAN BROWN: And you don't say one way or the other, but it's so generic that it seemed to me it applied to either one.

MR. STATTEL: That's correct. And that was the intent so, I mean, I really can't speak to what the design details were in an older design certification,

right, that's just now going into implementation. However, if they are changing that design, if they're deviating from that design, they're doing an amendment to their license, and they would have B- they would be subject to the criteria that we have established in this rule.

CHAIRMAN BROWN: Yes.

MR. STATTEL: And, basically, the criteria were based on what was changed in the standard and how - what safety improvements those brought to the table. So, again, if they're going from an analog to a digital technology, for example, then yes, there are new criteria that would need to be addressed.

CHAIRMAN BROWN: But you had a list of examples in the, whatever, Statements of Consideration which B-

MR. STATTEL: Right. Now, this table provides several examples. I have a couple I can talk to, if you would like, or I can move on.

CHAIRMAN BROWN: No, we can move on.

MR. STATTEL: Okay, that's fine.

MS. ZHANG: But I think, you know, where it - you know, this is B- it's not just, you know, they come in for a license amendment request. It's if they make the modification, you know, what are under 50.59

or whatever, like process. It's if they make that change.

MR. STATTEL: That's correct.

CHAIRMAN BROWN: It doesn't have to be an LAR.

MS. ZHANG: Yes.

MR. STATTEL: Right.

CHAIRMAN BROWN: Yes, that's what B-

MR. STATTEL: That is true. Yes, thanks for pointing that out.

CHAIRMAN BROWN: Okay, thank you.

MR. STATTEL: And then there are clearly cases where changes or improvements are being made to the designs at the plants, and they're not hitting this directional, so they're simply replacing components, they're not changing technology, they're not introducing any of the uncertainties that would be addressed by these new standards. So, in those cases which are the top three in this table we simply allow them to maintain their existing licensing basis. So, if they're a 2.7.9 plant, they can maintain that basis for the upgraded system. Okay?

All right. So, this slide lists the clauses that would add conditions and several new requirements for the use of IEEE 603-2009. What I'm going to do next

is we're going to go and discuss each of these clauses individually. And in the rule parlance here, it's 50.55a(h) Clause (4) through (9) are the additional conditions that are being imposed. And these did not exist in the old rule.

Okay. The first one is (a)(4), or (h)(4). This amplifies the system integrity requirements of IEEE 603, Section 5.5. This new clause would require that in order to assure the integrity and reliable operation of the safety system, safety functions shall be designed to operate in a predictable and repeatable manner. And I'll also refer back to the definitions we discussed earlier. Those are defined terms.

Predictable and repeatable operation of system requires that the results of translating input signals to output signals are determined through known relationships among controlled system states and required responses to those states. It also requires that a given set of input signals produces the same output signals for the full range of applicable conditions defined in the system's design basis.

Predictable and repeatable systems do not provide the capability for unscheduled, event-based interrupts or operator-based system interrupts to meet system safety requirements. Systems that operate in a

predictable and repeatable manner should not be designed with the capability for unscheduled event-based disruptions, or operator-based system functions that would inhibit or prevent the system from meeting its safety requirements.

Any analysis used to demonstrate predictability and repeatability characteristics should be based on the analysis of system characteristics, as opposed to a probabilistic analysis. Okay? So, this is the new condition that's being imposed. Any questions on that?

CHAIRMAN BROWN: Yes, just B- maybe it's a nuance, but I have no problem with the words you all stated. This is, obviously, an attempt B- not an attempt, a pretty good attempt, pretty good definition of trying to make sure that you have a fundamentally, I'll use the word "deterministic," but it's known from beginning to end. The way I look at it, it's from input signal to control actuation, control device actuation. Those words to me have more meaning than "known relationship among the control system states and required responses to those states for which a given" B- that almost sounds like a Ph.D. thesis abstract.

MR. STATTEL: Well, I will say this. There was a lot of discussion B-

CHAIRMAN BROWN: I can imagine.

MR. STATTEL: B- behind this. And a lot of our discussion revolved around different means, different ways to accomplish this. So, an example is the use of watchdog timers to basically assure that you achieve deterministic performance, or you're able to detect failures that would affect system performance.

What we settled on was these words that I just mentioned here. And really, it's just a question of those are a means to accomplish what's in the regulation, not the regulations themselves. Because as soon as we start becoming prescriptive and talking about specific things like watchdog timers B-

CHAIRMAN BROWN: I'm not asking B-

MR. STATTEL: B- the applicability becomes less generic.

CHAIRMAN BROWN: I understand that.

MR. STATTEL: And it becomes very problematic from a regulation B-

CHAIRMAN BROWN: I got that. I would not have looked at using watchdog timers in this particular deterministic B- where you're trying to define what that means.

MR. STATTEL: It's just one example.

CHAIRMAN BROWN: That doesn't obviate the

need for the real purpose of watchdog timers, is to insure you don't lose all the voters at once based on corrupt data transmission. This is needed, and I agree with the addition that you all have done, except I would have suggested that you be a little bit more crisp, like after you finished about known input, say for example, processing of data from input to control device actuation, as a little parenthetical after that just so you have an example, what do we mean by inputs and outputs, from where to where, so it's not so abstract as to be not very well defined. Because the critical nature of a deterministic system that's predictable and repeatable is input to control device actuation. That's how it B- and that's not specific, that's kind of a generic architectural type need. So that would have been my suggestion. It may well be, but not right now.

MR. STATTEL: Okay.

CHAIRMAN BROWN: That's just my thought process.

MR. STATTEL: In a lot of cases when we're hammering out this language we had a lot of discussion about specific examples. Inevitably, the discussions go there. Generally, we don't like to include the examples in the rule language.

CHAIRMAN BROWN: Well, I would B-

MR. STATTEL: I mean, I think there are some rare exemptions to that B-

CHAIRMAN BROWN: I would have suggested putting it in the Reg Guide.

MR. STATTEL: Right. But for the Reg Guidance, that's certainly B-

CHAIRMAN BROWN: Yes. I was not going to suggest putting it in the rule language. I would B- in this case, I would have caved.

(Laughter.)

CHAIRMAN BROWN: And agreed to putting it in the Reg Guide. I'm getting soft in my old age. Okay. That was just my only comment on this. Other than that, I don't disagree with those.

MR. STATTEL: Okay, very good. Next, we're going to get into the area of independence. This new clause has several new requirements, and I'm going to allow Deanna Zhang to present this section. And, of course, there are a lot of different aspects to the independence. And without further ado, I'll turn it over to Deanna.

MS. ZHANG: So, thank you, Rich. And, again, my name is Deanna Zhang. I'll be discussing the independence portion of the proposed draft rule in which I'll describe the new conditions imposed by the

proposed rule to amplify the independence requirements of Section 5.6 of IEEE Standard 603-2009.

So, proposed paragraph 50.55a(h)(5) provides several new requirements to the existing independence criteria in IEEE Standard 603-2009. The main concept for these requirements is to insure that the protection system and other safety systems include provisions to protect against identified hazards.

Section 5.6.1 of IEEE Standard 603-2009 states that redundant portions of a safety system provide a B-

CHAIRMAN BROWN: Before you get into that, can I B- this is an editorial question. When you all listed these as "i" and stuff in the Reg Guide, you listed them as 1, 2, 3, and 4. And in the Considerations part you listed them as i, ii, iii, and so on. Is that B-

MR. WATERMAN: That will have to be cleared up.

CHAIRMAN BROWN: Okay. I just wanted to make sure I had B- because I was going by the rule and wanted to make sure we had consistency.

MS. ZHANG: Yes, when I cite these, these are what's in the rule, not what's in the Reg Guide, so numbering-wise, just to clarify.

MR. WATERMAN: Yes, the Reg Guide has to be brought up B-

MS. ZHANG: Yes, with the rule.

CHAIRMAN BROWN: Okay. That takes care of my editorial comment.

MS. ZHANG: Thanks. So, again, you know, I'm going to go over what's actually specified in the standard and then what conditions we're imposing in addition to what's specified in the standard. So, just first I'll read what's in the standard just so people can know.

IEEE Standard 603-2009 states that, "Redundant portions of a safety system provided for a safety function shall be independent of and physically separated from each other to the degree necessary to retain the capability of accomplishing the safety function during and following any design-basis event requiring that safety function."

As you can see, the IEEE language uses the words "degree necessary," so we'd like to amplify what that means by the following condition. So, the first part of the proposed Paragraph 50.55a(h)(5) amplifies this section of 603-2009 to clarify the analysis necessary to support the criteria in the standard.

Specifically, this condition requires

that the safety system architecture incorporate independence between redundant portions of a safety system B-

CHAIRMAN BROWN: Deanna, you make B- you said the safety system architecture incorporate. You left out the word "must."

MS. ZHANG: Yes.

CHAIRMAN BROWN: Now, I bring this up intentionally. I notice it's "must" in the rule, not "shall."

MS. ZHANG: It's "must" because this is, again, where OGC B- we were using the word "shall," and they said legally you must use the word "must."

CHAIRMAN BROWN: Why? This is a rule.

MS. ZHANG: We're not too clear on why that was the case. Did you remember, Mike? There was specific language, they told us we couldn't use "shall" here, we have to use "must."

CHAIRMAN BROWN: I mean, when are we using OGC to set our technical standards as opposed to the classic legal words that are used that say this is a requirement, is "shall" in almost every legalistic document I've ever seen. "Must" is like saying "should," which is mush.

MS. ZHANG: We were told that "must" in

legal sense in the rule language means "shall".

CHAIRMAN BROWN: Then why not use "shall?" Where is that defined?

MR. THORP: We've overused it. It's considered a settling by the folks in OGC.

MS. ZHANG: That's what we were told legally.

MR. THORP: Yes.

MEMBER STETKAR: Which clause are you specifically referring to?

MS. ZHANG: (h)(5).

CHAIRMAN BROWN: It's whatever, (5)(i).

MR. THORP: That the safety system architecture must incorporate independence between redundant B-

CHAIRMAN BROWN: No, no, the independence between redundant portions B- oh, I'm sorry, John, you're right. I'm giving the second sentence. Says "must incorporate." Let's go on, I guess.

MEMBER BLEY: I think so. I mean, that's a legal thing, not our's. But "must" is not "mush." "Must" says if you don't do it, you're in violation.

CHAIRMAN BROWN: I used to get hammered, okay, between B-

MEMBER BLEY: You're in a different

organization that didn't go to court. Thank God we didn't go to court with our B-

(Simultaneous speech.)

CHAIRMAN BROWN: That's the way it was.

MEMBER BLEY: And that's the way it is in standards.

CHAIRMAN BROWN: But it's not here. All right. Let's go ahead.

MEMBER BLEY: This isn't the standard.

CHAIRMAN BROWN: This is the rule.

MS. ZHANG: Yes. We take it as a "shall," and that's what's been told to B-

MR. STATTEL: We treat it as a "shall."

MS. ZHANG: Yes, we treat it as a "shall."

MR. THORP: So, if there is any confusion later when we get into the public comment period or there's interactions opportunities with the public, I think that could be made clear in our discussions.

CHAIRMAN BROWN: Well, why don't you put it in the Reg Guide, "must" means "shall."

(Laughter.)

CHAIRMAN BROWN: I'm looking for any B- okay, let's go ahead to finish your B- I'm sorry to interrupt you, but it was a B-

MR. WATERMAN: In the glossary.

MS. ZHANG: So, in addition to must, you know, incorporate independence, we also imposed that the independence and safety system architecture must be analyzed to address safety system internal and external hazards, the extent of interconnectivity between redundant portions of safety systems, and the impact of failures or degradations in one portion of a safety system on the ability of a redundant safety system portion to accomplish its safety function.

CHAIRMAN BROWN: Okay. Let me focus on this first one. When I'm communicating from a particular division to a software-based voting unit and every other division, including my own, the same argument, not argument, the same discussion we've had in all the I&C upgrades or anything else. You have the potential for locking up all of them with corrupt data. The potential is there, so it's a significant vulnerability on the independence side.

These words are more general relative to general degradations or failures, not a literally communication forced potential lock up of a CPU function. Whether the CPU is a separate CPU as opposed to a processing one, or whether the algorithm for free voting is in the processing but a separate sub-routine somewhere, it makes no difference.

MS. ZHANG: We would consider B-

CHAIRMAN BROWN: Okay. You still need some type of watchdog on that which says if I lock up, I issue a trip. And I took these words and looked through the Reg Guide and other places, and I could not find a connection.

Now, if I go look and see what we're doing on the DSRS application for mPower, we're being very specific relative to how this potential problem is going to be resolved in the design. So, that's B- again, the DSRS is a standard B- it's a review spec. It's not a rule, but if it's not B- if we don't cover the vulnerabilities in a little bit more clear manner from a software B- this is where the hangup is. Look at the old systems, electrical isolation, clean. You've got an independent system. Software-based systems we don't have that armor if we don't have something that specifically addresses that lockup component of a voting unit B-

MR. STATTEL: There are two parts to this. One, what you described we would consider to be a hazard, and a hazard that would be required under the new rule to be analyzed and addressed, either mitigated or eliminated during the design and development process of that system.

Additionally, to address the area of not having sufficient information at the time of a design certification, for example, we have another clause that we're going to get to, that Deanna will get to shortly, as well. So, both of these apply, both of these clauses apply. But what you describe, we would consider that to be a hazard, and we would expect the hazard analysis and the resolution of that hazard analysis to be a part of meeting the regulations, that would be required for meeting the regulation.

CHAIRMAN BROWN: Okay, but B-

MR. STATTEL: And that may involve invoking a watchdog timer function, or some other method to insure that the hazard is addressed, the potential for that.

CHAIRMAN BROWN: We brought this up with some of the other design, in the design projects that we've looked at. The design agents were adamant that this will never happen. We have algorithms and cyclic redundancy checks, and all these good things, dual port RAM, and all dual port RAM is it's a transformer for software data. That's all it is. You put garbage in, you get garbage out. Okay? It's just a transformer for data stream.

MR. STATTEL: Right.

CHAIRMAN BROWN: And if you put corrupt data in, you'll get corrupt data out because it B- there's no intelligence in the thing. So, their argument is we B- our software is beautiful, our algorithms are foolproof, and we don't need to do that. And I just B- it just boggles my mind that we would be so complacent as to not define that unique hazard in some way, shape, or form somewhere for these folks to B-

MR. STATTEL: That's not to say that we would accept that. I'm not here to discuss the B- any specific example, but I would think in a case like what you're describing the Staff would have the prerogative to not accept that.

CHAIRMAN BROWN: The first meeting we had on this where we brought it up, the Staff said didn't need to.

MR. WATERMAN: But isn't that where diversity and defense-in-depth analysis comes in? No? Because you assume a common cause failure, who cares what it is?

CHAIRMAN BROWN: Is that a common cause failure?

MR. WATERMAN: Well, all channels B-

CHAIRMAN BROWN: It's a piece of software that nobody B- I mean, so how do you look at that? How

do you insure that that particular B- my concern, okay, fundamentally is how do we establish an armor-plate, and armor build similar to the electrical isolation independence requirement we had for analog systems? It doesn't exist, and every time we talk about it, there's push-back in terms B- and that was specific. It was incorporated by reference in the rule, so you could literally tell somebody, you could point to it, how you have something to point to, whether you B- you don't have to call it a watchdog timer. You can call it anything, a monitoring method to determine whether it has done such and such which will execute, you know, and tell that division is now not operational, and execute a trip out to the appropriate other two out of four breaker configurations and what have you. I mean, it just B- how do you translate from what we had before and eliminate where we had no vulnerability to where now we've introduced that vulnerability, and now we don't have anything to take its place.

MR. STATTEL: In the context of this proposed rule we are calling that a hazard analysis and we've imposed a new requirement for an applicant to perform that activity, and to assess that activity against the risks that would be potentially introduced with the new system. So, this is B- all we're doing is

explaining how we are addressing this within the context of this rule. Now, this discussion is not over because we will talk specifically about the new reactors applicability of this.

CHAIRMAN BROWN: But that's new reactors. What about back B- what about your, number 3.

MR. STATTEL: We'll talk about all of that.

CHAIRMAN BROWN: That's one of my other questions. When you get to the new reactors you've got all these list of things just for new reactors. Why doesn't that apply under number 3 with modifications to existing plants? And they don't the way you've written the rule.

MS. ZHANG: There's a couple of items, you know, as Rich has said, you know, we do B- you know, in adding this aspect of internal and external hazards we do expect that more detail be paid B- more attention will be paid on the types of failures different systems, different technologies could experience, and for a systematic analysis of how B- you know, what can manifest and how those should be mitigated.

In addition to that, we did add additional criteria which I'll go over later of what can be transmitted across redundant divisions. We wanted there to be some limitation and that not B- you know,

you don't just have inter-divisional communication for no good justification. So, I can go into that a little bit later.

MEMBER STETKAR: Let me try something sort of peripherally. You mentioned several times you expect that issue to be addressed in the hazard analysis. Where is the Staff in terms of its progress on developing guidance for the performance of said hazard analysis? The last briefing we had was it's infantile, let me put it that way, and it's not at all clear to me what the hazard analysis really is. So, where is the guidance that's available for someone to perform a hazard analysis of an integrated digital instrumentation and control system? And where has that guidance been piloted in terms of a real application for a real digital instrumentation and control system? Do we have that?

MR. STATTEL: There is existing guidance on performance of hazards analysis activities within IEEE standards, IEEE 1012 identifies the requirement to perform hazards analysis activities.

MEMBER STETKAR: Requirement, I understand that. I'm not saying B-

MR. STATTEL: There is also B-

MEMBER STETKAR: This is go out and make

world peace.

MR. STATTEL: Right, I understand. And we also B- there is also some guidance in the Standard Review Plan, guidance for the reviewers to basically look for hazards analysis activities. Additionally, there is an Annex in IEEE 7-4.3.2. The 7-4.3.2 Working Group is currently working on rewriting that Annex and updating that. I was talking with Warren earlier today about the status of that. We have a meeting this summer and we hope that standard would be going out for ballot I believe next year.

Additionally, Sushil might want to speak to the Research activities. Do you have any update on that, Sushil?

MR. BIRLA: This is Sushil Birla from the U.S. Nuclear Regulatory Research Office. I want to backtrack a little bit. The general concept of hazard analysis is not new, as Rich said. There's been guidance many years ago, there's a NUREG that applicants have referenced in the past. Hazard analysis take various forms, FTAs and FMEAs have been around for a long time, and I need not inform the members that the FTA guidance started with the NRC.

MEMBER STETKAR: I will interject there that I've read something just recently that says hazard

analysis, fault tree analysis and failure modes and effects analysis are inadequate to evaluate the hazards for digital systems and, therefore, a hazards analysis should be performed. So, the guidance for fault tree analysis and FMEAs apparently is useless because I have to perform a hazards analysis. So, I'm asking okay, if that's true, please tell me how to perform a hazards analysis, because I'd really like to do one.

MR. BIRLA: Yes. So, the delta is when there are interconnections and feedback paths, particularly introduced when you have complex software in the system. So, that's where the current practice, and standards, and guidance in FTA and FMEA have not been adequate. However, even in FTAs and FMEAs very competent practitioners have adapted them to such conditions. FTA adapted to systems that have feedback paths in them. FMEA applied it to functional FMEA level where you say no, it's not the 100 component light failure mode, it's the failure of a function, and then going down from there.

So, what I'm trying to say is that there is a backdrop. It's not a total vacuum. Now, Rich, with that backdrop coming to the specific question you asked, yes, Research is producing a recent Information Letter, an advanced copy draft is out in the public

domain. It's been out there since we reviewed it with the ACRS last September, a month before last September. Early content from that has been taken into the mPower DSRS Appendix A.

MEMBER STETKAR: We'll talk about that tomorrow.

MR. BIRLA: Okay.

MEMBER STETKAR: The point is, I believe, that we now have a rule that will apparently rely on the performance of a hazard analysis to provide reviewers assurance that many of these issues have been addressed. And fine, I'm okay with that personally, as long as I understand what that hazard analysis is, that there is guidance so there's no ambiguity about well, if the right person does the right kind of fault tree analysis, I might get the kind of answer that I might kind of like, but maybe tomorrow if you look at it you might not like that answer.

And second of all, if the guidance is developed we have ample experience with guidance that has been developed for evaluating complex phenomena in systems that has not been piloted in a real world application, that when people go out to use said guidance, it doesn't work. So, it's not simply somebody putting down some basic principles of hazard analysis,

ought to look at all hazards, and ought to evaluate them. It's how you do it, and have we actually tested it, because we're relying on that concept in our regulations.

MR. STATTEL: We recognize that there's no universal definition for hazards analysis or a universal understanding of how the concept is applied. And that's why we're doing the Research activities and that's why we're updating the Annex in the IEEE Standard. But, I mean, it's an evolving field. We recognize that.

We also acknowledge that FMEAs in and of themselves are not necessarily providing the adequate assurance that we need. That's not to say they're bad. Right? A lot of good things come out of the FMEAs. In large part, they're a good way of identifying what the hazards of the system are, but they may not be complete.

MEMBER STETKAR: Except that they're typically applied in the context of a single failure analysis.

MR. STATTEL: Right, exactly.

MEMBER STETKAR: And in these areas we're not talking about single failures. We're talking about threats and vulnerabilities at an integrated system perspective, and that's much broader than what FMEAs

typically address.

MR. STATTEL: Correct.

MR. BIRLA: This is B-

MR. STATTEL: Sushil, did you want to say something?

MR. BIRLA: Mr. Chairman, may I address you with a little follow-up?

CHAIRMAN BROWN: Oh, you can go on.

MR. BIRLA: Okay. This is Sushil Birla again. The results of such an analysis not only depend upon the technique and you, members of the Subcommittee, have pointed that out to us on the 19th of September when you had a review of the recent presentations. It also depends upon the competence and the quality of the information. And it's not just true with new kinds of hazard analysis, this has been true with FTAs also, and FMEAs, too.

FTAs have been around for over 30 years. Even today if you take two different practitioners on the same system and ask them to do fault trees, they cannot come up with the same results. So, we cannot overlook the need for competence that has been true in this kind of an analysis for 30 years, and will continue to be true.

MR. SANTOS: This is Dan Santos, NRO. I just

want to add that what we're doing here is augmenting B- you know, Charlie mentioned we had the barrier, and we're augmenting the current words to the degree necessary. But we're not solely relying on the concept of HA. In the case of existing reactors, they have completed design with an established safety baseline, and in the case of new reactors, that's why we felt we needed additional criteria in the absence of that. So, that's what Deanna is going to cover. So, while it's important to continue to work on HA, and we're doing that. We're trying to pilot it with the mPower design, there's ongoing research. We're not solely relying on just HA to be the anchor for this section on independence. So, I just want to mention that.

CHAIRMAN BROWN: I'll make one other comment based on B- let me backtrack. I'm just very laser focused here, to quote some famous words.

The electric B- the thing that could compromise the old analog systems was the introduction of electrical signal into redundant systems. It could damage it. If it was going to damage one, it could have damaged all if it was fed to all of them. That's what the isolation came from.

If I look at now software-based, and you're specific now, you've very specific as to what you do

to combat that. It must be isolated, electrically independent. Now you've got software-based systems where you are dependent upon sending serial communication data to multiple locations, whether it be trip data, whether it be monitoring, instrument data, or whatever it happens to be. The critical component that affects you from a safety standpoint is the trip data. So, when you embed the trip data inside a message anything can happen. Some of them bad, some of them good. That is the only vehicle, that's the only place for the most part where that communication occurs, and we are not specific as to how to combat that on the downstream side; whereas, we were on the analog side. And that's the point of my discussions, and my other discussions in past meetings.

So, in my opinion, okay, the right place to take action for this to provide an equivalent functionality B- functionality is the wrong word. Protection, the way we did in analog systems with isolation, is to insure that those voting units or processing, whatever form they take, algorithms within the same trip unit process or what have you, that if they for whatever reason lock up, you've got to tell something that I'm not working any more. Even if they're sending a reset signal back that tells it to start over

again, which is not unreasonable, that's what I would do, but in these systems, the way they're designed it's five to ten minutes before they're reset and walk through their reboot cycles.

When we faced this in the program that I came out of, our requirement was that it had to reboot, the first requirement was 250 milliseconds, a quarter of a second, a blink of an eye, just like when you turned an analog system back and took the power off, put it back on, the needles flash up, you see just about where you are. You may not be in spec as much, but you know about where you are. That was the requirement.

Now, because we've got more complex functions it's now three or four seconds, but not five to ten minutes. That one platform in one of the designs was a five, depending on how they rebooted and what cycles they had to go through, there was a 10 minute, it could be as short as five. So, that's not a good B- you can't rely on that if you are depending upon that as a safety, from a safety function.

MR. STATTEL: Respectfully speaking, I think the scenario you described, we are addressing this in Condition 3 that you see up on the slide here, so the impact of that failure B- I mean, that's a failure or a condition that would affect the ability

of the safety system to perform its safety function when required.

You can see in this criteria, you know, we do evaluate that, so if there is some situation where there's a timed response that would affect the ability of the safety function to maintain the plant safe, this right here is designed to address that.

MS. ZHANG: I just don't think we were as specific, you know, on the type of failure and the type of mitigation.

MR. STATTEL: And we couldn't be in the area of regulation. We didn't want to presume to be too specific B-

CHAIRMAN BROWN: Well, I mean, I have a little bit of disagreement. If I go to the section right above where this rule is that you all B- in this whole presentation, there's a whole section on welds. Well, they're so specific that it's ridiculous. You know, the notch has got to be a certain size with a certain depth, the sample has to have at least a minimum of 10 flaws that have this size and this length. I mean, so there's specificity, you know, the whole thing about there's no specificity in the rules is not right. Okay? It's there where people want to use it to their B- you know, to make sure they got the right answers.

MEMBER STETKAR: But in defense of the Staff, we have ample evidence of putting too much detail in rules requires many rule changes, or an awful lot of arguments about why we can't change the rule because we had too much detail in it.

CHAIRMAN BROWN: Well, I understand that, and I'm not looking for overly explicit detail. I just think right now we do not have the same comparable open circuit barrier to independence in the software-based systems that we do in these others.

And, quite frankly, the whole issue of lockup of B- was not even considered six years ago when I got here. It wasn't even considered. Everybody said huh, why would we even look at that? So, when you say it's going to be captured under the failures or degradation in one course of the system, while I agree with the B- I have no problem with the words you all put in. I just think we've missed the boat. That's me. So, anyway, we can move on now. All right?

And, by the way, don't take my comments as B- I'm not criticizing efforts here. That's not the point. The purpose of this was to have an interchange and discussion B-

MR. STATTEL: Understood.

CHAIRMAN BROWN: B- of what you're all

doing. Okay? So, I don't want anybody to think, you know, Brown is hammering me for some reason. I mean, this has been a good discussion.

MR. STATTEL: No, it continues to be so. Thank you.

CHAIRMAN BROWN: And that's the purpose of it, okay?

MR. STATTEL: Thank you.

MS. ZHANG: So, this next slide we talk about some of the additional criteria requirements that we impose for independence between safety systems and other systems, including non-safety systems. So, again, I'll go over what IEEE 603-2009 states, requires for independence between safety and other systems.

"The safety system shall be designed B- shall be such that credible failures in and consequential actions by other systems as documented in Clause 4," which is the designed basis clause. "Item H of the design basis shall" B-

CHAIRMAN BROWN: Deanna, I'm confused. Are we B- this is I(ii)?

MS. ZHANG: Yes.

MR. STATTEL: It's essentially the same clause but this applies to between safety and non-safety.

CHAIRMAN BROWN: Okay. Where were you reading?

MS. ZHANG: Oh, I was just reading what's in IEEE Standard 603.

CHAIRMAN BROWN: Oh, okay.

MS. ZHANG: Yes, just so that B-

CHAIRMAN BROWN: I was looking at the rule. I'm sorry.

MS. ZHANG: B- you know, when we go and we say B- we amplify this requirement B-

CHAIRMAN BROWN: I'm sorry.

MS. ZHANG: B- that we know what the requirement is in 603.

CHAIRMAN BROWN: Okay, thank you.

MS. ZHANG: "Shall not prevent the safety system from meeting the requirements of this standard." So, in Subsection 5.6.3, one of the subsections it states that, "Equipment that is not credited to perform a safety function but is connected to safety-related equipment shall be electrically isolated from the safety system, have digital communications independence and be classified as Non-Class IE." This is, as Rich had pointed out, this is different from previous versions of the standard.

So, the second part of the proposed

paragraph 50.55a(h)(5) provides requirements for applicants to address independence between safety systems and other systems, including non-safety systems. As stated previously, the standard specifically required beta communications independence. To insure that independence requirements remain technology neutral, the proposed rule specifies that independence must exist between safety systems and other systems for all signal technologies and not just digital signals.

In addition, similar to the additional conditions imposed for independence among redundant portions of safety systems, independence between safety systems and other systems must be analyzed to address hazards posed by other systems on the safety system, the extent of interconnectivity between safety systems and other systems, and impact of failures or degradations in other systems on the ability of the safety systems to accomplish the safety function. Any questions on this one?

CONSULTANT HECHT: Deanna, I'm sorry. In both this and the previous one you have the extent of interconnectivity between the safety systems and the other systems. Can you give me an example of excessive interconnectivity and the example of acceptable

interconnectivity? Could you clarify that for me?

MS. ZHANG: Well, we're not looking at, you know, what's an acceptable level of connectivity and what's not. What we're looking at in general is, is the interconnectivity necessary, and for what purpose? There needs to be a justification for the connection, and that's what we're looking for. So, it's not an absolute this is acceptable, and this is not acceptable, but we're looking for the analysis and justification as far as why this connection is needed.

CONSULTANT HECHT: Can you say when the NRC Staff would say that a passing of data between divisions is not acceptable?

MS. ZHANG: Well, we later added criteria to what is acceptable communication between redundant portions of safety systems and between safety and other systems. You know, we don't B- when we write rules we don't tend to say B-

MR. STATTEL: There are conditions that we have defined where the communication is not acceptable. We're going to get to that.

CHAIRMAN BROWN: Next page. Not next page of the slides, but next page of the rule.

MS. ZHANG: So, Section 5.6.4 of IEEE Standard 603-2009 provides detailed criteria on the

application of independence requirements specified in Section5.6 of the standard. This section references IEEE Standard 384-2008 for detailed criteria for the independence of Class 1 equipment and associated circuits. It also references IEEE Standard 7-4.3.2-2009 for criteria for separation and isolation of the data processing functions of interconnected computers.

As Charlie had pointed out, if you look at the 2003 version of IEEE Standard 7-4.3.2, it doesn't really get into a lot of detail how to address data communications independence, and what's acceptable, or how do you process data. So, we decided to add some additional conditions to amplify that requirement.

Conditions in the other standards are not really incorporated, directly incorporated by reference. You know, we decided we needed additional criteria, so we added four specific criterion, including independence of signal processing, fault detection criteria, current reactor independence criteria, and new reactor independence criteria.

So, the first detailed criterion would clarify that the signal processing portion of the safety system should provide the capability to insure that degradation or failures of signals exchanged among

redundant safety divisions, or between safety systems and other systems do not propagate in a manner that results in impairment of the safety function being performed by the safety system. Again, I think that speaks to B-

CHAIRMAN BROWN: That's not the rule. Where are you reading from right now?

MS. ZHANG: This is Clause 50.55a(h)(5)(iii).

CHAIRMAN BROWN: (iii)?

MS. ZHANG: Yes, if you look down, it's (a). It says, "Signals to redundant safety divisions and signals from a non" B-

CHAIRMAN BROWN: You used the word "propagate," and I couldn't B-

MS. ZHANG: Oh, that B- I'm speaking from the Statements of Consideration actually goes to B-

CHAIRMAN BROWN: Oh, okay. So, you're really talking B- okay, Statements of Consideration.

MS. ZHANG: Yes, Consideration, where we expand on what does that really mean.

CHAIRMAN BROWN: Okay.

MS. ZHANG: What's the intent of that.

CHAIRMAN BROWN: Okay.

MS. ZHANG: So, I think that really does

speak to, Charlie, your point about propagation of failures, you know, what needs to be considered. So, you know, examples may be, you know, safety function processors should not directly exchange information with processors outside the B- its division. You should look at correct B- properly addressed messages, et cetera.

So, the second detailed criterion would clarify that safety systems should be designed with provisions for detecting and mitigating the effects of signal faults or failures received from outside the safety division. Redundant divisions of safety systems should have the capability of tolerating such faults or failures in a manner that does not degrade the ability of the safety division to perform its safety function. So, communication faults such as corrupt messages and repeated messages should all be identified as a possible failure, and they should all be mitigated.

So, the third detailed criterion would clarify the independence requirements of IEEE Standard 603-2009 for communications between redundant portions of safety systems and between safety and non-safety systems in currently operating nuclear power plant designs.

Specifically, it would clarify that

communications or signals received by a safety system from outside the division or system should be limited to only those that support the accomplishment of safety functions or otherwise benefit safety. And I'll go into our definition of a safety benefit.

We defined it as a justification for adding safety system functionality that is not necessary to accomplish a safety function, but that contributes to safety such as increasing safety system availability, or increasing the safety of a mechanical, nuclear, or electrical system design.

MEMBER STETKAR: Deanna, let me B- while we get quiet in the back there. Let me ask you a question because I'm really hung up on this. This is for current reactors, so if I think of plants like Oconee or Diablo Canyon, or any one that backfits their analog less than efficient control system to a more integrated digital system, does this now prevent me from having what I call safety neutral communications that might enhance reactor operations or operator information?

So, for example, if I have safety-related displays that the operators can also pull up information about non-safety systems on those displays, does this prevent me from doing that, because that non-safety information does not directly enhance

safety in the context that you're providing here?

MS. ZHANG: You know, as we had stated, you know, we defined what safety benefit is, but it's B-

MEMBER STETKAR: Well, that's what I'm trying to understand.

MS. ZHANG: It was an example. It was an example of those things that I listed. Now, human factors could be a area where there is a safety benefit, and that would be the justification that B-

MEMBER STETKAR: I've actually seen Staff asking questions of applicants saying you cannot B- basically, RAIs beating applicants out of doing that because that's a non-safety signal and it does not directly enhance a safety function. We've commented on that B-

(Simultaneous speech.)

MR. STATTEL: Let me speak a little bit on this. As we were developing B-

MEMBER STETKAR: If we're going to do that, we ought not to do that.

MR. STATTEL: Right. As we were developing this particular condition, we did have a lot of discussion about some of the benefits that were being proposed. Right? And the arguments that licensees had been making, HFE is one of those arguments.

MEMBER STETKAR: That is the big one.

MR. STATTEL: And we did not, we specifically did not want to preclude those. What we do want is we want for a license to identify what those are and make a case for why these benefits outweigh the risk and hazards that might be imposed by incorporating them.

MEMBER STETKAR: And I understand that, but I'd suggest then in the regulatory guidance at least for reviewers, Staff reviewers, you amplify on that a bit. Because, as I said, we have in a different context run into that situation where Staff reviewers have read this type of language very, very, very literally in terms B-

MR. STATTEL: Now, another version that was actually considered was to basically disallow any communications if it was not specifically required to perform the safety function. Now, that's very problematic because there are actually regulatory requirements that have nothing to do with performing the safety function that really need to be performed in these types of situations.

So, for example, to alarm on actuation, or alarm on bypass, clearly that doesn't have to happen for the safety function to keep the plant safe, but it

is a regulatory requirement. So, we didn't want to paint ourselves in a corner by creating a regulatory requirement that no one would be able to truly meet. So, what we did was B- and we can certainly consider guidance, additional guidance in this area, but what we did is we provided the definition for a safety benefit. Right?

MEMBER STETKAR: But that B- kind of elaborating on that in guidance I think would help, because B-

MEMBER BLEY: And even beyond that, this language just is unsettling, and I think could be really cause problems. It's not just regulatory, there's a lot of operational needs in the plant that require information, but it's nothing to B-

MR. STATTEL: But those needs have a safety benefit, with it's HFE, or B-

MEMBER BLEY: But the way this is written, you know, 50 years ago, 40, 50 I think, regulators looked at the scram function, and we looked at the scram breakers and we thought, oh, the scram has to be completely passive. So, we did the breaker so that they wouldn't get all the signals that'll allow them to trip and force them to trip, and we did that for many years despite people pointing out the problems until one of

the plants had several cases of scram breakers failing because they didn't get the signal by design they really need to be driven shut. This could spawn that kind of thing, and it's just B-

MR. THORP: You are making some very good observations. I think we ought to B- there was a lot of discussion that occurred in this area, and I think it's worthwhile insuring that our guidance doesn't inhibit applicants or licensees from being willing and proceeding forward with uses of technology like this to insure that they can do their jobs in the control room simply because we're asking them to explain it. I think we need to ask B-

MEMBER BLEY: For more clarity and exactly what we're looking for here.

(Simultaneous speech.)

MR. THORP: B- prohibitive.

MEMBER STETKAR: We do have experience of review B- remember we're not going to be here, you know, 10 years in the future. Reviewers in the Staff are going to be interpreting these words in many cases very, very, very literally. We can only do this because our interpretation of these specific words us X.

MR. THORP: We appreciate the observations.

MR. STATTEL: And where we've had

challenges is where an applicant claims that there's a safety benefit, and there's a disagreement between the Staff and the applicant of what that safety benefit is. Our initiative here is really trying to better define what that safety benefit is.

MEMBER STETKAR: Well, this doesn't.

MR. STATTEL: And really force them, force the applicants to make that case, because in the absence of this B-

MEMBER STETKAR: Having the B- you know, I'm not arguing with forcing, if you want to use that word, having an applicant make a case that justifies communications between safety and non-safety systems, or non-safety and safety systems. Not at all arguing that. What I am concerned about is NRC Staff reviewers who will point to language in a rule without any additional clarifying review guidance to basically disallow things because of a very, very, very strict interpretation of what they feel a safety benefit is.

MR. STATTEL: And what "must" means.

MEMBER STETKAR: And what "must" means.

MR. STATTEL: And I also don't want to make light of what the potential benefits are, because they are real, they are tangible, we have seen them, they are HFE benefits, there are benefits in surveillance,

in monitoring of system performance. Quite frankly, the analog systems were pretty good, but in a lot of cases we relied on surveillance like channel check-type things to identify degraded performance, in which case we're basically allowing the system to operate for 24 hours at a time with the assumption that, you know, it's going to be performing. Whereas, the new technology really does introduce some benefits in those areas, particularly in the areas of prognostics, diagnostics, self-checking features.

Now, those have to be weighed. I mean, whenever you introduce those new technologies, we acknowledge that there could be potential hazards associated with introducing that. That has to be weighed, and that was our intent here B-

CHAIRMAN BROWN: I'm going to be a little contrary here. I mean, this is (c) for current reactors, is what B-

MR. STATTEL: Correct.

CHAIRMAN BROWN: B- you're talking about. And it's about the sharing of information between safety systems, redundant portions. That's what it says, "while sharing information among redundant portions of safety systems, and between safety systems." But you think about this between redundant

portions of safety systems.

MEMBER STETKAR: It says from outside the safety division, Charlie.

CHAIRMAN BROWN: It says, "While sharing the information among redundant portions of safety systems." It's right in the Reg Guide B-

MEMBER STETKAR: I'm sorry. That's a Reg Guide.

CHAIRMAN BROWN: The Statement of Considerations.

MEMBER STETKAR: The rule B-

CHAIRMAN BROWN: The rule just says "from outside the division during operation must support." But when you look at the Reg Guide, it has other delineations of information within it. Okay? So, all I'm trying B- the only point I'm trying to make is this sharing concept has got to be very carefully crafted because if somebody, which has been proposed, could come along and they'll say well, geez, I'd like to take all the sensor data that I've processed in each division, and I want to send that to the other divisions, and then we're going to evaluate that data to determine what the best data is. And then we're going to use all that common data to process itself up through each division. Some people think that's really a great

idea because it improves reliability by taking B- you know, throwing out the highest and the lowest, and averaging the two, and now that's the data that I'm going to send to something. You can come up with all kinds of schemes for evaluating the stuff. That's not a good idea. I don't think you all would buy in that, but yet it has been discussed before.

But yet, a maintenance B- a self-diagnostics within the division, that's B- you want to use these B- this technology to be able to do that. I mean, it's just B- really it's an improvement over what we had before to continue the self-diagnostics within the divisions. And if you send the results outside to the operator, nothing wrong with that as long as it's a one-way data transmission. It's just you've got to really be careful about how you bring other information from outside or within, or between safety and non-safety.

You all had an example somewhere about an anticipated trip, if you had a turbine trip you want to tell something is going on, and you want each division to know that the turbine is tripped; therefore you should be taking some action. That's a non-safety system. Well, that's the kind of information you want to come in. You've just got to do it the right way, and

I don't think B- even I wouldn't argue against doing that in spite of I'm so conservative with B- I might be viewed as saying that. I just want the enthusiasm for just throwing information all over these things to get carried away. That's all. And I felt this enthusiasm was building to the point of almost, I'm not going to use the terminology, but people were jumping up and down and waving flags.

MR. THORP: Well, in the end of the examination of the benefits to be achieved versus the risks and hazards posed B-

CHAIRMAN BROWN: Yes. I was willing to give the Staff, you know, some leeway to use their heads. Now, I don't know whether that's counter to the other points my colleagues are making or not, but is that counter to it? Okay. I just wanted to bring the temperature down a little bit in terms of the benefits of B-

MEMBER BLEY: I think your point of clarity is thinking B-

CHAIRMAN BROWN: Yes. I just B-

MR. STATTEL: I think we have to be very careful because you don't want to impose restrictions to address the hazards without consideration for throwing away the benefits that the technologies can

address.

(Simultaneous speech.)

MR. STATTEL: It works both ways, yes.

CHAIRMAN BROWN: There's risk to be weighed except for monitoring devices for the CPUs.

MS. ZHANG: I would like to move on to the new reactors criteria, if that's okay.

So, the forced detailed criterion would clarify independence requirements B-

CHAIRMAN BROWN: Well, before you go into all the details, why isn't this applicable to current reactors when they backfit and replace stuff?

MR. STATTEL: I'll answer that. The new reactors are licensed under Part 52, and in that process they are not required to provide design detail information at the time of the design certification. This is simply not the case for operating reactors. NRR requires design implementation details for evaluation prior to issuing license amendments for I&C safety systems. And even in the case of the 50.59s, we expect these evaluations to be completed by the applicants. It's NRR's practice to base the safety evaluation conclusions on complete safety system designs, including the implementation details.

CHAIRMAN BROWN: This is NRR?

MR. STATTEL: This is NRR, that's correct.

CHAIRMAN BROWN: Where is that, where are you reading that?

MR. STATTEL: This is within the Statements of Consideration.

CHAIRMAN BROWN: Okay. And is that reflected in the Reg Guide, as well?

MR. STATTEL: Yes. Yes, it is.

MR. WATERMAN: Hopefully. It's supposed to be.

MR. STATTEL: I think we took everything out of there.

CHAIRMAN BROWN: Well, I know. I almost did a B- I didn't do a word-by-word. I did a paragraph by paragraph back and forth.

MS. ZHANG: I think what you'll find in this Reg Guide, as well as the Statements of Consideration, it's a reasoning from the other side, why are we imposing this for a new reactor?

CHAIRMAN BROWN: Oh, I agree with what you all said and did.

MR. STATTEL: And what we recognize here is we recognize the fact that NRO is tasked with issuing a safety evaluation on a design certification when they don't have full design implementation details. And

that's a challenge, and we recognize that challenge. And because of that challenge we felt that it was necessary to impose these additional restrictions onto those designs as we evaluate them.

Now, for operating plants imposing those restrictions could have an adverse effect of limiting the useful or basically dismissing the benefits that could be provided by having communications between these systems.

In actuality, you know, I mean, if a design was proposed for an operating plant that met all of these restrictions, we would consider that perfectly acceptable.

CHAIRMAN BROWN: But why B-

MR. STATTEL: But it's not the only way.

CHAIRMAN BROWN: Why would these hamper them?

MR. STATTEL: Excuse me?

CHAIRMAN BROWN: Why would these Items (i) through (iv), why would these B- you made the comment that this would restrict the current reactors, or would not allow them to achieve the benefits. And I had a really hard time seeing how not utilizing these on the current reactor reviews would restrict them or inhibit their ability to achieve some benefits. I mean, the

benefits are the benefits, and these are just how you do some of those things. I mean, the current reactors there must be one way. Why would I want two-way communications between safety and non-safety systems?

MR. STATTEL: Because there may be benefits that are provided by those, and if ample controls are put in place B-

CHAIRMAN BROWN: If they're good B- if they're not good for new reactors, why are they good for the old reactors?

MR. STATTEL: Well, the thing is with the new reactor, we don't have the detailed design, so there isn't a way, there isn't a mechanism for us to evaluate those designs. For the operating reactors, we have the complete design detail, so if they put measures in place to address the hazards that would be imposed by such a design, then we have the obligation to evaluate that. Now, I'm not saying that we would accept all of them, we don't. However, we have the obligation to evaluate those and consider the benefits that are provided.

And as we stated in the previous slide, those benefits need to be quantified. They need to provide a safety benefit, they need to be quantified, and they need to be justified. Now, with the operating reactors there's really no way to come to a safety

conclusion without having the details of the design. So, that's the difference, it's really a process-related difference. And that's what B-

MR. THORP: Availability of information difference.

MR. STATTEL: Right. And really that's B- that's really the Statements of Consideration, that's what was considered for the development of these criterion.

CONSULTANT HECHT: Would you argue that if you are modifying a system in an old reactor you're left with the same uncertainty that you would have for a new reactor?

MR. STATTEL: Yes, and in that case using the Part 50 process, or license amendment process, such a modification would require an evaluation of the detailed design. It's not like we're approving a design certification where we have future ITAAC or DAC items that would need to be addressed. So, we're not issuing a safety evaluation without being able to confirm the implementation of the design. And that's the difference. And it's true B-

(Simultaneous speech.)

MR. STATTEL: And it's true really for any operating plant, you know. We evaluate the design, the

completed and implemented design for its merits, not just based on the higher level architecture. Right? So, we have the details of that design. I'm not saying it's easier. I mean, if an applicant chooses to basically cut the cords and not implement any communications and follow the types of restrictions we see on this slide here, we're not saying that's not acceptable. That could be a perfectly acceptable way to address regulation for an operating plant that's doing a modification. But we're also not willing to say that this is the only way that would be acceptable.

And we're not saying that for new reactors either, because as we'll talk about later there is an alternative process that's built into this. So, even on a new reactor design they can take exception or use an alternative to what's being put into this regulation, if the benefits B- if the safety benefits are there and can be justified.

CONSULTANT HECHT: Can I also ask a question with respect to III, other than data communications? Is that really what you wanted to say, because I could argue that an analog signal is also data. And I could argue B-

CHAIRMAN BROWN: Well, the way that they define data communications B-

MR. STATTEL: That's why we added definitions for those terms.

CONSULTANT HECHT: I see.

CHAIRMAN BROWN: It very clearly talks about the software specific format, headers, footers.

CONSULTANT HECHT: I see.

CHAIRMAN BROWN: All that type of stuff, so that's defined.

MS. ZHANG: Yes.

MR. STATTEL: Well, what I suggest is let's let Deanna go through the description on each one of these terms.

CONSULTANT HECHT: I'm sorry, okay.

MR. STATTEL: And then we can have further discussion.

CHAIRMAN BROWN: That's okay.

MS. ZHANG: So, again, for the fourth criterion we really wanted to clarify the independence requirements for new reactors. And I'll kind of go over not only what this means, but also why we decided to do this for new reactors.

So, for new reactor designs, "must insure that data communications from safety systems to non-safety systems is in one direction while the safety system division or channels in operation, and this must

be accomplished using hardware means. In addition, the transfer of signals between redundant portions of safety systems should only be accomplished when the signal transferred is required for the performance of a safety function."

So, this proposed condition limits the implementation of communications between redundant portions of safety systems and between safety and non-safety systems to really limit the failure modes and unexpected behaviors associated with communication, while preserving some of the benefits of digital technology and allowing functionality that improve reliability and availability. So, if we want to, as Charlie had mentioned, if we want to see comparison of sensor signals, you know, a way to do that would be to send that sensor signal to a non-safety system to analyze it and maybe provide an annunciation to the operators if there is a need to do so. But we felt that as a general principle that safety systems, for safety systems that hazard should be eliminated whenever possible during the design stage. Otherwise, it should be mitigated if it cannot be eliminated.

Communications that use programmable means to enforce independence in itself can introduce design B- failure modes associated with design

errors. And by implementing communications independence in the hardware architecture design the potential for the propagation of design errors is minimized.

The Staff recognizes that there are certain cases where safety division would need to receive a signal from outside its own division. For example, safety systems may need to receive signals from non-safety systems to support diversity, such as a signal from the diverse actuation system to actuate a safety component.

Also, the safety signal may need to receive a signal from non-safety systems to accomplish an anticipatory trip function such as a reactor trip upon a turbine trip. In such cases, these signals shall be transmitted using hardwired connections without the use of data communications. And just to clarify, we defined data communications as a method of transmitting and receiving information in which the information is encoded in a specific format, including header, data content, and end of message using software.

CONSULTANT HECHT: Right. So, having said that, if I use an FPTA and have the end of message and the header and the footer, is that not data communications?

MS. ZHANG: So as, again, this is B-

CONSULTANT HECHT: I'm using an FPGA to send the message rather than software. Is that B-

MS. ZHANG: It's still considered data communication.

CONSULTANT HECHT: Is that data communications?

MS. ZHANG: Yes.

CONSULTANT HECHT: Why?

MR. WATERMAN: You've got a header, you've got data and you've got a footer.

CONSULTANT HECHT: Well, it says in software.

MR. JUNG: Yes, we consider FPGA B-

MS. ZHANG: We've defined what software means in the context of this rule.

CONSULTANT HECHT: Software means an FPGA?

MS. ZHANG: Yes.

CONSULTANT HECHT: Okay. That's included in these definitions?

MS. ZHANG: I B-

MR. STATTEL: We have a definition for data communication.

CHAIRMAN BROWN: It's not in the glossary.

MEMBER STETKAR: Not in the glossary, but

it appears sporadically throughout the B-

MS. ZHANG: In the Statements of Consideration we discuss what we consider software, software logic. We've given examples of such in the Statements of Consideration.

MR. SANTOS: This is Don Santos. We in the NRC are pretty much treating all programmable logic the same whether it comes from traditional software, FPGA, programmable, HDL devices, and we have been revising guidance documents, Reg Guides to be very encompassed and explicit. If there's the opportunity in the SOCs to expand on that, I think that's a good comment. But the intention is to be all-inclusive when it comes to programmable logic.

CONSULTANT HECHT: Well, I would suggest that in a regulation, unless the software is defined in the context of that regulation to include any programmable device, that you might want to add that terminology there, because I could see a way around that.

MR. SANTOS: Good comment.

MR. WATERMAN: Well, you know, we've been through discussions with industry on FPGAs. That goes all the way back to when the same argument was levied on firmware, where we had the argument well, firmware

is not software so it doesn't apply. It does apply, because software isn't just what's loaded on the chip. It's the whole development cycle, everything from laying out requirements, design implementation, testing, the whole gamut encompasses what is software. Just because it's loaded onto an FPGA with place and route, doesn't mean it's any different from software that's loaded into a microprocessor. It's still an arrangement of logic that flows from one point to the next for the purpose of accomplishing a function.

CONSULTANT HECHT: I would argue that software is generally considered instructions that are loaded into a microprocessor.

MR. WATERMAN: I'm sure you would, and the industry has argued that, and we've gone over this over, and over, and over again. And I've had FPGA experts argue with me on and on, and then they turn right around and talk about their log logic as code. And it's like code, isn't that software?

MR. THORP: Yes, we've had this conversation multiple times with industry. They understand our position on this, that we do consider FPGAs to be included in software.

MR. WATERMAN: I get really spun up on this about B-

(Laughter.)

MEMBER STETKAR: You're usually pretty mild.

MR. THORP: This has been around some specific incidents, as well, so interactions with industry, so we're pretty firm on that. We're not soft on that.

CONSULTANT HECHT: You don't feel that there's a need to add a B-

MR. THORP: No, I think you have a reasonable suggestion that we ought to consider in the Statements of Consideration or guidance so that we're very clear on what we consider to be included within software. I appreciate your comment.

CONSULTANT HECHT: Okay. But with respect to headers and footers, if we are sending a series of bits perhaps we're doing in a B- you know, just these in a shift register. Is there not a need to have some kind of parity bit, some kind of means of validity of that bit, of that information?

MR. THORP: I don't have an answer.

CONSULTANT HECHT: I'm just relating to the headers and footers.

MS. ZHANG: Well, when it comes to details on implementing data communication we have other

criteria, other guidance.

MR. THORP: I mean, that could be a means of meeting the requirement.

MS. ZHANG: Yes, but we do have guidance in that specific area about the communications, particularly in the ISG-04, we do have specifications about checking headers and footers, and how to insure that they're valid. But in this B- in the context of this rule we did not go into that level of detail.

CONSULTANT HECHT: Well, if I send a message from one division to another, and I send it with some kind of parity check, is that better or worse than without, because this really seems to imply that I should just send the data without any additional, how shall I say it, headers or footers.

MS. ZHANG: I don't B- I think in the data communications itself, the headers and the footers would accomplish B- accompany the data. We're talking about in this case what is the data, what is the data used for? The data should be used for accomplishing a safety function.

MR. STATTEL: I think what you need to understand is that these communication paths, they're not relied upon for completion of -- the successful completion of the safety function. Right? So, the

communication link can be broken, the data can be corrupt. It doesn't matter because the direction of this data flow is away from the safety B- where the safety function is being performed. So, no matter what your postulate as far as a failure mode or an error in the communications, the safety function is maintained. That's what's in B-

CONSULTANT HECHT: Well, it says from non-safety systems, so are you saying, for example, dealing with the reactor trip example that we were dealing with B- the turbine trip example that we were dealing with earlier.

MR. STATTEL: Okay.

CONSULTANT HECHT: And we just sent one bit, turbine has tripped.

MS. ZHANG: Yes.

CONSULTANT HECHT: And we might mean that the turbine hasn't tripped. You know, that's the parity. That could be significant.

MS. ZHANG: I think in this case we're looking at the reliability of the communication that it does not affect safety system function, or the safety function itself. If the turbine has tripped and if it were to send a signal that it hasn't tripped, I think it should be dealt with with other means, or if their

design they propose a B- that they need data communications to indicate that for a good reason, then we'll look at it on a case by case basis.

MR. STATTEL: But for those cases we do specify that they don't use data communications for those signals. Those are basically a relay contact closure input to the system. That's what's mandatory.

MR. THORP: The case in which you're referring to a non-safety signal providing a signal that would create an actuation such as a trip, like turbine loss of load trip signal.

CHAIRMAN BROWN: That's a by staple signal as opposed to a B-

MR. THORP: Versus data communications.

CHAIRMAN BROWN: As opposed to a serial, or a data communication link.

MR. THORP: Right.

MS. ZHANG: Yes. Well, there's other parts of 603 that would say that has to be electrically isolated from the safety system.

CHAIRMAN BROWN: All right, keep moving.

MS. ZHANG: So, the last independence condition posed for new reactors addresses the alternative approach. Specifically, this condition specifies that any potential communication pathways

introduced by an alternative approach to Section 50.55a(h) between a digital safety system and other systems, such as non-safety systems, must be identified. And we'll go into a little bit more detail of what this means in the next slide.

MEMBER STETKAR: Deanna, well, get through this one.

MS. ZHANG: Okay. So, Paragraph (h)(5)(iv) addresses the potential communication pathways introduced by an alternative approach to Paragraph (h) between a digital safety system and another system. This paragraph would require applicants of design certifications, standard design approvals, or manufacturing licenses to identify all direct and indirect communication pathways to safety systems to facilitate the identification of interdependencies and failure modes in the alternative design.

For example, if a non-safety system is connected to a safety system either directly or indirectly through another non-safety system to provide information on the status of the plant, then this connection would need to be identified to insure that failure modes and unexpected behaviors associated with this connection is addressed. A direct pathway would be a direct serial connection from a non-safety

system in this case and an indirect pathway would be a non-safety system that is not directly connected to the safety system but may be networked with other systems, such as a maintenance work station that connects to the safety system. Any questions on this?

MEMBER STETKAR: Go back to the previous slide. In the interest of time, I want to make sure you checked off the last box. Number 3, there is B- I hung up on something when I read the rule, and the thing I hung up on is it literally says, "while the safety system is in operation only if the received signal supports diversity and automatic anticipatory reactor trip functions." I read that as it only applies to ATWS mitigation. Now, when I read B- because it says "and," diversity and. When I read the Reg Guide, the Reg Guide interprets that paragraph in a logical or context, because the Reg Guide says well, I may have communications from non-safety to enhance diversity and defense-in-depth or ESFAS functions, for example.

MS. ZHANG: Yes, thank you for pointing that out. I think that's an editorial B-

MEMBER STETKAR: Well, but people hang up on those words.

MS. ZHANG: Yes. So, we'll make sure B-

MEMBER STETKAR: So, check that because

when I read the Reg Guide, the Reg Guide interprets it in the way that I had hoped it would be.

MS. ZHANG: Yes.

MEMBER STETKAR: But this could be read as specifically limiting this to ATWS mitigation.

MS. ZHANG: Yes. Thank you for pointing that out to us.

CHAIRMAN BROWN: All right. I think that finishes the independence.

MS. ZHANG: Yes, thank you.

CHAIRMAN BROWN: Well, at least it concludes the current discussion on independence. We will go ahead and take a break for lunch now, and we will return and continue at B- let's see, how much time did we allocate? Okay, 1:25. All right. Recess.

(Whereupon, the proceedings went off the record at 12:25 p.m., and went back on the record at 1:35 p.m.)

CHAIRMAN BROWN: The meeting is now back in order. We can proceed. Rich, I think we're due to start on the diversity and defense-in-depth part, whoever is going to do that.

MR. STATTEL: Yes, our next area of discussion is in diversity and defense-in-depth. So, for this rule, for this proposed rule four new clauses

are being proposed for regulation to address the potential for software or logic implementation common cause failure.

Now, first of all I'll say that the Working Group decided not to be very creative with the development of this criteria because the criteria was already proposed to us in the form of SECY paper 93-087.

CHAIRMAN BROWN: Is this an NRC Working Group, are you talking about the IEEE B-

MR. STATTEL: NRC Working Group.

CHAIRMAN BROWN: Okay.

MR. STATTEL: Right. So, basically, the criteria that you'll see in here, they won't be foreign to you, there's nothing new being proposed here. They were derived directly from the Staff Requirements Memorandum, so there's nothing really new here. This would be the first time that these criteria appear in regulation.

Okay. The first of these criteria would be added to amplify the requirements stated in IEEE 603-2009, Section 5.16. Now, you might recall earlier today we discussed this clause in IEEE. The IEEE standard simply refers over to the 7-4.3.2 Standard, and we took exception to that. So, instead of basically following that rabbit trail, we're providing specific

guidance for D3, and we're adding that into the incorporate by reference, or in 50.55a(h). And these are the criteria that we're putting in.

Okay. The use of digital technology in safety systems has led to concerns that errors could lead to common cause failures that might disable one or more safety functions in redundant divisions of a safety system. Errors can be introduced into a system at any stage of the development life cycle, so that's really the pretense for this. These are words that are right out of the Staff Requirements Memorandum. And you can see the first clause here. I don't B- I wasn't planning on reading it, but if you have any comments on that.

CHAIRMAN BROWN: The B- you're talking about the clause in the rule?

MR. STATTEL: This is in the rule. The language you see on the slide here is what is in the rule.

CHAIRMAN BROWN: Oh, okay. I've got to flip my page. Where am I? Oh, I'm really ahead of you. Okay.

MR. STATTEL: Okay?

CHAIRMAN BROWN: Thank you.

MR. STATTEL: Now, the Working Group really didn't see any need to come up with any clarifying

language for this other than what's in the Statements of Consideration. And the reason for that is because we're already evaluating D3 analysis, and we're using the guidance that exists in Branch Technical Position 7-19. So, that B- so, we basically defer to Branch Technical Position 7-19 as B- for evaluation of D3 criteria.

CHAIRMAN BROWN: Before you leave that, yes, I see those words. And is this supposed to B- these aren't the same. Is that 1991? No, that's not, this is new.

MR. STATTEL: This is new. This is not in the standard. Remember, the standard provides a reference to IEEE 7-4.3.2, so we don't agree with that. So, instead of that we are adding language right out of the B-

CHAIRMAN BROWN: Oh, okay, now you've got the rule words. Okay, I'm sorry. I'm switching between papers.

MR. STATTEL: This is the rule words, or the proposed rule words.

CHAIRMAN BROWN: Got it.

MR. STATTEL: That's what's being added in.

CHAIRMAN BROWN: Okay. How did you punt on 7-4.3.2 again?

MR. STATTEL: Well B-

CHAIRMAN BROWN: You didn't accept that. I know you said you all deferred away from that.

MR. STATTEL: Right. So, as I explained earlier, the IEEE Standard, the Working Group instead of adding criteria for diversity, defense-in-depth, they provided a reference over to IEEE 7-4.3.2. Right?

CHAIRMAN BROWN: The IEEE Standard.

MR. STATTEL: Right, which we don't consider to be adequate for addressing diversity. And, therefore, we added this language, these four clauses that are on this slide and the next three directly into the IBR Rule, into 50.55a(h).

CHAIRMAN BROWN: Okay. Well, where do you say that you don't accept 7-4.3.2 for that?

MR. STATTEL: That's explained in the Statements of Consideration.

CHAIRMAN BROWN: So, that's the location. I thought I B- I remembered reading it somewhere, but I B-

MR. STATTEL: That's right.

CHAIRMAN BROWN: Okay.

MR. STATTEL: Okay. So, if you look at this clause that I have up on the screen here, are there any questions about this? I'm sure you've seen it before.

MR. WATERMAN: Rich?

MR. STATTEL: Yes.

MR. WATERMAN: Looking at what I captured in the Reg Guide out of there, we don't reference 7-4.3.2 in the discussion for common cause failures. Maybe it's B-

MR. STATTEL: That's right, because we're not endorsing that.

MR. WATERMAN: But we don't say it's not acceptable either. We just don't reference it.

MR. STATTEL: Did we mention that in the C-- I thought we mentioned that in the SOCs.

MR. WATERMAN: Well, I'm looking at the SOCs.

CHAIRMAN BROWN: And I just looked at the Statement of Consideration and I don't find the word 7-4.3.2. I don't see that in there. I'm looking at page 39.

MR. STATTEL: It's a statement of a negative. We're not endorsing it. We're adding additional rule language B-

MR. WATERMAN: We just didn't reference 7-4.3.2 in that discussion, Charlie. We simply B-

MS. ZHANG: Yes, but all B- in addition in Reg Guide 1.152 we did specifically say we do not

endorse any of these Annexes.

CHAIRMAN BROWN: In 1.152?

MR. WATERMAN: It's the Reg Guide.

MR. THORP: It endorses IEEE Standard 7-4.3.2.

CHAIRMAN BROWN: Okay. So, there's another Reg Guide that says you all don't recognize that.

MS. ZHANG: Yes.

MR. THORP: It endorses the 7-4.3.2, but it does not endorse the associated Annexes.

MS. ZHANG: Yes, we B- it was a specific statement.

CHAIRMAN BROWN: Oh, I do remember it didn't endorse the Annex. Okay. All right. I remember that now. Thank you. The point being is you don't have to positively push away from these in here, even though you've endorsed IBR, Incorporated by Reference, 603-2009.

MR. THORP: Any references that 603 makes to other standards are not in themselves considered to be incorporated by reference, just 603 is incorporated by reference. So, this is additional rulemaking beyond the 603.

MS. ZHANG: So, the reference in 603 when it references 7-4.3.2 or any other reference standards,

when we do a rulemaking it's not B- it was not explicitly saying we incorporate by reference.

CHAIRMAN BROWN: Is that stated somewhere else in the rulemaking?

MS. ZHANG: It's part of the rulemaking process.

MR. THORP: We definitely added that in. I can't point directly to it right now, but B-

CHAIRMAN BROWN: I'm just trying to understand the process here, that's all.

MR. THORP: Yes.

CHAIRMAN BROWN: How do we get it B-

MR. THORP: Dan, if you want to check that out, because it's a basic tenet of the rulemaking that you B- if you incorporate a standard by reference, it's B- the references or the standards referrals to other standards are not in themselves also incorporated by reference into law.

MR. DOYLE: This is Dan Doyle. I'm the Rulemaking Project Manager, so what John Thorp said is correct, but we obviously need to be very clear and specific on what we intend. So, when we incorporate something by reference, that document is what's incorporated and has the same status as a regulation that we directly publish ourselves. But it gets

confusing if that standard references or says other things are required, then it could raise a question of well, is that a requirement or not? And if so, if that's what we meant, then maybe that other document that's referenced should be incorporated by reference, at the very least we should explain how we're interpreting it or provide some other guidance.

MEMBER BLEY: I thought B-

MR. DOYLE: So, if we need to be more clear then we do need to take a look at that.

MEMBER BLEY: I seem to remember in other cases where standards are incorporated by reference the actual rule says but not the associated B-

CHAIRMAN BROWN: References.

MEMBER BLEY: B- references or appendices, or whatever. I thought that was right in the rule, usually.

MR. THORP: I was thinking that we were going to include that in the Statements of Consideration.

MR. DOYLE: No, I think it is actually in the rule. I mean, I can B-

MEMBER BLEY: It's your usual practice. Right?

MR. THORP: Yes, I mean, that was the advice

we got from OGC on that. It hadn't been done in the previous rule.

MEMBER BLEY: Oh, okay. That was just adding the B-

MR. STATTEL: I believe we added it B-

CHAIRMAN BROWN: List of things to check.

MR. THORP: I'm going to ask Doyle to check that out. It might already be there in an earlier page or at the beginning of the IBR B-

MR. DOYLE: Yes, I'll check.

MR. THORP: Okay.

MR. STATTEL: All right. Just another note. The Working Group when we were discussing the matter of diversity and defense-in-depth, we felt kind of constrained here because this is an area where we have some direction from the Commission in the form of the SRM, the Requirements Memorandum document, and any deviation that we would take from that would really constitute a change in policy. And that would have required an alteration in the direction from the Commission. So, in light of that we really chose to stick very stringently to the language that was in that SRM, and that's why you see these clauses put forth in this way.

Now, at the same time, as I mentioned

before, I have initiated a new rulemaking effort for a specific diversity rule, and in that effort I think it would be appropriate, or more appropriate to consider alternatives to what is in the Staff Requirements Memorandum as that if it goes forward.

Okay. The second criteria, postulated common cause failures shall be evaluated to demonstrate adequate diversity within the safety system for each design-basis event in the Accident Analysis section of the Safety Analysis Report. This introduces the concept of best estimate methods, and that's further clarified in the Branch Technical Position 7-19.

The applicant or a licensee shall demonstrate adequate diversity within the design for each of the events evaluated in the Accident Analysis for that plant. Okay?

The third criteria, if a postulated common cause failure could disable a safety function, diverse means unlikely to be subject to the same common cause failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety related system if the system is of sufficient quality to perform the necessary function under the associated event conditions. And, again, we have clarification on

this requirement in Branch Technical Position 7-10, as well.

And the final criteria on diversity is a set of displays and controls located in the main control room shall be provided for a manual system level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in (h)(4)(a), and (h)(4)(c). Okay?

Okay. The next area of discussion is a couple of notes on system maintenance and testing. Okay. The first change is 50.55a(h)(7), and this is to correct an error in the IEEE Standard 603-2009 in Section 6.5.1, which is titled, "Checking the Operational Availability."

This corrects an incorrect reference to an operating bypass instead of a maintenance bypass criteria which is what was intended. In our research, we discovered that the error was introduced during the conversion of IEEE Standard 279 to the 603-1991 Standard.

This is the actual text. You can see in IEEE 279 they refer to maintenance, but they don't provide a numerical reference to a specific clause. When that

was converted to IEEE 603, they basically separated out the clause and it should be 6.7, and it is in fact 6.6. So, we're basically providing that correction. 6.6 is operational bypass, and 6.7 is maintenance bypass criteria.

Okay, 50.55a(h)(8) clarifies the requirements with regard to the ability of a safety system to continue to perform its safety functions while redundant portions are in maintenance bypass mode. This is the criteria we previously discussed back on slide 14 of the presentation, and this was the one where we're referring back to the 1991 clause instead of the 2009 clause. And this is the actual rule language that's being proposed to accomplish that.

Okay. And the final proposed clause pertains B-

CHAIRMAN BROWN: Rich, before you go on, I guess I'm B- a little clarification. The 7 is titled, "Retaining Safety Function Capability During Maintenance Bypass," and then you've got the next 8 as Maintenance Bypass follow 6.7.

MR. WATERMAN: That should be during operating bypass on 7, Charlie. No, it's a correction. You pointed it out correctly, but I think it's really during B- retain safety during operating bypass is what

it should be titled.

MR. STATTEL: No, 6.7 is the maintenance bypass criteria.

CHAIRMAN BROWN: Well, I'm just looking at the Statements of Consideration. It says proposed (h)(7) would be added to 6.5.1, capability and testing; yet, it's talking about retaining safety capability. I mean, what I'm trying to figure out, and I didn't get it from reading when I read the maintenance bypass and the other, how are they different? Is there B-

MR. STATTEL: Oh, well, we can pull up the standard. We can discuss that. So, you're asking what the difference between the criteria for maintenance bypass versus operating bypass.

MR. THORP: Or is it the difference between the 1991 and the 2009?

CHAIRMAN BROWN: Retaining safety function capability during maintenance bypass. That's the title of 7. And that you're saying you're doing that because you are B- that's not the correction one. That's the next one. I guess I had a hard time figuring out what was the difference.

MR. STATTEL: I'm a little confused right now.

CHAIRMAN BROWN: 6.7.

MR. STATTEL: 6.7, yes. That's maintenance bypass criteria.

CHAIRMAN BROWN: And doesn't that include keeping the safety function when you're in B-

MR. STATTEL: Yes, it does.

MR. THORP: It's not in the title but its in the verbiage that's just below the title. Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass.

CHAIRMAN BROWN: Where are you reading from now?

MR. THORP: Yes, sir, from the 2009, IEEE 603-2009. So, the problem that B- and Rich described it for you earlier. The problem that we had with this B- the 2009 version was this "should" statement in that first paragraph, the second sentence, such that we prefer as the regulatory agency here to have the 1991 version of IEEE 603 maintenance bypass requirement to be what's in the rule. While we're incorporating 2009 by reference, what we're saying is we're taking a little exception to this particular paragraph and we're saying we want the 1991 to be met.

CHAIRMAN BROWN: So you like the word "shall" vice "should."

MR. THORP: Right. That's correct.

CHAIRMAN BROWN: Which we argued about before in terms of "must."

MR. THORP: We like "must", also.

(Laughter.)

CHAIRMAN BROWN: Okay. You wanted to go back to the B-

MR. STATTEL: Yes, sir. I understand it's a little confusing, but these are really just administrative or B-

CHAIRMAN BROWN: Well, I kind of gathered that except for "should" and "shall," which you seem to B-

MR. STATTEL: Okay.

CHAIRMAN BROWN: All right.

MR. STATTEL: Yes. Okay, so then the final requirement or condition that we're imposing has to do with documentation. Okay. So, 50.55a(h)(0) or (9) establishes requirements for maintaining documentation to support compliance with (h)(2) through (h)(8) requirements. So, all of these new conditions basically this statement creates an additional requirement that documentation, analysis, design details that demonstrate compliance with those previous criteria we discussed, that they be developed

and maintained by the applicant.

CHAIRMAN BROWN: One other observation, and maybe it'll come up when Mike talks, but in the rule you've got a (7) and in the Statements of Consideration you've got an (h)(7), (h)(8), and (h)(9), and in the Reg Guide, there's an (h)(7) and (h)(8).

MR. WATERMAN: Yes, I already caught that, Charlie, and that will be fixed.

CHAIRMAN BROWN: Okay. We're missing one section of some B-

MR. WATERMAN: Actually, two sections; 7 and 8 were combined at one time.

CHAIRMAN BROWN: Oh, and it didn't get split out?

MR. WATERMAN: And in the rule it's all one big section.

CHAIRMAN BROWN: Okay.

MR. WATERMAN: And that got carried over into the Reg Guide. And then when it got changed back to two separate sections, I thought I'm not going to keep chasing my tail here. When we get all the comments worked out I'll update the Reg Guide then. So, right now they're a little bit out of sync because if I keep changing things as we're changing those things B-

CHAIRMAN BROWN: All right. I'm happy,

you're just going to fix it.

MR. WATERMAN: Yes.

CHAIRMAN BROWN: Good.

MS. ANTONESCU: Configuration management.

CHAIRMAN BROWN: That's fine.

MR. STATTEL: Okay. The next area has to do with the alternatives clause that's included in the rule, in the proposed rule. This clause is not really changing. We are adding B- well, actually, the text has not changed from the existing rule. However, there's a unique aspect about this clause that I want to point out. Okay?

CHAIRMAN BROWN: Before you go on, to make sure I know where you're talking from.

MR. STATTEL: Okay.

CHAIRMAN BROWN: Where is this discussed in the Statement of Consideration? The only place I remember seeing B-

MR. STATTEL: Good question.

CHAIRMAN BROWN: B- is throughout the Statement of B- there were parts about the alternatives have to do such and such.

MR. STATTEL: I don't think it was discussed, and the reason is because we're not adding any new criteria, and we're not revising the existing

criteria. The reason I wanted to point this out, because I wanted to have a discussion on this, is because it is a unique aspect of this particular incorporate by reference rule, and it's important to understand what its implications are with regard to using alternative standards, or taking exceptions to the clauses that are located within this rule, within this proposed rule.

MS. ZHANG: So, there was a numbering change. It used to be 50.55a(8)(3).

MR. STATTEL: That's correct.

MS. ZHANG: In this proposed rule right now the numbering is at 50.55a(z), but the language itself except for a minor numbering change, I don't think there was one.

MR. STATTEL: I think it's all of (h), all of (h) is included in scope, so I don't think even that changed. I think it's exactly the same as what it was before.

So, normally when a licensee does not follow regulation an exception path or an exemption path must be taken to avoid a violation or enforcement action. The process for taking an exception or exemption from regulatory licensing requirements is covered by 10 CFR 50.11 and 50.12. And those are titled, "Exceptions and Exemptions From Licensing Requirements

and Specific Exemption."

However, what's unique about this clause here is when an applicant does not follow the requirements of 10 CFR 50.55a, they can use an alternative approach. Okay? And this is the clause, I just quoted it verbatim, so you can read exactly what the requirements of this clause are. There are cases, and we've seen several, where the applicant has proposed alternatives in the area of digital I&C.

So, for example, in a recent application they were installing a system that was developed to the requirements or the criteria of IEEE 603-1998 version instead of the 1991 version, so that is an alternative to the incorporate by reference standard. Okay?

Now, the existing regulation really doesn't provide any conditions or additional requirements other than it incorporates the standard into regulation. What's changing here is now we've added these conditions in (h)(2) through (9), and taking exception to those conditions falls in the same category, because as you can see the applicability, the second sentence of this clause proposed alternatives to the requirements of these paragraphs, including (h), or portions thereof may be used when authorized by the Director of Office of Nuclear Reactor Regulation or

NRO.

CHAIRMAN BROWN: So, you're giving them an out.

MR. STATTEL: Well, it's not an out. It requires that approval, but it's a different B- if it's a different set of criteria than what would be used had these criteria been incorporated into a separate rule, anything other than 50.55a. And that's what I want to point out.

CHAIRMAN BROWN: I missed the nuance.

MR. STATTEL: So, if the B- let's say, so we have the independence conditions that we've imposed here, that we're proposing.

CHAIRMAN BROWN: In (h).

MR. STATTEL: Now, let's say we incorporated them into 50., some new rule. Okay? And not 50.55a, so it's not in the IBR rule, the Incorporate by Reference Rule, it's a separate rule. If someone wanted to take exception to that they would have to go through the exemption process, which would be 50.11. Okay? Which has different criteria than what you see here on this one.

MEMBER BLEY: I don't remember them. Can you summarize roughly what the difference is?

MR. STATTEL: What's in 50.11? Do we have

a book around?

MEMBER BLEY: Are these more stringent or less?

MR. STATTEL: It is more stringent, and it requires special circumstances, I think is the terminology that's used.

CHAIRMAN BROWN: Is (z) more stringent?

MS. ZHANG: No, 11 and 12 is.

MR. THORP: 50.11 and 50.12 have more stringent requirements to do an exemption B-

MR. STATTEL: I mean, keep in mind the intent of 50.55a is not to develop new guidance or new regulatory criteria, it's to incorporate criteria that's in a standard into the regulation. So, the idea is if somebody uses a different standard than the one that's incorporated, then that would have to be evaluated, and it would have to go through this alternatives process.

But here we are today, what we're proposing is not only incorporating the standard, but adding conditions onto that. So, you know, we had discussions with OGC and the result was that if someone took B- basically, didn't want to do something that was in 50.55a(h), they could use this alternatives process in order to do something different. And that would have

to be evaluated and approved by the Director of whatever office is involved.

MR. THORP: I hesitate to read this to you.

CHAIRMAN BROWN: Okay, that's fine.

MR. THORP: It's just a lot of verbiage, Charlie.

CHAIRMAN BROWN: That's fine. I'm trying to get the gist of the difference, and I think I understand the difference between the incorporate by reference thought process of 50.55a, as opposed to if you had put it somewhere else and it has to follow some different process.

MR. THORP: Sort of an excerpt here, that the "Commission may upon application by an interested person or on its own initiative grant exemptions from the requirements of the regulations of this Part, Part 50, which are authorized by law, will not present an undue risk to the public health and safety, consistent with common defense and security. They will not consider granting an exemption unless special circumstances are present. Special circumstances are present whenever," and then they give a series of items, "application of the regulation conflicts with other rules or requirements of the Commission, the application of the regulation in this particular

circumstance would not serve the underlying purpose of the rule, compliance would result in undue hardship or other costs that are significantly in excess of those contemplated when the regulation was adopted," so there's a series of reasons for which they might grant an exemption. And it's B- I guess our subjective assessment of this is that it would, in essence, be more difficult for someone to go through that than to use an alternative standard for one that is being incorporated by reference.

CHAIRMAN BROWN: Well, I mean it's the words, Item 1 is where it says "acceptable level of quality and safety," could be almost interpreted to give the NRC open season to make sure that safety is very, very stringently adhered to. I know how to do that kind of stuff. Make it worse, in other words, make it so painful that they want to do it the other way. There's a lot of different B- that's a very open-ended B-

CONSULTANT HECHT: It can also be done the other way, too. Right?

CHAIRMAN BROWN: Oh, yes, it can be done the other way. It can be a significant reduction in safety and standards, depending on what you define as the level of quality.

MS. ZHANG: And we have used this, you know,

as Rich mentioned, in other places in the Office of New Reactors, there wasn't a proposed alternative to the independence requirements of 603-1991 submitted by Areva for their self-powered neutron detector design, in which there was not sufficient redundancy to provide the level of independence required.

Now, they are going through a level analysis from their safety analysis, a deeper level analysis to show that they can accommodate a worse case single failure that's undetected. So, you know, that was a lot of work on their part to demonstrate that it is an acceptable level of quality and safety. So, you know, that's a practical example that we've seen.

MR. THORP: I think our sense of it is that Staff certainly would not take this lightly. I mean, we would B-

CHAIRMAN BROWN: No, I'm not B- I wouldn't think you would.

MR. THORP: I didn't think you were saying that, but I just want to assure you that these proposed alternatives would certainly be considered very seriously, and would have to pass judgment.

CHAIRMAN BROWN: I guess my point is B- not point, my thought process is that if somebody proposes this, the Staff has to use a considerable amount of

thought process to insure that you meet these appropriate levels of safety and quality. I mean, it's like plowing new ground when you're doing that, and the only references you have are back to the standards that you use. And how do you then incrementally apply them to the new alternative they proposed?

MR. THORP: Not unprecedented, I think B-

CHAIRMAN BROWN: No, that's fine. Dennis, do you have any other comments on this?

MEMBER BLEY: No, I was just reading about this. No.

MR. STATTEL: Okay. What I would like to do next is turn the presentation over to Mike Waterman from the Office of Research. He's going to present basically the contents or the process for the draft Reg Guide, which is associated with this proposed rule.

(Off the record comments.)

CHAIRMAN BROWN: The way the agenda is written, Royce was going to be doing something at some point. Is that B-

MR. THORP: At the end of the B-

CHAIRMAN BROWN: Oh, that's at the end. We shifted.

MR. THORP: Right, we did. We felt like it would be more appropriate to have this be sort of a look

forward at what's going to be happening with the standard in the future.

CHAIRMAN BROWN: Okay. So, we're finished with the new reactors, and we're out through the B- all the rule stuff.

MR. THORP: That's correct. Now, we're looking at the draft Regulatory Guidance.

CHAIRMAN BROWN: Okay.

MR. STATTEL: Right, we did.

MR. WATERMAN: Okay. The Staff was requested to provide an informational briefing to the ACRS on several topics related to the 10 CFR 50.55a rulemaking effort. My name is Mike Waterman. I'm the Office of Nuclear Regulatory Research. I will be describing the draft of Reg Guide 1.153 which will be submitted for public comment at the same time as the proposed revision to 10 CFR 50.55a(h). Draft Reg Guide 1.153 provides guidance for meeting regulatory requirements in 10 CFR 50.55a(h).

CHAIRMAN BROWN: I'm sorry. I just looked at my notes. Can I backtrack for two seconds? Well, it will be more than two seconds.

MR. WATERMAN: Backtrack? Sure.

MR. THORP: You mean to Rich's prior presentation?

CHAIRMAN BROWN: Yes, I B- well, he can talk from over there. This is not a B-

MR. THORP: Sure.

CHAIRMAN BROWN: One of my questions had to do, if I can ever find them again, had to do with B- I've been looking and I lost them. Oh, here they are. No, that's not it either.

MEMBER STETKAR: You need some help?

CHAIRMAN BROWN: Oh, I need a lot of help.

MEMBER STETKAR: This staff member is B-

CHAIRMAN BROWN: Staff member. You're at it, aren't you?

MEMBER STETKAR: I am.

CHAIRMAN BROWN: Oh, here they are. One of the items we've been talking about in recent items is control of access, and I notice we've had an interchange on DRS mPower program on the control of access. And I notice that you all took no action at all relative to any clarifications in terms of communications, and in light of the discussions we've had on control of access. So, I B- did you just B-

MR. STATTEL: There is B- of course, we're addressing all of the topical areas that are covered by the IEEE Standard 603.

CHAIRMAN BROWN: Yes, control of access is

covered.

MR. STATTEL: There is a B- well, let me explain. There is a clause that's titled, "Control of Access," in IEEE 603, and it dates back to the old 1971 standard, the 279 Standard. It's not really intended to address cyber security, because if you think back in 1971 that was really not what they were thinking about. It's really written in the affirmative. In other words, the concern at the time was to make sure that there was adequate access for the authorized people in order to be able to maintain and perform surveillance testing on these systems. So, it's written in the affirmative, make sure that you have the correct access. It's not written in a negative way, prevent access to unauthorized people. So, it was really not the intent of that clause. That clause did not change from 1991 to the 2009 version, so basically the Working Group felt no need to address that.

MS. ZHANG: Well, in addition to that, we did explore addressing cyber security, especially cyber vulnerability.

CHAIRMAN BROWN: I'm not B- I'm separating cyber security from control of access.

MR. STATTEL: Okay.

CHAIRMAN BROWN: They are not uniquely

intertwined. I've made that statement. I've written it in letters, and responses back, and what the Committee has sent back to the EDO.

MR. JUNG: I know, I thought we're going to go through B- without addressing this. We'll be lucky to B-

CHAIRMAN BROWN: No way.

MR. JUNG: I just want to bring B- I agree with you, Charlie, that the Committee's concern is related to control of access away from cyber. When the Staff got the recommendation we wrote a letter to you last year that we are B- a very short letter. We are considering your recommendation, and will update you on the subject. So, when we said the consideration, I just want to give a little background because it was a really serious consideration. Okay? Which resulted in Office Directors level agreement to explore three options in parallel.

One agreement was to B- early engagement with the licensees during construction, so you B- the Committee has seen some of the Staff presentation regarding that subject. I know Diablo Canyon in which NRR and Office of Nuclear Security and Incident Response, they are working together to audit or inspect some of the early implementation of that. So, that was

one of the things B- we thought it was low-hanging fruit, and it's the right thing to do, is ongoing activities that I understand.

Second parallel option that we proposed and explored was to incorporate a requirement on your concern, on the Committee's concern. Although it is specific to sort of control of access and B- but the Staff wanted to address the issue in a more holistic way because that cyber hazard versus safety hazards is really hard to separate in pure nature. So, the direction was for this IEEE Working Group to discuss and see if there's a possibility to address this issue without giving specific direction to whether it's 5.9 or something else.

In my mind it's a partial success, so if you look at the new reactor criteria specific to independence, which is 50.55a(h)(5)(4), which talks about indirect and direct pathways. If you remember earlier, Deanna just went over those four bullets. That is the outcome of the Working Group's effort, so the criteria is a partial success because IEEE 603 is limited to safety system but, Charlie, your B- the Committee's concern is more directed actually to the communication from safety, non-safety, all the way to the outside, and there's specific recommendations.

So, at least we B- the Staff felt that at least B- for new reactors where some of the design details may not be fully in place at the time, at least identifying those indirect and direct pathways at the time of the design certification stage would allow identifying potential hazards, and then the COL applicants down the road would be addressing those, the pathways from a, you know, the existing cyber security programmatic framework.

And third option that we pursued in parallel is longer term solution to pursue a rulemaking on the subject of this particular issue. Remember previously our Division Director at the time, Tom Bergman, talked about some other regulation that allow in certain cases where that type of approach specific to new reactors can be introduced in terms of certain malicious type of activities. So, the outcome of that particular approach is the letter that the Committee has recently received where the B- for new reactors we are pursuing a policy paper to the Commission for a vote with options. That would provide options including option related to a rulemaking on the subject of control of access.

The third option is B- from the beginning we felt that that's the best way, because from a

holistic and firm regulatory perspective that would allow no further debate on Commission's direction regarding the cyber B- all the issues that the Committee brought up even before this control of access. The cyber security certain designs that potentially is better off to be part of the licensing review, all the things, the letter that we received, it is perhaps the best to go back to the Commission and see if there's a certain option for rulemaking would allow better pathways.

So, that's the current status, and so tomorrow we have mPower DSRS, and we can revisit that. This is the history, so in our mind the consideration the Staff made on this effort, we really take it very seriously. We are taking these three parallel path, and there's B- obviously, Rich and some B- there's a discussion of the intent of the 603, the way we reviewed previous designs are not obviously with the same interpretation as the Committee has done in the past. So, for mPower specific, we had a significant discussion whether can we use that as a pilot and move on? But I think generally the consensus, I think is one of those precedent setting issue, and also this is going B- some of the Committee's concerns are beyond the scope of the safety system itself. Probably it's best

to not just do it on mPower specific. So, some of these options, original intent was to be more broad, and to B- not just mPower. But during all these discussions, I think there's some partial success, early engagement with COL applicants and construct those B- those licensees construct, in construction we are early engaged. But I think the letter that we sent to you recently that provides a much better holistic path, that we visit B- we go back to the Commission for certain options.

CHAIRMAN BROWN: What B- which project B- was that a DSRS response letter B-

MR. JUNG: Yes, mPower DSRS.

CHAIRMAN BROWN: It was April 14th or something like that?

MR. JUNG: Right. That's correct.

CHAIRMAN BROWN: Now, when you think about it long term, I mean, if you look at B- I'll listen to Rich and what he comments. I understand the point about the different tone relative to the B- but if you looked at the words it talks about maintaining administrative control of access to the safety systems, et cetera, and the plant should be designed to insure that can be accomplished.

MR. THORP: Yes.

CHAIRMAN BROWN: I'm paraphrasing a little bit, but that's the key sentences I think that are in there, roughly.

MR. THORP: Right.

CHAIRMAN BROWN: And that worked fine in the analog design world. It doesn't work in the world where you have digital systems feeding into networks, a network, whether it's redundant network or whatever, that's a reliability issue, but then that feeds all whether it's the control room, technical support center, emergency operating facility, whatever, as well as these little boxes that lead off to the rest of the world. Totally different venue, and that complicates the ability for the operators to maintain assurance there their administrative control is satisfactory. And pushing off decisions, bigger picture decisions when you have the chance to another rule five or ten years later is not striking while you have the opportunity to establish some basis for giving that plant more control over access now. So, that's just B- I'm just putting B- I understand your point, but holistic or waiting is B- and I didn't digest the whole April 14th letter. I just didn't have time when I got it. So, I understand what you're saying, but let's see where we go with that.

MR. THORP: There's aspects of what we currently do that shouldn't be ignored. It's not as though we're waiting in a vacuum for rulemaking that's way down the road.

CHAIRMAN BROWN: I don't B- John, I don't disagree with you. I mean, a number of the projects that we talked about they've taken a very positive approach.

MR. THORP: And even in the operating reactor world, the Regulatory Guide 1.152 speaks to the secure development and operating environment, which goes right at the heart of access controls and insuring from the viewpoint of a non-malevolent inadvertent entry or change to the software or the equipment, that that's prevented through the controls that are put into place. And that's looked at B-

CHAIRMAN BROWN: Well, that's the vendors, though. I mean, you're talking B-

MR. THORP: No, no, no, no. That's B-

MR. STATTEL: It's operating environment.

MR. THORP: It's secure development and operating environment.

CHAIRMAN BROWN: Oh, and operating environment.

MR. THORP: Yes.

CHAIRMAN BROWN: Okay.

MR. THORP: Which is at the plant sites. So, that's taken very seriously, and that's part of the work that we do in the operating reactor world. In addition to kind of look at the malevolent side of things, we have been teaming, as Ian pointed out, with NSIR in conducting their audits that are looking B- leaning forward toward the full implementation of the 73.54 requirements. So, I don't think we're in a difficult position at this point. I understand your points, and they're well taken about the need to be sure that all these things are looked at in a digital world.

CHAIRMAN BROWN: Things are different, and we ought to be B- just another rulemaking if I follow the progress, as I've watched just the progress of this particular rulemaking over the last how many years now, three years, four years?

MR. STATTEL: Yes, it's been a while.

CHAIRMAN BROWN: Okay, thank you. You just made my point. And this is a potential vehicle, whether it's accepted or not, but it's at least one to give some thought to. That's all.

MR. STATTEL: Another point I'd like to make on this is even if you were to introduce new required control of access requirements into this, it's B- I'm speaking for the operating reactors, it's really a very

limited opportunity unless you apply this rule as a backfit to them, which we're not doing. Right? So, they're operating on their existing licensing basis, changing this rule wouldn't really impose any requirements unless they make changes.

CHAIRMAN BROWN: Oh, yes.

MR. STATTEL: So, as far as getting bang for your buck with regard to implementing cyber security measures, or control of access requirements, we feel that the programmatic approach that's covered in 73.54 for the operating plants, at least, I mean, that is a way to identify what the critical assets are that are in operation at the plants, and there's lots of them. Whereas, the upgrades, there's a handful, you know. So, there's a lot more opportunity to make improvements in those areas using the programmatic approach.

CHAIRMAN BROWN: Well, when you look at the existing plants, like you say, unless you backfit, how many of those plants have all of their data being dumped into a network and then being connected via the internet to the corporate headquarters? They have zero?

MR. STATTEL: I mean, they have done quite a few B-

CHAIRMAN BROWN: All the analog systems are now feeding their data in like that?

MR. STATTEL: Many clients have done upgrades on their safety and their non-safety systems.

CHAIRMAN BROWN: But if they do upgrades C-

MR. STATTEL: Again, this crosses the border of safety to non-safety, as Ian pointed out, so this B- changing this rule, (a) it doesn't impact the non-safety systems that are already in use at the plants, and it's only going to address from the operating plant perspective those safety systems which they're making changes to. And that's really a very small percentage of the digital systems that are in those plants.

MR. THORP: Additionally, the window within which they need to reach full compliance for this 73.54, and I think Tim Mossman can speak to that a little bit, we're looking at this point about two and a half years for full implementation throughout the industry. Tim, correct me if I'm wrong, but I B- those efforts are keyed on including the kinds of concerns that you have on the control of access. Tim?

MR. MOSSMAN: Yes, Tim Mossman, NRO. I previously worked in NSIR, and I'd be remiss if I didn't bring up, because I don't think we're either ignorant or indifferent to what your concern is. And in the cyber space, folks have to submit a cyber security plan, once

proved becomes part of their licensing basis. The plan includes provisions for establishment of a defensive architecture which is a grouping of systems with barrier devices between different layers. And your control of access comment I think speaks very directly to that Level 3 control systems to plant data network, which the Guidance 5.7.1 does spell out should be a one-way communication out. And if you look further in 5.7.1 it does specify that your one-way pathways must be hardware.

CHAIRMAN BROWN: It says it's preferred. It doesn't say has to be.

MR. MOSSMAN: Once folks sign up to that provision in their licensing plan, it becomes part of their licensing basis. And that is one of the first, what they refer to as the seven low-hanging fruit items that they're currently out inspecting against, is specifically those barriers, and how folks have implemented them. And I don't know how detailed I can get in an open meeting, but I B-

CHAIRMAN BROWN: You don't have to. I'm just B-

MR. MOSSMAN: So, they are looking at that, that is a very specific area of concern, precisely for the reasons you're concerned with.

CHAIRMAN BROWN: The difficulty is 5.7.1 is a Reg Guide, and it does not say "must" or "shall," it is the preferred approach to doing this defensive barrier is a data diode of some sort where they talk about it, but then they say however, in the standard Reg Guide B- and they go off and you can do B-

MR. MOSSMAN: You're correct, it is a Regulatory Guide, but once B- if folks adopt those provisions B-

CHAIRMAN BROWN: I agree if B-

(Simultaneous speech.)

MR. MOSSMAN: Right.

CHAIRMAN BROWN: Sign them up, and that's a different issue.

MR. MOSSMAN: Right. The evaluations to date have been focused on if anybody has taken deviations to those clauses, and I don't know that I can speak to what individuals have done. But I think the answer will be positive.

CHAIRMAN BROWN: That's fine. All right.

MR. THORP: If you wanted to pursue further discussions, I would suggest that you'd have a meeting with the folks from NSIR who can speak more directly to a lot of the specifics that you're concerned about.

CHAIRMAN BROWN: Okay. I just B- I wanted

to have the discussion.

MR. THORP: Thank you.

CHAIRMAN BROWN: I had forgotten about it at the end there. It was a catchall, not a catchall but it was my last one, I wanted to get through all the rest of the stuff before we did it.

MR. THORP: Okay. Thanks, Charlie.

CHAIRMAN BROWN: So, I thank you for allowing me to interrupt Mr. Waterman's progress here.

MR. THORP: Not a problem. Mike's a flexible guy, we can move forward.

MR. WATERMAN: Okay. Today I'll briefly describe the current version of Reg Guide 1.153, what it addresses, and what it does not address. I will then summarize the scope of the proposed Reg Guide 1.153 and discuss the relationship between the Reg Guide and the regulation.

This discussion will lead into an overview of the relationship between Federal Register notices, their associated regulations in the Code of Federal Regulations, and why the scope of the proposed Reg Guide 1.153 changed as much as it did in comparison to the current Reg Guide. I will then summarize the presentation.

Current Reg Guide 1.153 contains three

regulatory positions. IEEE Standard 7-4.3.2 is endorsed via reference to Reg Guide 1.152. Reg Guide 1.97 is referenced for accident monitoring instrumentation guidance. IEEE Standard 603-1991 and the correction sheet dated January 30th, 1995 is endorsed for plants licensed under IEEE Standard 279-1971. However, Reg Guide 1.153 provides no information regarding the Commission's intent in its codification of IEEE Standard 603-1991, or its interpretation of how the standard is intended to be used. So, let's contrast the current Reg Guide 1.153 with the proposed Reg Guide 1.153.

The draft Reg Guide 1.153 guidance was created by incorporating information in the draft Federal Register Notice that will solicit comments from the public on the proposed rule. This resulted in expanding the single page of guidance in the current Reg Guide 1.153 to 19 pages of guidance in the draft Reg Guide. So, why the Federal Register Notice?

The Federal Register Notice conveys the Commission's intentions regarding the rule language. The proposed scope of Reg Guide 1.153 identifies international standards and international guidance that are consistent with the standards incorporated by reference in the proposed rule.

Providing references to these international standards is in line with current NRC policy to provide references to supporting international standards and regulatory guides. This policy encourages NRC Staff and industry to view NRC guidance from an international harmonization perspective. These international standards, however, are not endorsed by the Reg Guide itself.

Proposed Reg Guide 1.153 clarifies rule applicability for modifications and installations of safety-related systems, independence requirements, CCF analysis requirements, and documentation requirements, and provides a glossary of terms used in the rule. The proposed guidance will be changed as stakeholder comments are incorporated into the proposed rule discussion.

For example, removal of a paragraph from the proposed rule will result in deletion of the associated guidance paragraphs in the draft Reg Guide. The next slide provides an outline of the rule Federal Register Notice.

The Office of the Federal Register publishes Federal Register Notices on its public website to solicit comments from the public on proposed rules. Further, stakeholders needing to understand the

underlying basis of a regulation after it has been published can use the Office of Federal Register website to access the regulations associated Federal Register Notice.

The Federal Register Notice provides stakeholders with guidance on how the public may respond with comments, background information describing why the regulation is being proposed, how the proposed regulation is different from the existing regulation, the Commission's intent, that is the underlying basis regarding the paragraphs in the regulation, and what the proposed regulation will state if it is enacted. Let's take an overview look at the Federal Register Notice outline sections that are relevant to the proposed Reg Guide 1.153.

Federal Register Notice sections provide the public important information regarding proposed regulations. The Federal Register Notice sections include boilerplate sections, and sections applicable to the scope of the Federal Register Notice. The discussion section paragraph by paragraph discussion section and rule section are relevant to this presentation, as it these sections that convey the Commission's intent; that is, the underlying basis of the corresponding regulation. It is this underlying

basis that has been transcribed into the draft Reg Guide.

The purpose of the Federal Register Notice topical sections describing a proposed rule is to convey the Commission's intentions regarding the language in the rule. Included in these sections are topics such as definitions of terms, reasoning behind rule paragraphs, et cetera, and NRC Staff scope when applying rule requirements.

Of significance, the Federal Register Notice is a commitment levied on the NRC Staff on how the rule is to be interpreted and applied. The discussion does not impose a similar commitment on the industry. The paragraph by paragraph discussion summarizes the Commission's intended purpose of each paragraph.

The other Federal Register Notice section relevant to this presentation is the Federal Register Notice Rule Section. The purpose of this section is to present the proposed rule as it would appear in the Code of Federal Regulations. The published rule references the Federal Register Notice. For example, 10 CFR 50.55a(h) currently references Federal Register Notice 36 FR 11424 which is dated June 12th, 1971, and other Federal Register Notice discussions. A reference to 72

FR 49999, or 49499 simply states the 10 CFR 50.55a(h)(3) rule without a corresponding discussion. Other references are for ASME amendments to 10 CFR 50.55g.

The Office of the Federal Register and the National Archives and Records Administration maintains these Federal Register Notices on its public website, thereby allowing NRC Staff and the public to access the underlying basis of regulations. Let's take a brief look at the Office of Federal Register role as it relates to this presentation.

The Office of Federal Register maintains Federal Register Notices for public access. These Federal Register Notices are maintained on a 20-year rolling basis. Volumes 59 and later are currently accessible. The FRN database is searchable by the Federal Register Notice number. For example, the underlying basis of 10 CFR 50.55a(h) is published in Federal Register Volume 36, page 11424.

So, all a person needs to do to understand the Commission's intent when it published 10 CFR 50.55a(h) is to use 36 FR 11424 as the key word and search Federal Register database, and therein lies the rub. Searching for FR 36 B- for FRN 36 FR 11424, which is older than 20 years, yields the following message. Looks like we're not going to give it to you. That's

essentially what it says, because only got Volumes 59 to current. You want documents published before that, you have to go to the Federal Depository Library. Ah hah, you might say. I'll just go to the Federal Depository Library website and access 36 FR 11424 there. So, let's go to the library.

The Federal Depository Library system maintains all Federal records regardless of age. The FDL system is publically available through the internet and through in-person visits to the libraries within the system. The Federal Depository Library website first requires a selection with the system, and within which to search for the desired record. These libraries include the Library of Congress, and Regional Federal Libraries. So, a person access the FDL website, selects a library and enters 36 FR 11424 as the search keyword. Alas, the keyword search field does not support FRN number searches. Adding salt to the wound, the person finds that the Code of Federal Regulations does not explicitly provide keywords with which to search.

Summarizing, the Commission's intentions are relatively difficult for the public, NRC Staff, and the industry to obtain especially when they're over 20 years old. This challenge leads to the question, how can the NRC better support the public, the industry,

and the NRC Staff in making available the underlying bases of 10 CFR 50.55a(h)? The search for an answer to this question provided the impetus for changing the scope of Reg Guide 1.153.

The next slide illustrates the comparison between the current scope of Reg Guide 1.153, the proposed scope of Reg Guide 1.153, and the significant differences between the two scopes.

The public and other stakeholders are presented the opportunity to comment on draft federal regulations using Federal Register Notices. In the case of 10 CFR 50.55a(h), the FRN is made up of references to standards, and the Commission's intentions regarding the underlying basis of the regulations. This information is published in the Federal Register Notice discussion section and summarized in the FRN paragraph by paragraph section. Only the regulation paragraphs are published in the Code of Federal Regulations, such as Title 10 of the Code of Federal Regulations.

The FRN discussion is maintained by the National Archives and Records Administration, Office of the Federal Register. The current version of Reg Guide 1.153 provides supplemental endorsements of certain IEEE 603-1991 daughter standards and guidance. Currently, both 10 CFR 50.55a(h) and Reg Guide 1.153

Revision 1, current revision, only reference IEEE Standard 279-1971, 603-1991, and the correction sheet dated 25 January, 1995, or January 30th. The Commission's intent that forms the basis of 10 CFR 50.55a(h) is maintained by the Office of the Federal Register.

As you can see, Reg Guide 1.153 Revision 1 with supplementary endorsements to two other standards is essentially a reflection of the regulation, 10 CFR 50.55a(h). The Commission's intentions are maintained only in the Office of the Federal Register or the Federal Depository Library system.

CHAIRMAN BROWN: That's the Statements of Consideration you're talking about?

MR. WATERMAN: Yes, sir.

CHAIRMAN BROWN: Okay.

MR. WATERMAN: Statements of Consideration.

CHAIRMAN BROWN: You can't find them, in other words. They're hard to get.

MR. WATERMAN: Very B- they're difficult to reach. There is a private company that maintains those records. I can't remember the website right now, but what concerns me is this is a dot com company. Right?

It's a company. Will it be in business next year, five years, ten years, twenty years, forty years? We don't know, we don't control it. We have no control over that.

Okay. The proposed revision to 10 CFR 50.55a(h), in addition to IEEE Standard 279-1971, and IEEE Standard 603-1991 will incorporate by reference IEEE Standard 603-2009. Further, wherein the proposed 10 CFR 50.55a(h) will reference these standards, regulations have been added to apply additional conditions.

The basis underlying the Commission's intentions for incorporating the standard and conditions via the Federal Register Notice are incorporated into the draft Reg Guide. Notice that the proposed Reg Guide will provide the Commission's intent and provide references to the standards; whereas, the current Reg Guide revision only provides references to standards, and no guidance on what the Commission intended.

Take a look, there's quite a bit more scope there, quite a bit more information that the public can use, the Staff can use, and our licensees and vendors can use to understand what the heck are they talking about.

The current Reg Guide revision only

provides references to standards, and no guidance. Now, there are several advantages for changing the scope of Reg Guide 1.153 to capture relevant sections of the Federal Register Notice.

First, the proposed scope addresses the Office of Federal Register, Federal Depository Library FRN availability issue in that no matter when the Federal Register Notice is published, the Commission's intent via the Reg Guide will be readily available from the NRC. For example, the NRC website provides access to regulatory guides that are over 40 years old. For example, Reg Guide 1.6 was published back in 1971. It's still on our website, still accessible.

Second, the NRC website is a logical repository of the underlying basis of 10 CFR 50.55a(h). Stakeholders seeking information regarding how to apply the regulation, or what the regulation is intended to mean will logically first visit the NRC website for that information. If the information is not maintained by the NRC, stakeholders must then navigate away from the NRC website to other websites to obtain information that the NRC did not provide. The perception is that while the NRC may have regulations, other federal agencies control the information supporting those regulations.

Third, the revised scope of Reg Guide 1.153 allows the public to readily access from the NRC website the Commission's definitions of terms, the reasoning behind rule paragraphs, NRC Staff commitments on applying the rule. And, fourth, making the Commission's intentions known via Reg Guide 1.153 provides the public assurance that interpretations of the Commission's intentions are consistent between the NRC and the stakeholders. In other words, everybody is reading the same bible verse the same way.

In summary, Reg Guide 1.153 documents the Commission's intentions regarding 10 CFR regulation paragraphs. The guidance in Reg Guide 1.153 will change in response to changes in the proposed rule as these changes will result in changes to the discussion section, the Statements of Consideration section, and the paragraph by paragraph section.

The Commission's intent with regard to definitions of terms, the underlying basis of the regulation paragraphs, and the NRC Staff commitments for applying the regulations will be available to the public from the NRC website regardless of the age of the FRN that transmitted the proposed regulation. That's the presentation.

CHAIRMAN BROWN: Is this common practice?

MR. WATERMAN: Not that I know of.

MR. PETERSON: That was my question.

MR. WATERMAN: Yes, not B- is this common practice regarding the presentation, or regarding B-

(Laughter.)

MR. WATERMAN: But in all of them, both of those.

MR. THORP: Mike did a pretty snazzy presentation. I'll pat him on the back, very nice.

MR. WATERMAN: I've been disturbed in the past when I tried to figure out what does the Commission mean by a particular regulation. And then when it goes to digging it up, you really have to know your way around the Office of Federal Register of all places, too. I once went to the Federal Depository Library system when I was doing thermal hydraulic analysis of mid loop operations because I wanted to know are there some equations out there that defines drawing a vortex on a reactor coolant B- on a residual heat removal pump. I was doing some of the TH analysis then. So, I thought well, I'll just go to the Library of Congress and plug in vortex, keyword, right? And I will have my answer in a jiffy. Well, the vortex shedding off of airplane wings, there's vortex on hydroelectric dams, all kinds of air entrainment vortex type stuff, right, tornadoes

are vortexes and stuff. I was inundated by information, and that always stuck with me. That was years ago, and it just stuck with me about, you know, if you don't have good keywords and things like that, you go into a Federal Depository Library system, you're lost pretty quick. And it just seemed to me that when we were doing the discussion section on this rule, maybe this was a good time to start capturing all of that discussion about what was it the Commission intended when they wrote this rule. Maybe putting it somewhere where people can find it relatively easily, because just about everybody in the nuclear industry knows where the Reg Guides are. They can bring them up, they can read them. So, essentially, that's why we made the decision to go this route. It seems like a good decision.

CHAIRMAN BROWN: It was very useful to me. I checked it against the Statement of Considerations and you all pretty much regurgitated B-

MR. THORP: I'm not in Mike's Research, Office of Nuclear Regulatory Research Management chain, but I applaud his initiative in pulling this information together.

CHAIRMAN BROWN: I do have one question. I don't disagree. I do have one question. There's the use on page 17 of your Reg Guide where it says, "For example,

10 CFR 50.55a(h)(5)(iii)(d)(1), which is an "i" in the rule, about seven lines down it says, "The use of physical means (i.e., hardware devices)." So, I naturally went to the glossary to find out physical means vice physical mechanisms, and it's not there. So, I B- that seemed to be one disconnect in terms of change in terminology. Did you mean physical mechanism, physical B- or is this something else that you all have in mind relative to B- and those same words are in the Statements of Consideration.

MR. WATERMAN: They should be because it was really a transcribed discussion into there, and changing the woulds into is's.

CHAIRMAN BROWN: You just change B- yes, exactly.

MS. ZHANG: It's probably something we missed when we were writing it. So, we do mean physical mechanism.

CHAIRMAN BROWN: Okay. Well, I would suggest you go fix that on page 18 of the Reg Guide.

MR. WATERMAN: And it was also suggested that B-

CHAIRMAN BROWN: That's a high-quality comment.

MR. WATERMAN: It was also suggested the Reg

Guide provide additional examples.

CHAIRMAN BROWN: Okay.

MR. THORP: So, I think we're at a point where B- break? You want a break? That's up to the Chairman.

MS. ZHANG: It's up to him.

MR. THORP: Next up is Royce Beacom to speak to the B-

CHAIRMAN BROWN: About how long does he have?

MR. BEACOM: I have a half an hour.

CHAIRMAN BROWN: We'll take a 10-minute break just so we won't have any interruption.

MEMBER STETKAR: It'll be 15.

CHAIRMAN BROWN: That's why I said 10, because I know it'll be 15.

MEMBER STETKAR: Okay.

CHAIRMAN BROWN: Okay, we'll recess for 10 minutes. We'll be back at 3:10.

(Whereupon, the proceedings went off the record at 2:51 p.m., and went back on the record at 3:13 p.m.)

CHAIRMAN BROWN: The meeting will now come back into session. Just to make sure we've got everybody's attention with a dynamic drawl, and I'll

turn it back over to John here so you can proceed with Royce.

MR. THORP: Thank you, Charlie. And Royce Beacom, as I mentioned earlier, is Chairman of the 603 Working Group and is a member of the NPEC Committee within the industry, so his representation on those groups has been a benefit to the Agency. And he's got some insights and sort of a look ahead at what the standard is going to be going through in the future.

MR. BEACOM: I'm also in John's group.

MR. THORP: Yes, Royce is a member of B-

(Laughter.)

MR. THORP: Member of my Branch, so I'm very happy to have him in my Branch.

MR. BEACOM: Okay. I'll be describing some of the of the B- the status of the next revision. I will be screening the rulemaking changes for inclusion into the next revision of 603, and what's been communicated to the IEEE Technical Committee as proposed changes.

Now, this morning I've heard several instances where it was said to ask the IEEE Working Group. Well, now is your chance. I counted three instances.

CHAIRMAN BROWN: Step back through that, I just lost the bubble.

MR. BEACOM: Oh, okay.

CHAIRMAN BROWN: Step back a little bit, a couple of sentences before.

MR. BEACOM: Okay. I'll be describing the status of the next revision of 603.

CHAIRMAN BROWN: Okay.

MR. BEACOM: Okay? And how we've been screening the rulemaking changes and how they will go into the next revision.

CHAIRMAN BROWN: When you talk about B- in other words, if you revise this and you foresee wanting to revise a(h), if needed, to incorporate whatever you want more stuff in the rule a little bit?

(Simultaneous speech.)

MR. BEACOM: That's right. There's some I call them tangible issues, non-predecisional issues. The tangible issues such as on maintenance bypass the use of the "shall" versus "should." The use of a shall within the note is against IEEE policy and guidelines, so that has to be addressed. That is an issue that we can address directly in this coming revision of 603.

The technology specificity of identifying digital technology, we have to re-look at that through the circumstances how that came about in the 2009 version, because I think we want to maintain this

standard as technology neutral. But due to the Interim Staff Guidance on digital communications at the time, and also we had not B- well, the IEEE standard on digital technology had not been updated to include the Staff's digital communications criteria at that time.

CHAIRMAN BROWN: In that 7-4.3.2?

MR. BEACOM: That's right. I'll try to stay away from using that nomenclature. I'll call it the IEEE standard on digital technology. It had not been incorporated, the NRC Staff Guidance on digital communications. So, that's one of the reasons why we went to including technology specific language in 603. But there's also other B- there's enhancements in independence that I think right now can be considered predecisional by the Staff that won't necessarily go into this right away until we get to hear from the public, the public comments after it goes out, and we get the final version in the FRN. A final FRN is when we'll know for sure on those types of things if they should affect the 603 standard itself.

CHAIRMAN BROWN: You're talking about the FRN we're dealing with now, or the newer B-

MR. BEACOM: Yes.

CHAIRMAN BROWN: B- whatever subsequent C-

MR. BEACOM: The FRN for the rulemaking, for this rulemaking.

CHAIRMAN BROWN: For this rulemaking.

MR. BEACOM: Right. If you notice, in some cases you're going beyond what is stated in the standard, particularly when you amplify system integrity, where you amplify independence.

MR. THORP: So, if I could clarify, what the Standards Committee is going to do is they're going to keep a sharp eye on what we as an Agency do with rulemaking and consider that an input to their standards development. So, they view the NRC rules as a source of information that might help improve the standard, so things that we're adding to the IBR rulemaking, the 50.55a(h) which don't really have a foothold yet in 603 might be considered by this Working Group for inclusion within 603.

CHAIRMAN BROWN: At the next revision.

MR. THORP: At their next revision of their standard, right.

CHAIRMAN BROWN: I'm getting the flavor, maybe I'm misinterpreting your words, that the existing FRN and the rule as it's being written because of public comments may eliminate or disagree, or take out some of these things that are being proposed.

MR. THORP: Yes, sir.

CHAIRMAN BROWN: Which are not of great interest.

MR. BEACOM: You can't say that B- no, I wouldn't say they're not of great interest. They can definitely impact the standard for sure.

CHAIRMAN BROWN: Well, but the standard is being modified in the rule to take into consideration the things that the Staff feels need to be covered. The present standard is being IBR's in the new rule with modifications.

MR. BEACOM: With modifications, right. Now, do those modifications pertain strictly to the standard or is that regulatory criteria? There's also a clause within the design basis of 603 that identifies special requirements. One of those special requirements is the regulatory criteria. Does it come under that category, or is it something that is more tangible, that is particularly if it is contrary to what the intent of the standard is that is specific, like such as I mentioned on technology neutrality.

CHAIRMAN BROWN: Yes.

MR. BEACOM: Or the use of "shall" versus "should." Are those issues that we can address right now, because we have a time limitation on the next

revision to the standard. That's another issue. We don't have quite the time afforded a rulemaking process, so we have to take what we can see as being tangible from the rulemaking process and consider that for inclusion in the IEEE standard revision.

MR. THORP: I suggest that we go ahead and get into the slides so you can see what Royce is going to show you relative to what their plans are for the next revision of the standard. And as I pointed out earlier, I think what I'm hearing is that while we B- we have a voice in the Standards Committee, the Standards Committee has membership from throughout industry.

CHAIRMAN BROWN: Yes, I understand.

MR. THORP: So, they won't necessarily make a change to the standard just to reflect what we've done, but they view NRC rules and technical guidance, et cetera, associated with this standard as a source of information to them as an input. So, they'll consider that as they go forward.

CHAIRMAN BROWN: Right.

MR. THORP: So, why don't you go ahead and move through the slides, Royce.

MR. BEACOM: Okay. I can't stay away from B- so, maintenance bypass, maintenance bypass is an excellent example. Now, the NRC definitely does not

want to soften that maintenance bypass requirement.

CHAIRMAN BROWN: You noticed that.

MR. BEACOM: They want to go back to a "shall." Now, why did the IEEE standard go from a "shall" to a "should?" Maybe industry wants to maintain a "should." That will be B- that we can B- we'll consider that. We'll consider whether we want to revise the language in that particular criterion, and we'll put it out for the ballot and see what we get as far as comments back from the industry.

CHAIRMAN BROWN: But that does not preclude the NRC from doing B-

MR. BEACOM: Right.

CHAIRMAN BROWN: I'm just trying to make sure we don't lose track while the standard itself may change to be more technology neutral, if you want to change it the next time somehow.

MR. BEACOM: Right.

CHAIRMAN BROWN: That doesn't mean that the NRC Staff won't issue another revision to the rule because you've now lost something by doing that. There's a potential for trying to B-

MS. ZHANG: Well, the 2009 version of the rule doesn't go away. We incorporate by reference just because IEEE moves on to like 2014, 2015 standard, we

still B- the official version we incorporate by reference is the 2009.

CHAIRMAN BROWN: No, I understand that. I mean, if you want to upgrade to the next version then you may be faced with expanding the other modifications or subject to's, or whatever. Okay.

MR. BEACOM: Right. Okay. Now, I'll go on. Here we go.

MR. THORP: Okay. Thanks, Royce.

MR. BEACOM: Hang on here.

CHAIRMAN BROWN: Trying to understand the process.

MR. BEACOM: Okay. And there's three B- like I said, there's three instances where it was ask the IEEE Working Group this morning. One was on Criterion 5.6.3.1 on digital communication independence. I'm ready to address that. I'll address that later. The other one John brought up was the Criterion 583 on indication bypass, Part B. Now that one I wasn't prepared to discuss, but that's a very good B- that's a good comment. And I can give you some history on that, but I can't entirely answer that.

CHAIRMAN BROWN: Okay.

MR. BEACOM: And then the 516 common cause failure, definitely have a discussion of that prepared.

So, now I'll move on.

So, the revision status of the new IEEE 603, that's not the 2009 version, the one B- the next one coming up. 603-2009 must be revised by 2019. New policy, IEEE new policy is a 10-year life cycle for standards. There's no reaffirmations versus before it was a five-year, we could always reaffirm the standard saying that there is no changes to the standard. It should be okay as is, and you've got another five years, or whatever. But the new policy extends the life and it essentially is revise a standard or it goes inactive. And if you'll notice if we did that the last time, the time between the '98 and 2009, it would have gone inactive. So, the Working Group is bound by the IEEE Standards Association policy and procedures to move on with and include the revisions that we have identified to date. I'll explain those, too.

The revision request has been reviewed by the Nuclear Power Engineering Committee. When approved, we will have four years to complete the revision, including the balloting time. Approval is expected to follow the rulemaking presentation in July which Ted will be doing. We're making a presentation there.

One of the comments I had when trying to

B- when I submitted the revision request was, in effect, "Secretary's initial response is the request is approvable, but the concern is why the NRC has not been able to IBR the standard over the last three years." So, that's sort of being held up until we explain entirely and he sees all the rulemaking changes affecting the standard itself.

To date there have been some B- there's been a few predecisional rulemaking changes identified for the standard. Now, I also talk about the screening process I use to identify what those are. Here are some of the examples. I brought that up a couple of times. The maintenance bypass criterion revision where use of the "shall" statement within a note is against IEEE guidelines. But we also have to consider in the body of the criterion whether or not to maintain a "should" or a "shall." What does the industry want in that case?

The common cause failure criterion where that also is centered around a "shall" statement, indicating that a requirement is necessary. This goes back to the 1998 version of the common cause failure , 516. 516 then had one statement that caused a lot of consternation both by the Working Group. Well, there's only one B- carry over one person from the 1998 Working Group to the 2009 Working Group.

MR. THORP: We're talking the Standards Working Group.

MR. BEACOM: The Standards Working Group. Thank you. I'm only talking about the IEEE Working Group at this point. But you'll see in the '98 version it says that "plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common cause failure. See IEEE 379."

Now, that is a statement which there is a lot of comments to as to whether or not they should keep in the 2009 version. It was eventually decided not to, because that is really a misinterpretation of, one, 379. 379 is on single failure criterion. It so happens the Working Group also is responsible for that standard.

379 on single failure says that for each design basis in the event of a single failure, not a single common cause failure. Hopefully, in the latest revision of 379 we've been able to clarify the differences between common cause failure and single failure. But, nonetheless, we left out that statement at the last minute because there is a lot of comments within the Working Group, in fact within the NRC about that particular statement.

Now, if you take that sentence out of there, that's where you just are left with 7-4.3.2 provides guidance on performing an engineering evaluation on common cause failures, and you don't have a requirement. We've already discussed B- the IEEE Working Group has already discussed possible solutions to that, and it also is in line with, John, your comment this morning about if we B- have we entirely eliminated hardware common cause. I agree with you. We are going to make this at least one statement within that criterion generally applicable to both hardware and software, and then possibly provide a reference to the Standard 7-4.3.2 for digital technology.

MEMBER STETKAR: For the digital B-

MR. BEACOM: Right. I think we can't exclude anything yet, but unfortunately there's no standard with which we can point to for hardware.

MEMBER BLEY: Yet, the existing IEEE standard is pretty much saying do all these things such that it won't be a problem.

MR. BEACOM: Are you talking B-

MEMBER BLEY: I forget the number of it.

MR. BEACOM: Oh, 379?

MEMBER BLEY: Yes, I think that's it.

MR. BEACOM: You can do all these things.

That's right.

MEMBER BLEY: They're good things.

(Simultaneous speech.)

MEMBER BLEY: They're good things, and they get rid of the bit hitters, the biggest hitters, but they don't really leave you with nothing.

MR. BEACOM: That's right.

MEMBER BLEY: There are still common cause failures that occur and that aren't covered by B-

MR. BEACOM: Yes, sir. And we just updated that and Mike has provided a good flow chart.

MEMBER BLEY: I mean, that was the hope 40 years ago. We kind of said well, if we do all these things well there won't be anything left. And the hope hasn't proved out.

MR. BEACOM: No, it has not. We agree with you, so there's no way to eliminate hardware.

MR. WATERMAN: The problem with the way 379 stated it was certain common cause failures should be addressed as single failure. And then the next paragraph it says the common cause failures due to external B- need not be considered are those caused by external events which are handled by equipment qualification, manufacturing defects which are handled by quality assurance, or maintenance errors or operator

errors which are handled by training and procedures. Right?

MR. BEACOM: Exactly.

MR. WATERMAN: Well, when you go through that, what the heck is left? I mean, you know, name me a common cause failure that isn't covered by those things.

MEMBER BLEY: But those things don't guarantee they won't happen, they just reduce the likelihood, and not low enough so that we don't see them.

MR. WATERMAN: Yes, so it's like they exempt all common cause failures for hardware.

MR. BEACOM: The other issue is on the technology specific instances to be removed. The Working Group has again discussed that, and that's one of the items that we've identified in the revision process that we're waiting approval on. But what's most important is the screening process which we've been using in the predecisional phase once the rulemaking B- and will be used once the rulemaking description has gone completely public.

CHAIRMAN BROWN: Can I B- on the technology neutral thing, I'm just trying to come up with an example, so I was looking at the Standard 2009, and I'm

looking at the independence part under isolation where it says "isolation devices shall insure electrical isolation and digital communication independence." Is that B- you would then remove the terms such as "digital communication independence" to make it technology neutral?

MR. BEACOM: That is correct.

MR. WATERMAN: Could we remove the word "digital" and still be technology?

CHAIRMAN BROWN: Well, I'm trying to connect the dots in my brain as to why the standard has to be technology neutral.

MR. BEACOM: Well, there's another statement in there that I'll point this out to you later here. So, give me a minute and I'll point that out, why it should be technology neutral.

MEMBER STETKAR: I mean, in principle, Charlie, if I want to take my existing old analog relay-driven I&C system today, and for whatever reason if I want to replace it, change a little bit of its functionality, and change B- replace it with a new old analog relay-driven system, there ought to be a standard that applies to that. Right?

CHAIRMAN BROWN: It used to work, why doesn't it still work even though you've got the B-

MEMBER STETKAR: But, I mean, you know, why try to make it technology neutral is to try to cover all of those eventualities, or some hybrid, you know, which we are seeing.

CHAIRMAN BROWN: I just think it makes it too mushy.

MR. BEACOM: Mushy if you don't B-

CHAIRMAN BROWN: I mean, if it's neutral you say nothing.

MR. BEACOM: No, no, no, no. You have functional requirements.

MEMBER STETKAR: You have functional requirements that apply to everybody regardless of B- you don't have to have this artificial definition of what is data communication, for example.

CHAIRMAN BROWN: Yes, but there's a big difference between data communication in a computer-based system, there is in an analog system.

MEMBER STETKAR: At the fine design area, but not at the functional requirements.

CHAIRMAN BROWN: I guess I would disagree with that, but that's B- we'll have to have that disagreement.

MR. BEACOM: We'll get to the intent of the standard. You're right, it's more on the functional

requirement stage versus what widgets we have implementing the functional requirements.

CHAIRMAN BROWN: Well, this doesn't sayB-

MEMBER STETKAR: What ought to be done, rather than how to do it.

MR. BEACOM: So, the screening rulemaking changes in IEEE 603, this is the existing criterion within the design basis of the standard. It says, "Any special design basis that may be imposed on the system design, diversity interlocks regulatory agency criteria." So, this is the first thing that when we went to screen the rulemaking changes, that should be identified in the next revision of 603.

The next issue is, is a change consistent with the application section of the standard which says, "Good engineering judgment should be exercised in the analysis to determine the design basis so that adequate margins exist in the design without imposing unduly restrictive criteria." This statement iterates good engineering judgment should insure adequate margins exist when determining the design basis without imposing unduly restrictive criteria.

Now, this standard is a performance-based standard versus a prescriptive-based standard. It is based on an engineering evaluation of a design

established on objectives, functional statements, performance requirements, and design basis scenarios for the design and evaluation of safety systems. That's why we use several phrases of "to the degree necessary," also.

And as John mentioned early this morning, he calls 603 a philosophy. Well, to some extent I definitely agree with that. I say it is, it is in its general nature. I think we'll agree that also it is not a prescriptive standard.

The other issue is this standard does say, "The standard is general in nature and requires supportive standards to comprise a minimal set of requirements." This also is the Foreword to the Standard. I has "supportive standards shall contain both general and detailed criteria to comprise a minimal set of requirements."

So, we ask ourselves for each change is the change inherent to a support a standard? If so, it should be moved to support a standard and not part of the general standard. So, let's take a look at what changes we've identified to the Nuclear Power Engineering Committee.

The revisions to IEEE 603 are being reviewed by NPEC, can be described as follows. To remove

the Informative Annex B on Electromagnetic Compatibility. As Rich said, the industry uses Reg Guide 1.180 as the latest guidance on this subject, and NRC Research is preparing to update it based on the information from several standards. This Annex is Informative as the new Reg Guide 1.153 points out. NPEC agrees that a new Normative Standard is warranted on the subject of EMI/RFI.

Remove the technology-related criteria to insure the standard remains technology neutral. The standard states that it's general nature, and requires supportive standards such as the IEEE Standards for digital technology, 7-4.3.2 containing both general and detailed criteria to comprise a minimal set of requirements. This change may induce some backtracking related to the recent revision to maintain the stated intent of the standard; that is, it's general in nature and technology neutral.

We're also going to add the IEEE style manual on word usage. The sub-clause on deliberate use of "shall", "should," "may," and "can" confirm its practice throughout the standard. Insure each requirement has a "shall" statement. Example again is the 516 on common cause failure would be consistent with this requirement. Also, this criteria is one of the two

criteria in the standard that the "shall" statement to be added.

MR. THORP: Are you going to bring up the discussion of "must," and "shall," in your Committee discussion.

MR. BEACOM: Must. Okay.

MR. THORP: In your Working Group discussion? It might be worth just having a discussion about it. I'm fascinated with that.

MR. BEACOM: Yes, the IEEE style manual is very discrete, very directive as far as identifying when those four words should be used, "shall," "should," "may," and "can." There is no B-

MR. THORP: "Must."

MR. BEACOM: B- "must."

MR. THORP: All right. Thank you. Keep going.

(Laughter.)

MEMBER BLEY: Royce?

MR. BEACOM: Yes?

MEMBER BLEY: Your first bullet up there, is there work headed on doing the new standard, or is it just B-

MR. BEACOM: We're trying to find where we can get it.

MEMBER BLEY: Sorry?

MR. BEACOM: We're trying to find where there is one standard on EMI/RFI. Looking at the prospective that Research has identified as part of their B- before they B- about to send the purchase order out for updating Reg Guide 1.180, they've listed four or five different standards to incorporate and review to come up with the revision to 1.180.

MEMBER BLEY: I'm not directly familiar with 1.180, but does it look at both natural sources of EM problems, as well as human caused ones?

MR. BEACOM: Natural sources?

MR. WATERMAN: As in solar flares?

MEMBER BLEY: As in solar flares or other B- yes, I think there are some others, but yes, definitely that.

MR. BEACOM: There is another issue. Okay? Something else we can remind Research to take a look at.

MR. THORP: We can take a note on that, and that's a great follow-up. We'll pass that on to Russ Sitner and the folks in Research.

MR. WATERMAN: How technology neutral should the standard go? Because if you really want to be technology neutral you have to take electrical out

of there, also.

(Laughter.)

MR. WATERMAN: Think about it. I've seen there's a lot of emergency diesel generator starting systems that are pneumatic, all pneumatic logic. You have hair dryers, the whole bit, and it's dry air in a pneumatic system, and that's the way they start.

MEMBER BLEY: Back to natural lighting is another one.

(Simultaneous speech.)

MEMBER STETKAR: They claim it was that, the trip B-

MEMBER BLEY: Yes, there were reports of actual lightning getting into containment and bouncing around. And I've seen stuff through work at the Army where they thought they had Faraday cages built around things and actually the lightning protection brought the lightning inside because they weren't perfect. It's pretty interesting. It's not simple stuff, that's for sure.

MR. BEACOM: So, we'll insure other user feedback is provided that it's appropriate included. That helps the Working Group significantly when issues emerge during the revision of the standard, such as the issue you just brought up in 583. I'll include that in

the Task List, and we'll consider that for whether or not that should be revised.

CHAIRMAN BROWN: Are any military standards, like Mil Standard 461 evaluated for the EMI?

MR. BEACOM: Yes, there was, or yes, it is. And yes, it will be also looked at, the updated. I think it's the F 461 B-

PARTICIPANT: 461 E.

CHAIRMAN BROWN: F is out.

MR. BEACOM: F is out, right. And that's also identified by Research to be looked at to update 1.180.

MEMBER BLEY: There's some international C-- what's the B- we've got the IEEE but internationally it's the I B-

(Simultaneous speech.)

MEMBER BLEY: Yes, there's some real extensive work in that area. That's all on the table being examined?

MR. BEACOM: Yes. But there is no one source is the issue.

MEMBER BLEY: Yes.

MR. STATTEL: The philosophy that that Reg Guide incorporates is basically establish an envelope of qualification, so basically there's a test regimen.

They test the equipment to certain levels at varying frequencies, so that establishes an envelope. And then the next stage is evaluate the environment into which the equipment will be installed, and to insure that that's enveloped by what the equipment was tested to. And it provides some allowance for the envelope to be expanded or contracted based on the level of testing that was performed. So, that's the general philosophy.

MEMBER BLEY: Thanks. I've never read it. I have to take a look at it.

MR. THORP: Our Staff most recently has applied that particular Reg Guide in their reviews of the overall implementation plans for the spent fuel pool level instrumentation work being done by industry in response to Order EA 12-051 as one of the Fukushima Lessons Learned. And they were doing exactly that process.

MR. BEACOM: So, I'll summarize where the B- when and how the changes for rulemaking will feed back into and materialize within the standard itself. The Working Group will consider the changes by review of the final positions of the NRC Staff delineated by the rulemaking in the public FRN.

When does that happen? Well, that can B- perhaps beyond the next 2018 we'll call revision.

It'll be close whether or not we'll be able to get everything in that the public rulemaking has comments to in the final FRN.

Also, the review of the predecisional issues for inconsistency with latest IEEE standard development policies and guidelines, that's currently ongoing, and that's something we're constantly looking at as far as being in the Rulemaking Working Group and being able to identify that to the IEEE Working Group.

Review of all changes for consistency with the standard's application and purpose. That, again, that can be done ongoing and part of the next revision. I hope I've been able to identify how it's a feedback now as far as what the Rulemaking Working Group is coming up with changes or amendments to the standard. And you can write that back into the standard itself in the next revision, if it's in the time we have available.

MR. THORP: And, of course, that gets balloted, you know, discussed by all the various stakeholders within that Standards Working Group.

MR. BEACOM: Right. Once we get the review, the revision process approved, we have a four-year window to revise it. And we can extend that to another year which will take us out to 2019 maximum for the

10-year life of the standard itself. That's the time line that we are required to meet based on the Standards Association.

I am done, I think we are done.

MR. STATTEL: That concludes our presentation.

MR. THORP: Any other final questions from the B-

MR. WATERMAN: I think there's one clarification, that even if the standard dies in 2019 doesn't mean it's no longer part of the regulation. Just like 279-1971 is no longer supported by the IEEE, it's still a regulation.

MR. STATTEL: Good standards never die, they just B-

(Laughter.)

MR. STATTEL: B- go to the library.

CHAIRMAN BROWN: All right. Well, I'll go ahead and get any additional Member comments. Dennis?

MEMBER BLEY: Nothing additional, but thanks to everyone for good discussions today.

CHAIRMAN BROWN: John?

MEMBER STETKAR: Same here. We covered a lot of ground, more ground than you thought you'd probably covered, so we appreciate that. Healthy discussion, we

appreciate that.

CHAIRMAN BROWN: Okay, Myron, anything?

CONSULTANT HECHT: No.

CHAIRMAN BROWN: Yes, I wanted to echo this. I thought the meeting really laid out a lot of information. There were some great discussions on some very interesting topics which is B- I think it was well worthwhile to get the exchange of information. Whether we agreed with each other or not is irrelevant, but they were put on the table. And I thought the B- I personally like, and I don't B- since I found out that this is not really done, I thought incorporating the Statements of Consideration in this circumstance, anyway, it makes sense to make it clear when people want to use these why they were put in, and what's the background and bases for them. And I think that provided a tremendous amount of illumination and an understanding of the shorter comment.

MEMBER BLEY: I'd go even further. I appreciate that a lot. In other areas I've had people try to find them, and it's B- I've given up and asked for help, but people usually find them, and they're very helpful.

MR. THORP: I think Mike may have identified a model that Research ought to consider for the future

for these Reg Guides.

CHAIRMAN BROWN: Christina is going to go open the B- make sure the phone line is open, and we'll request people on the phone first.

Is there anybody on the phone line that would like to make a comment? First of all, would somebody say something to make sure we know the phone line is open?

PARTICIPANT: Yes, it is open.

CHAIRMAN BROWN: Thank you very much. Now, is there anybody on the line that would like to make any comments?

(No response.)

CHAIRMAN BROWN: Hearing none, I will turn to our honored guests. Any comments? None? Hearing none, I guess we will go B- and I want to take a couple of minutes. We're going to have the presentation to the full Committee in July, and we don't have eight hours or seven and a half hours in which to do this. And I was B- you all are going to have to be creative. You'll have a B-

MR. STATTEL: Do we have a date in July?

MS. ANTONESCU: Not yet. We're going to decide which date.

MEMBER STETKAR: It will be the Wednesday

of the B-

CHAIRMAN BROWN: Second week in July.

MEMBER STETKAR: B- second week in July.

CHAIRMAN BROWN: It's either the 8th or the 9th.

MEMBER STETKAR: Like the 9th of July, I believe.

MS. ANTONESCU: No, it's going to definitely be the 9th, because the 8th we have a DAC Subcommittee.

MEMBER STETKAR: Right. And it will be that Wednesday.

MR. STATTEL: Yes, because we have some Staff availability issues that week. We're going to be performing a Diablo Canyon audit.

PARTICIPANT: I think that's in July, not June. Right?

MEMBER STETKAR: July.

MS. ANTONESCU: July.

MEMBER STETKAR: July.

PARTICIPANT: Okay, that should be good.

MS. ZHANG: We'll resolve that.

MEMBER STETKAR: We have you slotted for that first, that week in July, and we're targeting Wednesday of that week.

MS. ANTONESCU: We'll manage.

CHAIRMAN BROWN: Okay. So, my suggestion would be to B- and this is B- you can B- you've got to present this to the full Committee, but you ought to focus a little bit more on the meat as opposed to some of the B- the lead-in is useful but the first 13 or 14 pages were good for us, but can be compressed probably to a couple of slides, what's the intent, this is where we're going, blah, blah, blah, and I'll let you all figure out how to do that.

MR. THORP: Thank you, Charlie, good points. I don't know that we'll include every presentation that we've heard today B-

CHAIRMAN BROWN: I don't think B-

(Simultaneous speech.)

CHAIRMAN BROWN: We don't need the FRN, we don't need Royce's in this circumstance, while they were useful for us in terms of understanding the process, it really is the meat and potatoes part of the particular changes to the rule. And what drove you to do those based on the Lessons Learned we've had in the design reviews.

MR. THORP: Understood. For the sort of angle to it we'll perhaps include, if there is one by that point, whatever resolution there is in the

concurrence process.

CHAIRMAN BROWN: Oh, yes, yes, yes.

MR. THORP: Yes, so we'll include B-

MEMBER STETKAR: That's up to you.

CHAIRMAN BROWN: If you have it, then we would expect to hear about that during that presentation.

MR. THORP: Right.

MEMBER STETKAR: And, John, I think for the benefit of the members who haven't had the benefit of participating here, if you organize it according to each of the sections in the rule, 55a(h)(5), and then if you want to make reference back to the standard, the applicable stuff in the standard do it that way rather than parallel, or whatever. That will provide a much better context.

MR. THORP: What's the time frame we're talking about?

MS. ANTONESCU: Two hours.

MEMBER STETKAR: Probably a couple of hours.

CHAIRMAN BROWN: It won't be any more than that.

MEMBER STETKAR: It won't be any more than two hours. It might be as short as an hour and a half.

MR. THORP: For a two-hour time frame I would suggest we would approach a one-hour presentation, and allow another hour for the discussions and questions.

CHAIRMAN BROWN: We would probably be trying to provide a little illumination to the other members who might be as familiar, and I'm sure we will have B-

MR. THORP: Right, that will take some time.

CHAIRMAN BROWN: B- some of their own B-

MEMBER STETKAR: As a general rule of thumb is plan for about half the time you're allocated in terms of presentation of material.

CHAIRMAN BROWN: Okay. Other than that, I would like to thank you all very much. It was very good presentations, informative, and we thank you for taking the time to provide the level of detail that you provided. That was very useful.

MR. THORP: Okay. Thanks, Charlie.

CHAIRMAN BROWN: Okay. With that, the meeting is recessed.

MEMBER STETKAR: Adjourned.

CHAIRMAN BROWN: Excuse me, adjourned.

(Whereupon, the proceedings went off the record at 3:53 p.m.)

Rulemaking for 10 CFR 50.55a

Incorporation by Reference of Institute of Electrical and Electronics Engineers Standard 603-2009

Presented by: IEEE Std. 603 Rulemaking Working Group

Richard Stattel (NRR)
Royce Beacom (NRR)
Michael Waterman (RES)
Deanna Zhang (NRO)

Agenda

- IEEE Standards Revisions Process
- Describe Reasons for this Rulemaking Activity
- Describe changes made to IEEE Std. 603
- Describe Changes to Regulation
  - Incorporate new version of IEEE 603 2009 by reference into 10 CFR 50.55a.
  - Make changes to applicability of the standard
  - Impose new conditions on the use of IEEE 603
- Draft Reg. Guide to update RG 1.153 being issued concurrently with this rule

Reasons for Changing the Rule

Reasons for this Rulemaking Activity

- The current IBR Standard IEEE 603-1991 has become out of date:
  - It does not address the introduction of digital technologies such as FPGA based systems into I&C safety systems
  - It does not address certain design concepts that have been made possible with digital technologies:
    - Data Communications
    - System Self Diagnostics
    - Integration of systems
    - Consolidation of Functions
- Newer I&C systems are being designed and built to the newer versions of the standard.
  - New I&C systems are designed to 1998 standard
  - Alternative Standard Evaluations required for license submittals
- There has been much disagreement between the NRC staff and applicants over the existing applicability statements

Objectives of Rulemaking Activity

- The proposed rule would update the current NRC regulations to include the most recently promulgated version of IEEE Std 603-2009

  "Criteria for Safety Systems for Nuclear Generating Stations"

  - Define the conditions which would allow existing licensees to replace plant equipment while maintaining existing licensing basis.

  - Defines the conditions for which existing permit, license, certificate, standard design, and standard design approvals would be required to address the new standard in modifications and applications.

  - Imposes conditions upon the use of IEEE 603-2009 in the areas of system integrity, diversity and defense-in-depth analyses, independence, maintenance bypass, and maintenance of records.

What Changed in the Standard

The new version of the standard:

1. Addresses potential safety issues that might arise from incorporating components using advanced technologies in safety systems.
2. Contains additional and updated references and eliminates references that are no longer in effect.
3. Provides added guidance to address electromagnetic compatibility issues for I&C safety systems.
4. Adds new criteria to address the potential for common cause failures
5. Adds classification requirements for equipment not credited to perform a safety function but connected to safety-related equipment
6. Removes a requirement in section 6.7, “Maintenance bypass,” for meeting the single failure criterion during maintenance activities
7. Adds a specific requirement for electrical isolation and digital communication independence between safety systems and non-safety systems

What Changed in the Standard

The new version of the standard:

1. Addresses potential safety issues that might arise from incorporating components using advanced technologies in safety systems.

Sections affected:

Definitions – Expanded the definition for “Component” to include non-hardware based system components such as software, and firmware.

Multiple references to IEEE 7-4.3.2 added to address computer and digital technology based systems. (5.3, 5.4, 5.5, 5.6.4, & 5.15)

What Changed in the Standard

The new version of the standard:

2. Contains additional and updated references and eliminates references that are no longer in effect.

Sections Affected:

Entire Standard. It is normal practice for IEEE to completely update all references within a standard as a part of the revision process.

The NRC endorses many of these referenced standards through its Regulatory Guidance documents. We therefore rely upon updates to these Reg. Guides to address standard updates.

What Changed in the Standard

The new version of the standard:

3. Provides added guidance to address electromagnetic compatibility issues for I&C safety systems.

Sections Affected:

Informative Annex B was added to the IEEE Std. 603 standard during the 1998 revision.

Section 4 “Safety System Design Basis” Item “g” includes a foot note which refers to the new EMC annex.

What Changed in the Standard

The new version of the standard:

4. Adds new criteria to address the potential for common cause failures

Sections Affected:

5.16 – Common-cause failure criteria – This new clause was added to the standard. It refers to IEEE Std. 7-4.3.2.

What Changed in the Standard

The new version of the standard:

5. Adds classification requirements for equipment not credited to perform a safety function but connected to safety-related equipment

Sections Affected:

5.6.3.1 Interconnected equipment – (Subsection of Independence Criteria)

What Changed in the Standard

The new version of the standard:

6. Removes a requirement in section 6.7, “Maintenance bypass,” for meeting the single failure criterion during maintenance activities

Sections Affected:

Section 6.7 – Maintenance Bypass - Establishes performance criteria for situations requiring systems or portions of systems to be placed in a bypass state.

EXCEPTION Clause of Section 6.7

EXCEPTION (in Clause 6.7 of IEEE Std 603-1991): One-out-of-two portions of the sense and command features are not required to meet 5.1 and 6.3 when one portion is rendered inoperable, provided that acceptable reliability of equipment operation is otherwise demonstrated (that is, that the period allowed for removal from service for maintenance bypass is sufficiently short to have no significantly detrimental effect on overall sense and command features availability).

NOTE (in Clause 6.7 of IEEE Std 603-2009): For portions of the sense and command features that cannot meet the requirements of 5.1 and 6.3 when in maintenance bypass, acceptable reliability of equipment operation shall be demonstrated (e.g., that the period allowed for removal from service for maintenance bypass is sufficiently short, or additional measures are taken, or both, to ensure there is no significant detrimental effect on overall sense and command feature availability).

What Changed in the Standard

The new version of the standard:

7. Adds a specific requirement for electrical isolation and digital communication independence between safety systems and non-safety systems

Sections Affected:

5.6.3.1 – Interconnected Equipment – Added the following sentence:

"Isolation devices shall ensure electrical isolation and digital communication independence."

5.6.4 – Detailed Criteria – Added reference to IEEE 7-4.3.2 for criteria on separation and isolation of data processing functions of interconnected computers.

What is Changing in the Regulations

The proposed Rule:

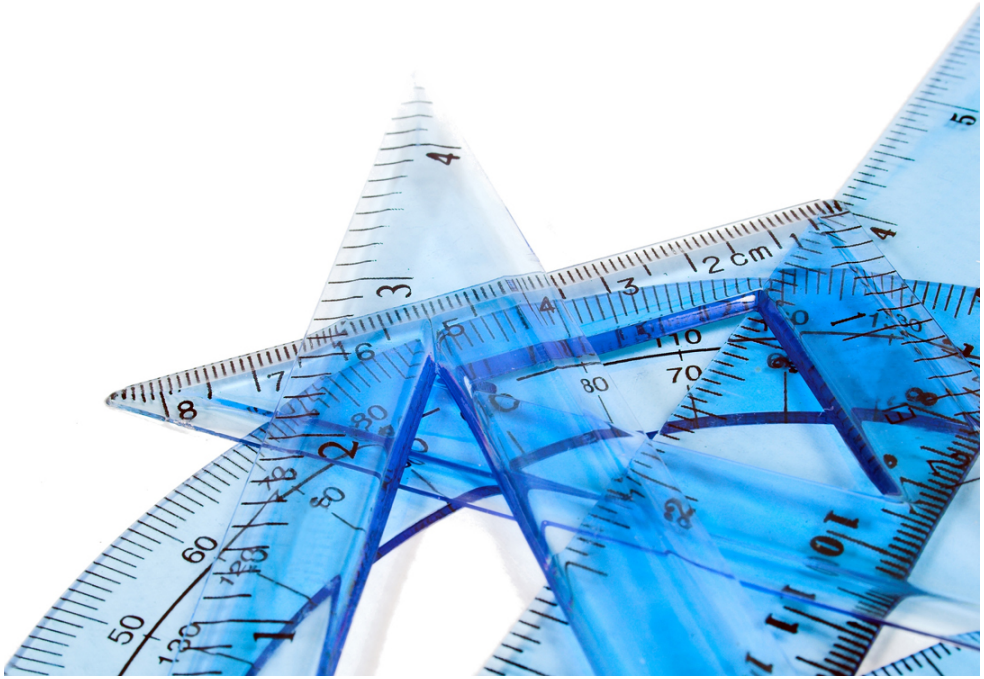
1. Provides definitions for several terms used in various standards and within the proposed regulation.

2. Establishes conditions for applicability of the new and previously incorporated versions of the standard.

3. Imposes several conditions for the use of IEEE Std. 603 2009.

4. Retains the incorporation by reference for IEEE Std. 279-1971, IEEE Std. 603-1991, and the IEEE Std. 603-1991 correction sheet dated January 30, 1995.

IEEE Standards Revision Process



Agenda

- The Revision Process for IEEE Nuclear Standards
- The Revision Status of the new IEEE 603 Standard
- Discussion of the Proposed Changes
- Addressing Regulatory Criteria in IEEE Std 603
- Conclusion

Revisions to IEEE Nuclear Standards

- **The project for a revision to an IEEE Nuclear standard is proposed by the Working Group of the:**
  - **Nuclear Power Engineering Council (NPEC)**
- **This revision project is then reviewed and approved by:**
  - **IEEE STANDARDS ASSOCIATION (SA)**
    - **To be completed in 4 years (including balloting)**
  - **Within the lifetime of the standard – now 10 yrs.**
    - **This was a policy change from a 5 year life.**
  - **Policy dictated reaffirmation is no longer possible.**
    - **The standard goes "inactive" at 10 years.**

The Revision Status of the new IEEE 603

- IEEE Std 603 (2009) will go inactive in 2019.
  - If the standard is not revised by then.
- The Project Request has been submitted to the IEEE STANDARDS ASSOCIATION (SA)
  - Approval is expected in time to officially begin work at the July 2014 NPEC meeting.
  - This allows maximum life of the project (4 yr.) plus 1 year if extension of the project is necessary.
- Rulemaking affects on the next Revision to the Std.
  - To date there have been a few changes not considered “Pre-decisional” (i.e. maintenance bypass, CCF requirement, technology specifics etc.)

Discussion of the Proposed Changes

- **Project description to the Standards Association:**
  - **Remove (informative) Annex B, “Electromagnetic Compatibility.” – The industry uses RG 1.180 as the latest guidance on this subject and NPEC agrees that a new normative standard is warranted.**
  - **Remove technology related criteria to ensure this standard remains technology neutral.**
  - **Add IEEE style manual "Word usage" sub-clause on the deliberate use of “shall, should, may and can" and confirm its practice in the standard. Ensure each requirement has a “shall” statement.**
  - **Revise the standard to include the latest IEEE style manual guidelines.**
  - **Ensure other user-provided feedback is appropriate and included.**
  - **Update references, definitions and the bibliography as necessary.**

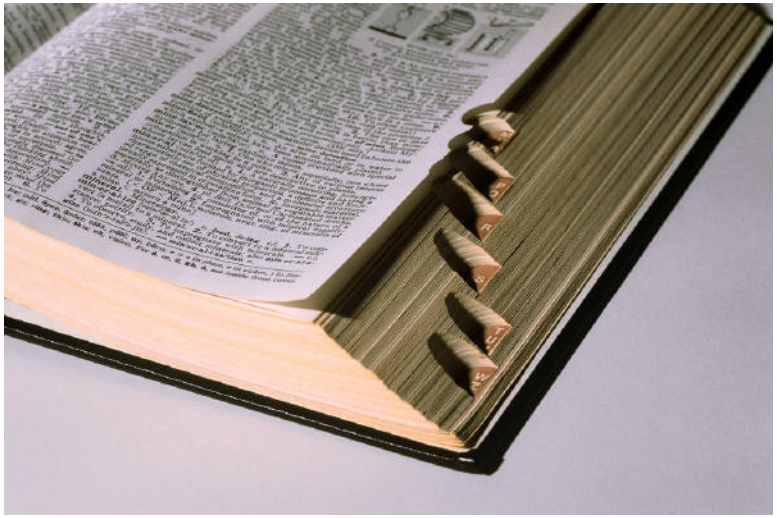
Addressing Regulatory Criteria in IEEE 603

- **There is an existing clause for which existing *and new* regulatory criteria may be imposed on the safety system. Section 4, "Safety System Design Bases," states "The design basis shall document" including:**
  - **4.l); "Any special design basis that may be imposed on the system design (e.g. diversity, interlocks, regulatory agency criteria)".**
- ***When* the final rule is available, the IEEE working group will decide changes to the design bases or the standard by determining:**
  - **The regulatory criteria identified by 4.l) vs. requirements that should be in the standard.**
  - **Consistency with the Application Section of the standard which states "good engineering judgment should be exercised in the analysis (to determine the design basis) so that adequate margins exist in the design without imposing unduly restrictive criteria."**

Conclusion

- **The IEEE working group will consider changes to the standard by:**
  - **Review of the positions of the NRC staff delineated by the rulemaking in the final public FRN – in a future revision.**
  - **Review of the pre-decisional issues for inconsistency with latest IEEE standard development polices and guidelines. – in 2018.**
  - **Review of all changes for consistency with the application and purpose of the standard which are discretely described.**
- ***Finally* the IEEE working group shall decide changes to the standard relative to the nature and relationship to other IEEE standards:**
  - **This is performance based standard that establishes criteria that are general in nature, requiring supportive standards to comprise a minimal set of requirements for safety systems.**

New Definitions



Definitions Provided in FRN

1. Terms Defined in FRN

- Protection System / Safety System
- Best Estimate
- Current Reactors
- Data Communication
- Defense-in-depth
- Diversity
- Function / Functionality
- Hardwired Connections
- New Reactors
- Physical Mechanism
- Repeatable
- Safety Benefit
- Safety Function
- Safety System Function
- Signal Sharing
- Support(s) the Safety Function

What is Changing in the Regulations

2. Establishes conditions for applicability of the new and previously incorporated versions of the standard.

Construction Permit, Standard Design Certification, Combined License, or Manufacturing License Issue Date	**10 CFR 50.55a(h)(2) Paragraph**	**Standard Applicability[1]**
Nuclear power plant construction permits issued before January 1, 1971	**(h)(2)(i)**	Licensing Basis IEEE Std 603-1991[2]
Nuclear power plant construction permits issued on or after January 1, 1971 and before May 13, 1999	**(h)(2)(ii)**	IEEE Std 279-1971 IEEE Std 603-1991
Standard design certifications issued before May 13, 1999	**(h)(2)(iii)**	IEEE Std 279-1971
Standard design certifications issued on or after May 13, 1999, but before 30 days after **[THE EFFECTIVE DATE OF THE RULE]**	**(h)(2)(iv)**	IEEE Std 603-1991
Standard design certifications issued 30 days after **[THE EFFECTIVE DATE OF THE RULE]**	**(h)(2)(v)**	IEEE Std 603-2009
Applications submitted 30 days after [EFFECTIVE DATE OF THIS RULE] for nuclear power plant construction permits and operating licenses under 10 CFR part 50.	**(h)(2)(vi)**	
Nuclear power plant combined licenses and manufacturing licenses under 10 CFR part 52 issued 30 days after **[THE EFFECTIVE DATE OF THE RULE]**	**(h)(2)(vii)** Referenced SDC[3] issued before 30 days after **[THE EFFECTIVE DATE OF THE RULE]**	IEEE Std 279-1971 IEEE Std 603-1991
	(h)(2)(vii) Referenced SDC[3] issued 30 days after **[THE EFFECTIVE DATE OF THE RULE]**	IEEE Std 603-2009

Examples of modifications and replacements of components, functions, and systems

Example	Modification or Replacement Example	Was Functionality, Technology, Independence strategy, or Diversity strategy changed?				Applicable Standard
		F	T	I	D	
1	Power supply replaced in one power train division	N	N	N	N	Licensing Basis Standard
2	Pressure measurement instrumentation replaced with new pressure measurement instrumentation in all four channels of the protection system	N	N	N	N	
3	DNBR safety function replaced with improved DNBR safety function	N	N	N	N	
4	Added functionality to DNBR safety function to allow manual selection of one of four channels of input data for each DNBR channel	Y	N	Y	N	IEEE Std 603-2009 (subject to the conditions in paragraph (h)(4) through (h)(7))
5	Modified a protection system with components based on a different technology	N	Y	N	N	
6	Modified channels or divisions such that independence was changed	N	N	Y	N	
7	Modified a safety function such that protection system diversity strategy was changed	Y	N	N	Y	

What is Changing in the Regulations

3. Imposes several conditions for the use of IEEE 603 2009.

Regulations Affected:

50.55a(h)(4) – Amplify “System Integrity” requirements

50.55a(h)(5) – Amplify “Independence” requirements

50.55a(h)(6) – Amplify requirements for “Common Cause Failure”

50.55a(h)(7) – Correct reference, “Checking Operational Availability.”

50.55a(h)(8) – Clarify requirements for use of “Maintenance Bypass”

50.55a(h)(9) – Provide requirement for “documentation”

System Integrity

50.55a(h)(4) – Amplify “System Integrity” requirements

Applicable Section of IEEE 603:

Section 5.5 “System Integrity”

New requirement added:

In order to assure the integrity and reliable operation of safety systems, safety functions shall be designed to operate in a predictable and repeatable manner.

Independence

Independence

50.55a(h)(5) – Amplify “Independence” requirements

Applicable Section of IEEE 603:
Section 5.6 “Independence”

i. Provides requirements for applicants to address independence among redundant portions of safety systems.
ii. Provides requirements for applicants to address independence between safety systems and other systems.
iii. Detailed Criteria: Clarifies requirements that apply to section 5.6 of IEEE Std. 603-2009.

Independence

50.55a(h)(5) – Amplify “Independence” requirements

i. Provides requirements for applicants to address independence among redundant portions of safety systems.

Criteria Applies to System Architecture

Imposes new requirement for applicant to perform analysis activity to address the following:

1) Safety system internal and external hazards,
2) Extent of interconnectivity between redundant portions of the safety system, and
3) Impact of failures or degradation in one portion of a safety system on the ability of redundant safety system portions to accomplish the safety functions.

Independence

50.55a(h)(5) – Amplify “Independence” requirements

ii. Provides requirements for applicants to address independence between safety systems and other systems.

Criteria Applies to System Architecture

Imposes new requirement for applicant to perform analysis activity to address the following:

1) Hazards posed by other systems on the safety system,
2) Extent of interconnectivity between the safety system and other systems, and
3) Impact of failures or degradation in other systems on the ability of the safety system to accomplish the safety functions.

Independence

50.55a(h)(5) – Amplify “Independence” requirements

iii.Clarifies requirements that apply to section 5.6 of IEEE Std. 603-2009.

Provides Detailed Criteria for the application of Independence Criteria.

A. Independence of Signal Processing
B. Fault Detection Criteria
C. Current Reactor Independence Criteria
D. New Reactor Independence Criteria

Independence

50.55a(h)(5) – Amplify “Independence” requirements

A. Signals between redundant safety divisions and signals from a non-safety-related system to a safety division must be processed in a manner that does not impair the safety functions of any safety system division.

Independence

50.55a(h)(5) – Amplify “Independence” requirements

B. Safety system divisions must detect and mitigate signal faults and failures received from outside the safety system division in a manner that does not impair the safety system safety functions of the division.

Independence

50.55a(h)(5) – Amplify “Independence” requirements

C. For current reactors, communications or signals from outside the safety division during operation must support safety or provide a safety benefit.

Independence

D. For new reactors,

I. Data communications between safety and non-safety systems must be one-way, enforced by a physical mechanism, from safety to non-safety systems while the affected portion of the safety system is in operation.

II. Signals between redundant portions of safety systems may be shared only if the signals are required to perform a safety function.

III. A safety system may receive signals from non-safety systems while the safety system is in operation only if the received signal supports diversity and automatic anticipatory reactor trip functions. These signals must be transmitted over a hardwired connection using means other than data communication.

IV. Applicants for design certifications, standard design approvals, or manufacturing licenses who propose an alternative under 10 CFR 50.55a(z) for complying with the requirement in paragraph (h)(5) above for data communications independence shall identify direct or indirect communication pathways to safety systems from other systems.

Independence

- Proposed paragraph (h)(5)(iv) imposes additional requirements on the applicant of design certifications, standard design approvals, and manufacturing licenses if they propose an alternative approach to the independence conditions imposed in the proposed rule. Specifically, these applicants would need to identify:
  - Any direct pathways from other systems (e.g. direct connections from non-safety systems to safety systems).
  - Indirect pathways from non-safety systems to safety systems (e.g. networked connections from non-safety systems to safety systems).

- This additional requirement facilitate the identification of interdependences and failure modes in the alternative design, including any cyber vulnerabilities the design.

Diversity & Defense-In-Depth

Common Cause Failure

50.55a(h)(6) – Amplifying criteria for addressing “Common Cause Failure” requirements

Applicable Section of IEEE Std. 603:
Section 5.16 “Common-cause failure criteria”

I. Applicants and licensees shall assess the defense-in-depth and diversity of digital safety systems to demonstrate that vulnerabilities to common-cause failures have been addressed.

Common Cause Failure

50.55a(h)(6) – Amplifying criteria for addressing “Common Cause Failure” requirements

Applicable Section of IEEE Std. 603:
Section 5.16 “Common-cause failure criteria”

II. Postulated common-cause failures shall be evaluated to demonstrate adequate diversity within the safety system for each design basis event in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The applicant or licensee shall demonstrate adequate diversity within the design for each of the events evaluated in the accident analysis section of the SAR.

Common Cause Failure

50.55a(h)(6) – Amplifying criteria for addressing “Common Cause Failure” requirements

Applicable Section of IEEE Std. 603:
Section 5.16 “Common-cause failure criteria”

III. If a postulated common-cause failure could disable a safety function, then a diverse means unlikely to be subject to the same common-cause failure shall be required to perform either the same function or a different function. The diverse or different function may be performed by a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.

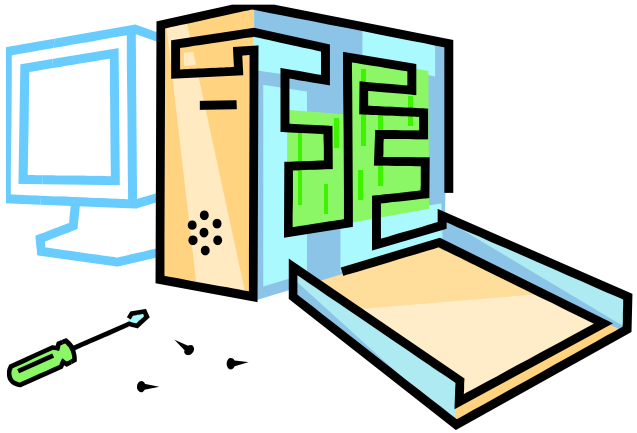
Common Cause Failure

50.55a(h)(6) – Amplifying criteria for addressing “Common Cause Failure” requirements

Applicable Section of IEEE Std. 603:
Section 5.16 “Common-cause failure criteria”

IV. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in (h)(iv)(A) and (h)(iv)(C)..

System Maintenance / Testing



Maintenance Bypass

50.55a(h)(7) – Correct reference, “Checking the operational availability.”

Applicable Section of IEEE 603:
Section 6.5.1.b “Retaining safety function capability during maintenance bypass.”

The constraints referenced in IEEE Std. 603-2009 Section 6.5.1.b shall be the constraints described in section 6.7, “Maintenance Bypass.”

Maintenance Bypass

50.55a(h)(8) – Clarify requirements for use of “Maintenance Bypass”

Applicable Section of IEEE 603:

Section 6.7 “Maintenance Bypass.”

The maintenance bypass requirements stated in Section 6.7 of IEEE Std. 603 1991 shall be met instead of the requirements stated in Section 6.7 of IEEE Std. 603-2009.

Documentation

Documentation to Support Compliance

50.55a(h)(9) – Documentation supporting compliance

Applicants and licensees shall develop and maintain documentation, analyses, and design details demonstrating compliance with paragraphs (h)(2) through (h)(8) of this section..

Alternatives Clause 10 CFR 50.55a(z)

50.55a(z)

(z) Alternatives to codes and standards requirements. Proposed alternatives to the requirements of paragraphs (b)(4), (b)(5), (b)(6), (c), (d), (e), (f), (g), and (h) of this section or portions thereof may be used when authorized by the Director, Office of Nuclear Reactor Regulation, or Director, Office of New Reactors, as appropriate. The applicant or licensee shall demonstrate that:

(1) Acceptable level of quality and safety. The proposed alternative would provide an acceptable level of quality and safety; or

(2) Hardship without a compensating increase in quality and safety. Compliance with the specified requirements of this section would result in hardship or unusual difficulty without a compensating increase in the level of quality and safety.

Draft Reg. Guide 1.153

Draft Regulatory Guide (DG)-1251 (RG 1.153,

“Criteria for the Power, Instrumentation, and Control Portions of Safety Systems for Nuclear Power Plants,”

Provides additional guidance for implementing the requirements of the rule. This Guide is based upon the discussion in the FRN, and does not modify the scope of 50.55a(h).

END

Draft Regulatory Guide 1.153

(Proposed Revision 2 of Regulatory Guide 1.153, dated June 1996)

CRITERIA FOR THE POWER, INSTRUMENTATION, AND CONTROL PORTIONS OF SAFETY SYSTEMS FOR NUCLEAR POWER PLANTS

Presented by: IEEE 603 Rulemaking Working Group

Richard Stattel (NRR)
Michael Waterman (RES)
Deanna Zhang (NRO)

Introduction

- Current Reg. Guide 1.153
- Draft Reg. Guide 1.153
- Reg. Guide 1.153 and 10 CFR 50.55a(h)
- FRNs and Regulations
- Why the scope of RG 1.153 changed
- Summary

Current Reg. Guide 1.153

- **Regulatory positions**
  - **Endorses IEEE Std 7-4.3.2-1993 via reference to RG 1.152, Rev. 1**
  - **References RG 1.97, Rev. 3 for accident monitoring instrumentation**
  - **References IEEE Std 603-1991 and correction sheet for safety system power, instrumentation, and control design, reliability, qualification, and testability**
    - **Allows IEEE Std 279 plants to use IEEE Std 603-1991**
- **No guidance is provided on the underlying basis of 10 CFR 50.55a(h)**

Draft Reg. Guide 1.153

- Scope of RG 1.153 increased to provide the Commission's intent from the FRN Discussion
- Draft Reg Guide 1.153
  - Identifies international standards and guides that are consistent with the Rule–endorsed standards
  - Clarifies Rule applicability
  - Provides a glossary of terms used in the Rule
- Guidance will be revised consistent with revisions to the proposed Rule Discussion

Rule Federal Register Notice

- The Rule FRN consists of several sections that include
  - How to comment
  - Background information
  - How the proposed regulation is different from the existing regulation
  - The Commission's intentions underlying the regulation
  - What the proposed regulation will state

Rule FRN Outline

Summary

I. Obtaining Information and Submitting Comments

II. Background

III. Discussion

IV. Paragraph–by–Paragraph Discussion

•

•

Rule

FRN Topic Sections

- The FRN describes the Commission's intentions in enacting a Rule
  - Definitions of terms, reasoning behind Rule paragraphs, etc.
  - NRC Staff scope of applying Rule requirements
    - NRC Staff commitment
    - Not an industry commitment
- FRN Paragraph-by-Paragraph Section
  - Commission's intended purpose of each Rule paragraph

FRN Topic Sections
(continued)

- **CFR Regulation (Rule)**
  - Provides the proposed Rule paragraphs
  - CFR Rules reference associated FRN(s)
    - For example, 10 CFR 50.55a(h) references FRN 36 FR 11424, dated June 12, 1971

Office of Federal Register

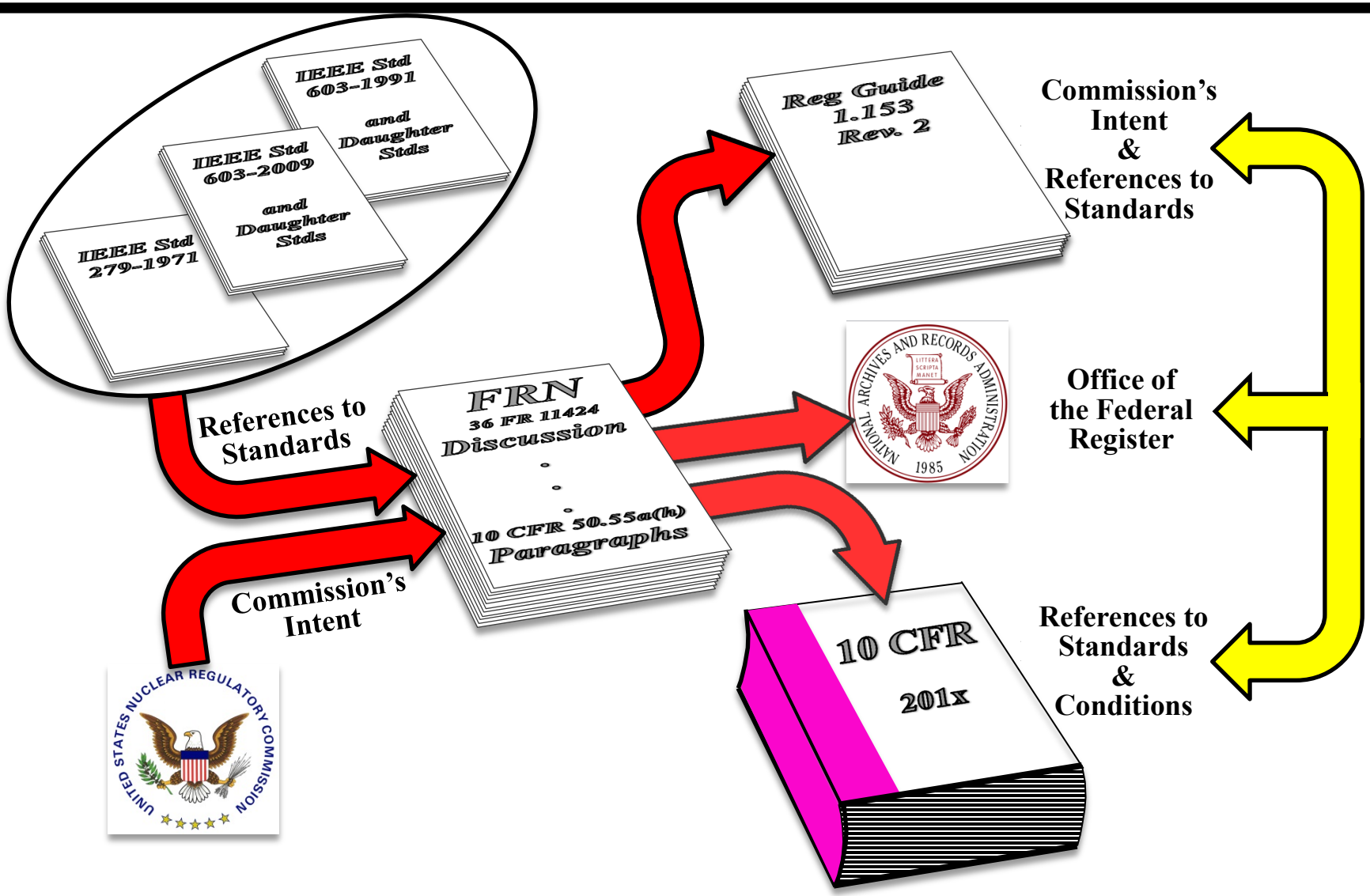
- **Office of Federal Register**
  - **Maintains FRNs on a 20-year rolling basis**
    - **Volumes 59 and later are currently accessible**
  - **Searchable by FRN number**
    - **36 FR 11424 is referenced by 10 CFR 50.55a(h)**
- **Searching for FRN 36 FR 11424 yields**
  - **"It looks like you were searching for the citation 36 FR 11424. We were unable to find any articles with that citation. *FederalRegister.gov* covers articles published starting in January of 1994 (volumes 59-current). Documents published before 1993 (Volumes1-58) are available through a Federal Depository Library."**

Federal Depository Library System

- **Federal Depository Library (FDL) System**
  - **FDL website requires selection of a specific library in which to search**
    - **Libraries include the Library of Congress and Regional Federal Libraries**
  - **The keyword search field does not support FRN number searches**
  - **CFR does not explicitly provide keywords**
  - **The arcane FDL system does not readily reveal the Commission's intentions**

How Can the NRC Better Support the Public, the Industry, and the NRC Staff in Making Available the Underlying Bases of 10 CFR 50.55a(h)?

10 CFR 50.55a(h) and Reg Guide 1.153



Advantages of Draft Reg Guide 1.153 Scope

- Addresses the OFR – FDL System FRN availability issue
  - No time limit on availability of 10 CFR 50.55a(h) underlying basis
- NRC website is the logical repository
- NRC website provides Commission's
  - definitions of terms
  - reasoning behind Rule paragraphs
  - NRC Staff commitment on applying Rule
- Consistent Stakeholder and NRC staff interpretations

Summary

- 10 CFR 50.55a(h) FRN comprises
  Draft Reg Guide 1.153
- Guidance will be consistent with the Regulation
- NRC website will provide Commission's
  - definitions of terms
  - reasoning behind Rule paragraphs
  - NRC Staff scope on applying Rule requirements
- No time limit on availability of 10 CFR 50.55a(h) underlying basis