Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: 616th Meeting of the Advisory Committee on Reactor Safeguards (ACRS)

Docket Number: (n/a)

Location: Rockville, Maryland

Date: July 9, 2014

Work Order No.: NRC-899 Pages 1-194

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

616TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

WEDNESDAY

JULY 9, 2014

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Advisory Committee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2B1, 11545 Rockville Pike, at 8:30 a.m., John W. Stetkar, Chairman, presiding.

COMMITTEE MEMBERS:

JOHN W. STETKAR, Chairman

HAROLD B. RAY, Vice Chairman

DENNIS C. BLEY, Member-at-Large

RONALD BALLINGER, Member

SANJOY BANERJEE, Member

CHARLES H. BROWN, JR., Member

MICHAEL L. CORRADINI, Member

DANA A. POWERS, Member

JOY REMPE, Member

PETER RICCARDELLA, Member

MICHAEL T. RYAN, Member

STEPHEN P. SCHULTZ, Member

GORDON R. SKILLMAN, Member

DESIGNATED FEDERAL OFFICIALS:

CHRISTINA ANTONESCU

WEIDONG WANG

TABLE OF CONTENTS

P R O C E E D I N G S

8:32 a.m.

CHAIRMAN STETKAR: The meeting will now come to order. This is the first day of the 616th Meeting of the Advisory Committee on Reactor Safeguards.

During today's meeting, the Committee will consider the following: the proposed revision to 10 CFR 50.55a(h), endorsing IEEE 603-2009, criteria for safety systems for nuclear power generating stations, Peach Bottom extended power uprate, the draft final design-specific review standard for B&W mPower small modular reactor Chapter 7 on instrumentation and controls, and preparation of ACRS reports.

This meeting is being conducted in accordance with the provisions of the Federal Advisory Committee Act. Ms. Christina Antonescu is the Designated Federal Official for the initial portion of the meeting.

Portions of the session on the Peach Bottom extended power uprate may be closed in order to discuss and protect information designated as proprietary. We have received written comments and a request to make oral statements from Eric Epstein, a member of the public, regarding the Peach Bottom

extended power uprate session.

There will be a phone bridgeline. To preclude interruption of the meeting, the phone will be placed in a listen-in mode during the presentations and Committee discussion. A transcript of portions of the meeting is being kept, and it's requested that the speakers use one of the microphones, identify themselves, and speak with sufficient clarity and volume so that they can be readily heard. And I'd ask everyone in the room to please silence your, whatever sort of electronic devices you have.

As an item of interest for today, we'd like to announce and congratulate Dr. Michael Corradini for being appointed to his third term on the Committee. Please also congratulate Dr. Joy Rempe for being appointed to her second term on the Committee.

(Applause.)

CHAIRMAN STETKAR: We will all appreciate enduring both of you for another four years. And with that, we'll come to the first item on the agenda, which is proposed revision to 10 CFR 50.55a(h). And I'll turn the proceedings over to Mr. Charles Brown.

MEMBER BROWN: Thank you, John. Just one very quick comment is that, as most of you know, we have been dealing with how to apply the existing

regulations and rules to digital instrumentation control systems in both new plants, as well as backfit plants modification. And the staff, over the last few years, has also been looking at the adequacies, or inadequacies I should say, of the existing rule for how it deals with the new technology.

So they have now prepared a revision, a revised rule, to incorporate the latest version of IEEE 603-2009. And they have also incorporated conditions, I think is how you refer to it, conditions into the rule to deal with those aspects of the application of technology that aren't really covered by the IEEE standard.

And so they are here to present that. We've had a subcommittee meeting on it, which was very thorough and detailed, back-and-forth interactions, and I'm sure we will have some more today. So I'll turn it over to, I think, Mr. John Thorp to do the introductions and get moving.

MR. THORP: Thank you, Member Brown, Chairman Stetkar, and other members of the ACRS. Thank you for allowing us -- as well as Christina for arranging our opportunity to be here for the first thing on the agenda. I appreciate that assistance and coordination with us.

Our staff was requested to provide an informational briefing to you, the ACRS, on several topics related to the 10 CFR 50.55a rulemaking effort. We had made a previous presentation on this topic to the subcommittee, as Member Brown referred to, on May 20th. We have several presenters, not as many this time. We have a much shorter time frame in which to try to present to you the essence of this rulemaking.

Rich Stattel on my left will be presenter, as well as Mike Waterman over here on my right on the end, and Terry Jackson from the Office of New Reactors. Mike represents the Office of Nuclear Regulatory Research.

This staff will present the results of an extensive effort by the working group over the last four years to develop new regulations for safety-related instrumentation and control systems. This proposed rule is a preliminary draft proposed rule, and, essentially, it's preliminary draft proposed rule text because we're not presenting the entire rule itself. It's undergoing concurrence reviews by the various offices.

We're prepared to present the contents of this proposed draft rule text and to discuss the rationale used by the working group in its

development. This preliminary proposed rule text includes a discussion section, which includes many statements of consideration. These statements provide an explanation of matters considered during the development of the preliminary proposed rule text. They also provide clarification of what is intended for each clause of this proposed draft rule.

Once the concurrence is completed within the offices, the proposed rule will be made public and will undergo a public comment period, after which the working group will reconvene to address any of the comments received and try to deal with those items.

Next slide. With respect to the agenda you see before you here, this proposed rule would incorporate a voluntary consensus standard, IEEE Standard 603-2009, into the NRC regulations to establish functional and design requirements for power, instrumentation, and control systems for nuclear power plants. The prior standard that is currently incorporated by reference in our 10 CFR 50.55a is the standard from 1991. So it is time, beyond time for us to have updated this.

This action would be consistent with the provisions of the National Technology Transfer and Advancement Act of 1995. That encourages federal

regulatory agencies to consider adopting voluntary consensus standards as an alternative to de novo, or from the beginning, agency development of standards. This action is also consistent with the NRC policy of evaluating the latest versions of consensus standards in terms of their suitability for endorsement by regulations or by regulatory guides.

So moving forward, Rich Stattel will now begin to explain the reasons for changing the rule.

MR. STATTEL: Thank you, John. And good morning, everyone. As John mentioned, one of the main driving forces for this rulemaking activity was the fact that the current incorporated by reference standard has become outdated. The state of I&C technology has changed a great deal since that standard was issued in 1991. There are several design concepts that are being incorporated into I&C systems, particularly for balance of plant applications, such as feedwater control.

The industry has matured and has gained a great deal of experience of using digital I&C systems. The NRC has also raised several concerns over the last 20 years concerning different failure modes of digital systems, particularly for highly-integrated systems in more recent years. The NRC has also raised concerns

over the potential for software common-cause failures or errors that could occur within these systems using multiple instances of software across divisions, safety divisions.

The fact of the matter is very few I&C systems that are being proposed to the NRC today were actually developed using the 1991 standards. Additionally, the working group had identified the need for clarification of applicability requirements based on the experience that we've had with the existing regulations.

The primary objective of the rulemaking activity was to update this incorporate by reference standard to the more recent IEEE Standard 603-2009 version. This standard establishes the minimum functional and design requirements for power instrumentation and control systems, as John mentioned.

There was an intermediate 1998 version of this standard. However, the NRC, at the time, chose not to incorporate that version because the changes to that standard were not considered substantial at that time and the safety benefits of that new standard were not considered significant to the effect of warranting the resources that were required to incorporate it

into regulation.

Additionally, the proposed rule defines conditions which would allow existing licensees to replace plant equipment while maintaining their existing licensing basis. And it defines the conditions for which existing permit, license and certificate, and 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, independence, maintenance bypass, and maintenance of records.

Okay. So what changed in the new standard? Here's a list, as you can see on this slide. And I apologize in advance because I realized after we printed them that the copies that you have don't have the slide numbers on them. That wasn't intentional because my note pages have the numbers on them. So it's just a quirk of the system there.

MEMBER SKILLMAN: John? Excuse me. Rich, may I please ask this question? On unnumbered slide the reasons for rulemaking activity, it's back two, please. My question is have there been any instances where the licensees have used an older standard and,

as a consequence of having used the older standard, created an unworkable or an unsafe system or configuration?

MR. STATTEL: There have been several instances where an applicant used an older standard to develop their system. And what they used is an alternative process. So, basically, there is a clause, which we will talk about at today's presentation, there's an alternative clause that's included in the old regulation and the new regulation whereby an applicant can basically propose an alternative standard through the 603-2009, and then we have a means for reviewing that and approving that.

Now, your question is specific to did it result in an unsafe condition or an unsafe or unapprovable --

MEMBER SKILLMAN: Unworkable.

MR. STATTEL: -- design. I would say, no, we haven't really seen that. The best example I can think of is the Oconee reactor protection system. They actually used the 1998 standard, which, as I mentioned, we never incorporated. But they applied for an alternative, and we were able to review that and accept that system. And we consider that to be a safe system that's operating today.

MEMBER SKILLMAN: And were those changes conducted under their 50.59 process? Is that what --

MR. STATTEL: No, they submitted a license amendment.

MEMBER SKILLMAN: Oh, they did license amendment. Okay.

MR. STATTEL: That's correct.

MEMBER SKILLMAN: Well, actually, they must have done a 50.59 and concluded they needed an --

MR. STATTEL: That's correct. That's exactly right.

MEMBER SKILLMAN: Okay. Hey, thank you. Good, thanks.

MR. STATTEL: Certainly. Okay. So we're now on the current slide that you see here, which is --

CHAIRMAN STETKAR: Oh, Rich? I was reading ahead in your slides --

MR. STATTEL: Okay.

CHAIRMAN STETKAR: -- and, just for the benefit, because Dick raised this one question, could you briefly -- we had some discussion at the subcommittee meeting that the wording of the rule in terms of its applicability, I want to make sure that the members understand exactly to which reactor this

rule will apply because, for example, it will not apply to AP1000. It will not apply to AP600. It will not apply to ESBWR.

MR. STATTEL: I don't think that's entirely true. I think it actually does apply to ESBWR --

CHAIRMAN STETKAR: I, I don't think so. No, it --

MR. STATTEL: Well, I guess it depends, it depends on when the rule is actually issued.

CHAIRMAN STETKAR: Right. But they already have the certified design.

MR. STATTEL: I wasn't aware that --

CHAIRMAN STETKAR: Okay. ESBWR is certified. It will apply -- well, it depends now on when the rule is issued, but it may apply to EPR, US-APWR, and any future designs to come.

MR. STATTEL: That are not yet certified.

CHAIRMAN STETKAR: That are not yet certified. So, for example, plants, even though we don't have an ESBWR on the horizon, and it has substantial back in their digital I&C, they still only have to comply with, I think, the 1991, if I remember correctly, version of the rule.

MR. STATTEL: Right. Now, I will mention

that the applicability of this rule was a major challenge for the working group developing that because we're applying this to operating reactors, we're applying it to 30-year-old plants, we're applying it to new reactors, we're applying it to future reactors.

And particularly in the new reactor realm, and Terry can chime in on this as well, but, you know, the reviews that are in progress, this actually does affect some of the reviews that are in progress. And some of them have been in progress for a number of years, so we're kind of changing the rules on them midstream. But since those design certifications were not issued, this rule, when it gets issued, would apply to them, as well.

CHAIRMAN STETKAR: And it will apply to any future upgrades for existing plants --

MR. STATTEL: Well, we have a slide to talk about that.

CHAIRMAN STETKAR: Oh, okay, okay.

MR. STATTEL: So we have a way -- because that was basically a lesson learned from the existing regulation where we were constantly having debates every time a license amendment would come in about whether or not they had to use the 1991 version of the

standard or whether they could use their existing licensing basis.

CHAIRMAN STETKAR: Yes.

MR. STATTEL: And it wasn't really well defined in the rule, so one of the things that we've attempted to do in this update is provide some definition to applicability. So we have certain criteria we use to determine the applicability of this standard. And that's mainly aimed at the operating plants.

CHAIRMAN STETKAR: Okay.

MEMBER BROWN: I want to make one observation for the members relative to your comment. Now, when he says they looked at it, there is a multi-page inclusion in the rule that goes through about every if, then you can imagine, in terms of, even back to 279, and who and who shot John and everything. No pun intended there, John.

So, I mean, it is a very extensive evaluation of all the old plants' potential modifications, who should do what. It's very, very thorough. At least in my opinion, it was. I'm not good at some others, but it was a lot of writing. So, anyway, it is well covered.

MR. STATTEL: Okay. So in the development

of this rule, the working group evaluated and compared the new 2009 version of the standard with the 1991 and the 1998 version, and this slide summarizes the changes to that standard that the working group identified.

Now, what I'm going to do next is I'm going to explain each one of these seven items in a little bit more detail. Okay. The first item, this change was included to address the introduction of digital components, such as field-programmable gate arrays or computer-programmable logic controllers technologies into I&C systems at nuclear power plants. Back when computers were first being introduced to the industry, the IEEE had decided to develop a separate standard as a companion standard to provide guidance for digital computer-based systems. Instead of including -- they did that, instead of including the technology-specific guidance, in the 603 standard itself.

In 1991, that standard, which is IEEE 7432, at the time it was 1982 version, was generally referenced. However, no specific topical references were included in the old 603 standard. In 1998, specific sectional references were added to the 603 standard, and that's basically the gist of that

change.

Okay. The second change involved, in the new version of the standard, it updated the entire list of reference standards. This is basically a standard practice by the IEEE working group. They do that every time they update one of their standards.

Since the reference standards are not considered by the NRC to be incorporated by reference into regulation, these changes were not considered by the working group to be technically relevant to the IBR rulemaking process. Instead, the NRC does endorse many of those standards that are referenced, but we do it through our regulatory guidance.

Okay. The third change occurred during the 1998 revision of the IEEE 603. A new informative annex titled "Electromagnetic Compatibility" was added to the standard. Now, the NRC does not endorse this informative annex. Instead, electromagnetic compatibility, or EMC, has been addressed by a separate reg guide. That reg guide is Reg Guide 1.180, which is titled "Guidelines for Evaluating Electromagnetic and Radio Frequency Interference in Safety-Related Instrumentation and Control Systems." And that endorses several other standards.

Okay. In 1998, a new section, 5.16, was

added to IEEE 603 in attempt to address the criteria for software common-cause failure. In actuality, the added clause does not introduce any criteria at all. Instead, it referred to IEEE 7432, the companion standard, and it states that the reference standard provides guidance criteria in this area.

Now, though the NRC does endorse 7432 via Reg Guide 1.152, the NRC does not consider the guidance within 7432 to be complete or adequate for addressing common-cause failure. Instead, the NRC refers back to the staff requirements memorandum that was issued against SECY paper 93-087 via the standard review plan guidance and Branch Technical Position 719 for its evaluations of software common-cause failure susceptibility. Additionally, I'll discuss NRC position on this particular topic in greater detail when we get to the conditions that we included in the rule.

Okay. Number five. So there are some numbers on this slide that help keep us inline here. This section of the standard was enhanced to provide additional guidance for maintaining independence between safety systems and support systems, and that includes those which are classified as non-safety related. The revised section expands on the concept

of associated circuits, and it provides guidance criteria for establishing necessary independence between these systems.

Now, for the most part, the NRC doesn't take exception to any of that enhancement language that was added to the standard. However, we decided to add some conditions for independence, and we'll cover those separately.

Okay. Number six. The standard requires system surveillance testing to be performed periodically to ensure safety functionality during plant operations, so it is necessary for licensees to be able to bypass or prevent safety system actuation during maintenance activity. The purpose of this clause of the standard is to establish performance criteria for situations requiring systems or portions of systems to be in a bypass state. It requires the safety system to retain its capability of performing the safety functions while those 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. The exception clause identified conditions where certain portions of the safety system could be tested or placed in maintenance

bypass without satisfying the criteria of the preceding clause.

The next two slides show the exact text of this exception clause. And so what it is is the first slide shows what the 1991 version says, and if you flip to the next slide -- I'll kind of go back and forth -- you can see what words change. So they changed a "shall" to a "should." You can see that. And they changed the exception to a note, okay?

So when IEEE revised the standard, this exception was determined to be contrary to IEEE policy. So, basically, their policy, the IEEE policy is that a requirement isn't really a requirement if there can be allowable exceptions to it.

To address the policy, the standard working group changed the "shall" to a "should," which effectively changed the requirement into a recommendation. This exception clause was also re-worded and re-titled as a note, as indicated on these slides.

MEMBER SKILLMAN: Rich, back one, please, to the next to the last line on that slide, "to ensure there is no significant detrimental effect on overall sense and command." To go into bypass, maintenance bypass, that's normally an I&C function. There's no

procedure. It's conducted through work control. But I can imagine a shift manager saying, "I give you permission to go into maintenance bypass because I don't think that there's any significant detrimental effect." How is significant detrimental effect interpreted?

MR. STATTEL: I think you need to take the entire clause into account. There was a slight re-wording on that.

MEMBER SKILLMAN: Yes, I did. And I've seen words like this before that become, in all candor, the name of the game. A smart operator is not going to take the plant at risk. But someone who's clever and trying to get done before the shift ends just might go down and say, "Hey, you know what? I don't think there's any significant detrimental effect. Let's do it."

MR. THORP: So the logic of the phrase that I'm seeing is that the removal from service for maintenance bypass, the time period allowed for that is sufficiently short to ensure there's no significant detrimental effect on overall sense and command feature availability. And, oftentimes, there's also guided by the presence of technical specification limiting conditions for operation that provide a time

limit for how long you can be in maintenance bypass. The plant that I worked at, it allowed a 48-hour time frame for troubleshooting and maintenance bypass; is that correct?

MR. STATTEL: That's correct.

MR. THORP: Yes. So this, in systems that we're talking about here, like reactor protection system, engineer safety features, we're talking about pretty carefully controlled procedures and technical specification controls. So I think, in theory, your position is clear and well taken, but I don't think that's a big vulnerability post here.

MR. STATTEL: Also, this clause is really not a normative clause. It's really just providing an example. But, yes, it would be our expectation when we're evaluating these systems and how they're operated that they wouldn't use this kind of rationale for, for instance, bypassing a safety injection function in anticipation of an event that could challenge that function.

MR. THORP: Or to do so for some lengthy period of time.

MR. STATTEL: Right.

CHAIRMAN STETKAR: I mean, in principle, the tech spec should cover you. This specifically

applies to one out of two, so it could be either one out of two, you know, if you only have a two-train output --

MR. STATTEL: That's right.

CHAIRMAN STETKAR: -- or it could be one out of two input signals to reactor trip, like source range or intermediate range flux, you know, which are typically one out of two instead of two out of four. The tech specs should have you covered on the output because it shouldn't allow you to take both trains of your safeguards actuation or reactor --

MR. STATTEL: Well, most of the functions of reactor protection systems and SFAS systems are basically performed by the four divisions or four channels of instrumentation. And, therefore, taking one of those channels out and going to a two out of three, I mean, that's what the main --

CHAIRMAN STETKAR: That's what the main clause is.

MR. STATTEL: -- but really just, as a result of just having, basically, those functions filter down after the voting when you get down into the voting and the actuation of components, you know -- for instance, most plants only have two trains of safety injection.

CHAIRMAN STETKAR: Right.

MR. STATTEL: So you get down to two --

CHAIRMAN STETKAR: That's right.

MR. STATTEL: You get down to two components sooner or later, and really what this exception is intended to address is how do you make sure you maintain the operability of those, you know, that limited set of electronics that is actuating those components on the two-channel system and still maintain your safety.

MEMBER SKILLMAN: Yes, I was really thinking about a pre-GEC plant that's, at least on the surface, very central. But it turns out, in its simplicity, the fact that they only had one last man standing becomes the most important thing that they have in the plant, and if they defeat it then they are probably where they're not supposed to be. And I agree with John. Tech specs probably --

CHAIRMAN STETKAR: Tech specs --

MEMBER SKILLMAN: This allows them to go into that status. I got it. But this wording can be, can be gamed. That's the point I'm making.

CHAIRMAN STETKAR: Or if it does -- I've seen plants that do but they give you a specific, you know, one hour, or they specify. Whether that's

sufficiently short to have no significant detrimental effect is a different issue, but the tech specs, if they do allow you to get into a severely degraded state, typically do specify a time frame.

MR. STATTEL: Yes. And I want to make clear that the clause does not allow them to defeat the safety function for any amount of time at all. What it allows is for them to take one of those two trains out of service. The other one is still performing, capable of performing that safety function, but there's no, it doesn't meet single failure criteria, for example. So if a failure were to occur that disabled that one train, then you wouldn't --

MR. THORP: Suffer that loss.

MR. STATTEL: Right. So in other words, you know, we don't want them not to test those two-channel portions of the system. We want them to test them, and we recognize that there are cases where, you know, you just have a limited amount of redundancy, so there's really no other alternative other than to be able to bypass one, test it, and then put it back in and bypass the other one. So it just allows for that reality.

MEMBER BROWN: Rich, my memory is failing

me right now. This is the IEEE 1991 version.

MR. STATTEL: That's correct.

MEMBER BROWN: The words and the exception that's in 1991.

MR. STATTEL: That's correct, yes.

MEMBER BROWN: In 2009, the standard was changed, not by you all but by the IEEE, to the "should" and the changed exception.

MR. STATTEL: Should and note.

MEMBER BROWN: And the note. Well, but the note was there -- yes, as a note, as opposed to an exception. Now, my memory is failing me in that I thought you all took issue with that relative to a condition.

MR. STATTEL: Well, it was not -- we did not address that as a condition. What we did -- we don't agree with the softening of the requirement.

MEMBER BROWN: Yes, but that's, you said that in the new rule.

MR. STATTEL: Right. So the new rule states --

MEMBER BROWN: I didn't hear you say that --

MR. STATTEL: That's my next sentence.

MEMBER BROWN: Oh, I'm sorry. I

apologize. I didn't see it on these pages, and I just wanted to make sure -- so go ahead.

MR. STATTEL: So the new proposed rule states that the criteria for the 1991 standard, the old standard, should be used in lieu of the new clause 6.7. And that's to clarify the requirements for the use of maintenance bypass. So, essentially, if the rule gets issued as proposed, the 1991 version of this clause becomes the operative clause.

MEMBER BROWN: You got that, Dick?

MEMBER SKILLMAN: Yes.

MEMBER BROWN: You had a big question. I just want to make sure to get that across. They wanted to retain the rigor of the old rule.

MEMBER SKILLMAN: What I'm taking away is the revised standard retains the requirement for defense in depth.

MEMBER BROWN: The rule, yes, brings that back.

MEMBER SKILLMAN: And when going into maintenance bypass, the final safety function has not been defeated. The redundancy has been reduced, but the function has not been. So I understand.

MR. STATTEL: That's correct.

MEMBER SKILLMAN: Thank you.

MR. WATERMAN: This is Mike Waterman. Just one clarification. Rich, if you could go back to the note.

MR. STATTEL: Which version do you want?

MR. WATERMAN: This one right here.

MR. STATTEL: Okay.

MR. WATERMAN: In IEEE standard space, notes are not normative. In other words, if somebody claims compliance to IEEE Standard 603-2009, they don't have to be in compliance with that note because that note is not a normative requirement. So even though there's a "shall" down in that note that makes it look really strong, it's not strong at all because the note is not what we call normative. Just to comment -- claiming compliance for 2009 does not mean compliance for that note.

MEMBER SKILLMAN: Thank you.

MR. STATTEL: Okay. And the last change, number five. This clause was added to the standard and to introduce technology-specific guidance for communication independence. It was a departure from the IEEE's earlier position to place such guidance in the companion standard, and we'll have a more detailed discussion later in the presentation about this. But you can see the sections affected and the change

that's being made on this slide.

Okay. Now, the next part of the presentation I'm going to discuss how the rule is addressing those seven changes that were made to the standard. I'll also discuss several conditions, several of the conditions that are being proposed in the new rule.

Okay. For the context of this rule, there are several terms that are defined in the Federal Register notice, the statements of consideration. This was done to provide a common understanding for each of the terms as they are being applied to the different standards being referenced by the CFR. It is intended that these definitions be applied by the NRC for the underlying basis of 50.55a(h). Some of these terms are being introduced by the rule. These terms are, those terms are bolded in your handout.

The rest of the terms are used within the reference standards. However, the working group, as we were reviewing the documentation, we recognized that the definitions in the standards are not always consistent. So we decided to provide a common definition within the rule package to avoid ambiguity.

MEMBER BROWN: Are the non-bolded ones included in the rule, or are those just in the RG

1.153, the associated reg guide?

MR. STATTEL: They are included, they're not, they were not defined prior to this rulemaking.

MEMBER BROWN: No, I understand that. I understand that.

MR. STATTEL: They are included in the statements of consideration --

MEMBER BROWN: But that's in the FRN.

MR. STATTEL: In the FRN, yes. They're not going to show up in the Code of Federal Regulations.

MEMBER BROWN: So how does the FRN apply relative -- so you want people to use those as common terms. If they're just in the FRN, how does that get translated to the future? I didn't ask that question in the subcommittee meeting.

MR. STATTEL: Correct me if I'm wrong, Mike, but I think those definitions will be transferred to the reg guide.

MEMBER BROWN: I thought they were.

MR. WATERMAN: I think all of those terms that are defined in the FRN are used in the rule language.

MEMBER BROWN: Yes, but the definition is what I'm interested in.

MR. WATERMAN: Because those terms are used in the rule language, we felt it necessary to let the stakeholders know this is what the Commission intended to mean when they --

MEMBER BROWN: That's FRN. That's the FRN.

MR. WATERMAN: That's the FRN.

MEMBER BROWN: Are all of these included in your RG 1.153 associated explanation of the new rule?

MR. WATERMAN: As far as I know they are.

MEMBER BROWN: I thought they were.

MR. STATTEL: I'm pretty sure they are because they're --

MEMBER BROWN: I looked at it. You had a list of definitions, but I didn't go count every one.

MR. WATERMAN: If they're in the FRN, yes.

MEMBER BROWN: Okay.

MR. STATTEL: They're in the glossary portion of the draft reg guide.

MEMBER BROWN: Okay, okay. The FRN will get lost in a few years. It's not in the Code of Federal Regulations. I'm happy. Just go on.

MR. STATTEL: Okay. I know this slide is a little busy, but it's really just a copy of a page

from the statements of consideration. The backfit analysis that was performed for this rulemaking activity determined that the application of this 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 such as the introduction of digital technology into I&C safety systems.

We created this table, and there's corresponding language that goes with this that's included in the statements of consideration, to better define and clarify the applicability of the standard. The previous date-based applicability clauses were left in place, and that was in order to maintain the existing design basis for current licensed operating plants. These conditions are based on the issue date of the plant's construction permit, standard design certification, or manufacturing license.

A new set of criteria was then added to define the applicability of the 2009 standard criteria, including the conditions that are implemented by this rule. The rule also allows voluntary application of the new standard for previously-licensed facilities.

So someone can always choose to use the newest standard instead of the license basis standard for the associated plant, okay?

MEMBER POWERS: I mean, they can't make exotic decisions to switch standards.

MR. THORP: You mean one week to use the new standard and then the next week to harken back to the old one.

MR. STATTEL: No, that's not the intent. So, basically, it's forward-looking. We consider the new standard to be perfectly adequate and appropriate to apply to an analog system, for example. So if someone chooses to upgrade their analog system and they want to use, they voluntarily want to commit and use the current-day standard to develop that system, they're able to do that. They're not required to because we're not applying this as a backfit to them, so we're not making it mandatory for them to use the new standard for an older plant, for example. But they can voluntarily use the newer version of the standard.

Now, what this table identifies is certain conditions, depending on the nature of the change that they're making to their design, there are conditions that would basically -- if you're changing from analog

technology to digital technology and you're adding new safety functions that were not part of the original licensing basis for the plant, well, then we would expect them to use the new standard for the development of that system.

I think the next table also goes into a little bit better detail about that. Okay, yes. So this table, it kind of works with the previous table. This is also in the FRN document. It basically provides several examples of I&C system modifications, and this is intended to aid in the determination of the applicability for the new standard.

So as you can see on the table, if all they're changing in their system is updating their power supplies in one division, then really there would not, the expectation is they would use their initial licensing basis as a minimum and that they would not be required to use the 2009 standard. However, if they're modifying the protection system with components based on, they're changing their technology, then we would expect that they would use the 2009 version of the standard.

Any questions on that? Okay.

Now, these listed clauses --

MEMBER BROWN: Let me ask you a question.

I might be way off base, and this is just based on a recent experience that -- talk about the first item, the power supply. There are power supplies that incorporate computer software-based components to monitor their functionality, as well as to be smart.

MR. STATTEL: Yes.

MEMBER BROWN: So that's not exactly an analog type situation.

MR. STATTEL: That's correct. And that's an issue we've kind of coined the term "embedded digital technology." And it's something the IEEE is actually working on, developing a new standard to address those types of issues to basically identify what criteria would need to apply for that.

Our intention here would be, yes, that's a change of technology. If you're adding computer control function into a power supply, it's no longer using the analog technology. So our intention here, my interpretation of that and certainly the working group's intention would be that they would have to use the new version of the standard.

MEMBER BROWN: Okay. I just wanted to provide that just to make sure I understood a little bit of your thought process. That's fine.

MR. STATTEL: Okay.

MEMBER BROWN: Thank you.

MR. STATTEL: Okay. So the next part of the presentation is talking about what's actually changing in the regulation, okay? This slide lists the clauses, and these clauses would add conditions. So, basically, we're endorsing or incorporating by reference the new version of the standard with all the changes that I just went over. In addition to that, these listed clauses would add conditions and several new requirements for the use of the 2009 version of the standard.

So we'll now discuss each of those clauses individually. Okay. The first one is to amplify system integrity requirement of IEEE 603. This new clause would require that, in order to ensure the integrity and reliable operation of a safety system, the safety functions shall be designed to operate in a predictable and repeatable manner. And we also added definitions for those terms, okay?

Predictable and repeatable operation of the system requires that the results of translating input signals to output signals are determined through known relationships among the control system states and the 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 design basis.

Predictable and repeatable systems do not provide the capability for unscheduled event-based interrupts or operator system interrupts to meet system safety requirements. Systems that operate in a predictable and repeatable manner should not be designed with a capability for unscheduled event-based disruptions or operator-based system functions that would inhibit or prevent the safety system from meeting its safety requirements.

Any analysis used to demonstrate predictability and repeatability should be based on analysis of system characteristics, such as definitive design and performance criteria as opposed to a probabilistic analysis.

Okay. The next section of conditions is for independence, and I will --

MEMBER BROWN: Can I ask you a question on this? Those words will be, that's the H4 words that will be in the rule? All the other words you read are in the reg guide?

MR. STATTEL: Verbatim. Word-for-word, what you said is correct.

MEMBER BROWN: I want to make sure that

you understood. Those are the words that will be here. What they intend is now in this new reg guide, which goes through every item in the standard, in the rule -- excuse me -- and explains what they mean by the condition. We didn't have that before, did we?

MR. STATTEL: No. Yes, this clause did not exist.

MEMBER BROWN: No, no, no, I mean the companion explanation of the reg guide.

MR. STATTEL: Well --

MEMBER BROWN: But there wasn't, there weren't any of these conditions in --

MR. STATTEL: It technically existed, but it was kind of buried in the statements of consideration for the old rule --

MEMBER BROWN: Okay.

MR. STATTEL: -- which is very difficult to find and it's not, it's not really an operative guide. So practically speaking, a reviewer, an NRC reviewer would have, there was nothing in the standard review plan that would tell him to go look at that. Now, he could, but there's nothing that obligates him to go look at that, what was intended --

MEMBER BROWN: But now you've covered that omission. Well, not omission but that lack of

information.

MR. STATTEL: And that's our idea. So our idea here, as a practical matter, so the future reviewer, as he's reviewing a design, he will be pointed to the reg guide because the standard review plan will point directly to the reg guide, and it will have -- all the words that I just read will be right in there. So there should be really very little left to interpretation at that point. So the rule language is here and how that's interpreted, how that was intended to be interpreted will be contained within the guidance --

MEMBER BROWN: I just wanted to make sure of that because you went through that whole litany, and I wanted to make sure people understood that that explanation was not there. It's just in this part.

MR. THORP: So this process and this concept includes a contemporaneous development of the reg guide and issuance of the reg guide in parallel with the rule. So that will be available.

MEMBER BLEY: A question about that kind of structure. I'm asking it for response from you guys as member of staff but also some of you have worked for power plants, as well, and from them. In trying to delve into issues in other areas like this,

if I talk to lawyers here, they go to the statements of consideration immediately and they know what those are, and they do provide much depth behind the things we have.

Does staff refer to them as -- are they as conversant with them as I seem to see with the lawyers? And are the folks out at the power plants at all conversant with statements of consideration?

MR. STATTEL: Well, I'll be honest with you, you know. I was at the power plant for 20 years. I didn't know they existed.

MEMBER BLEY: That's kind of what I --

MR. STATTEL: Until I came to the NRC, I did not know they existed.

MEMBER BLEY: So this is a really good idea, and not just here. Maybe some other areas --

MR. STATTEL: Now, the reg guides, I knew they were there. So I knew, when I submitted an application, I knew that the NRC reviewer was going to be using the criteria in that reg guide to evaluate my system. So, of course, I'm very cognizant of what's in the reg guide, but statements of consideration I had no clue. I learned of their existence the first year I was at the NRC.

MEMBER BLEY: So at least on staff you're

aware of them.

MR. STATTEL: Oh, I am aware of them now. The lawyers made sure of that.

MR. JACKSON: For the inspection staff, they're aware of the statements of consideration. They'll refer to them, but it's not very often that you would need to refer to the statements of consideration.

MR. THORP: When there's a question or a controversy of some kind, you know, that has to be examined in further detail, that's when they'll dig into things like this.

MEMBER BROWN: One other -- this reg guide, it was a very good idea to do this. I think it's very extensive, very thorough, and it really does explain the intent behind what the staff is trying to do and it really delves into the application of the new technologies. So I think it's a personal opinion. I used it extensively during my, during my review.

MR. STATTEL: But it's a very unique reg guide because our normal practice is the reg guide would endorse a standard as a guidance, as a measure of guidance. When the working group convened, one of the first questions that came up is why do we even need a reg guide because this is regulation. You

know, what's in this standard is regulation. It's incorporated into the CFR. But after reviewing that, we felt it was necessary to have the reg guide clarify that.

MEMBER BROWN: Okay. Let's go on.

MR. STATTEL: Okay, certainly. So for the independence part of this presentation, I will turn over to -- Terry Jackson will be presenting these criteria.

MR. JACKSON: Okay. So I'm going to talk about the criteria that's in the proposed rule, 10 CFR 50.55a(h)(5). So if you're following along in the Federal Register Notice, it's about page 71.

CHAIRMAN STETKAR: Yes, we're all doing that, Terry. Don't worry.

MR. JACKSON: So this section here on the independence, there's three subparagraphs that provide additional criteria on independence. This slide here is going to talk about the two general requirements that apply overall, and then there's some detailed criteria which I'll talk about on the next slide.

Clause 561 of IEEE Standard 603 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.

So the first subparagraph there, 5(I) amplifies clause 561 by requiring that applicants address independence between redundant portions of the safety system and, further, that hazards introduced into the safety system by information sharing must be analyzed. And the second subparagraph there also amplifies clause 563 by requiring that applicants address independence between safety systems and other systems and that the independence must be analyzed for hazards by such information sharing.

So, basically, what these two subparagraphs are doing is, one, they're requiring, they're making more explicit that there should be analysis when you're doing communication between redundant safety divisions or between safety systems and non-safety systems. And that analysis should cover, as a minimum, the safety system internal/external hazards, the extent of interconnectivity that is in the design, as well as what the impact of failures of degradation are.

And then one of the other things that, particularly 52 covers, is that digital communication

independence is extended to include other signal technology. So in the 2009 version, they put in there digital communication independence, and we expanded it to be any kind of communication independence independent of technology.

Okay. So on this next slide here, we're going to try to illustrate the detail of the criteria, which is in 5.3. And first of all, what we'll be talking about is the --

MEMBER BROWN: 5.3 or 5.63?

MR. JACKSON: Actually, it's in the draft rule. It's paragraph 5 --

MEMBER BROWN: Oh, a little after it.

MR. JACKSON: A little after it.

MEMBER BROWN: Okay, all right. I'm sorry. I was thinking of the standard.

MR. JACKSON: So we're talking about independence between safety division or safety systems and also between safety and non-safety systems. And, first, there is criteria which is in big letter A there in that subparagraph which describes criteria that applies to all reactors. And what this does is paragraph 5IIIA allows communications between the safety division or safety system and other safety divisions and safety systems and from non-safety

systems into the safety division or safety system, provided safety is not impaired.

MEMBER BROWN: And that's what the arrows mean?

MR. JACKSON: Yes. So, basically, what it's describing there is new communication direction. So you could have communication basically between redundant safety divisions, you could have communication from a non-safety system in this clause here particular. But you kind of have to take all the clauses together and for what particular reactor, which I'll describe the other ones coming up, as well.

Now, big letter B requires features in the safety division or safety system for detecting and mitigating faulted signals from another safety division or system and faults from non-safety systems. So, basically, this is having some kind of diagnostic feature on communication system that can alert you to communication failures.

Okay. So big letter C within that same subparagraph allows signals from other safety divisions or safety systems and from non-safety systems if those signals support safety or benefit safety, in addition to paragraphs A and B. So right here, this is not just only including if you need it

to perform a safety function, but if it would provide safety in terms of enhancing reliability and availability, then it could be allowed.

CHAIRMAN STETKAR: Terry, we had a little bit of discussion on this one at the subcommittee meeting. And, in fact, I can't recall the design; it doesn't make any difference. It's come up in some of our discussions with reviews of -- as I said, I can't remember whether it was a new reactor or an upgrade and it doesn't make any difference -- where there's a danger that reviewers may interpret that requirement very, very literally, to the extent of prohibiting communications that might enhance operator reliability but cannot be demonstrated in a deterministic licensing basis as an improvement to safety because they don't enhance any of the safety-related functions. And that's a bit of a concern if the staff is going to interpret that support or I think the words are provide a safety benefit very, very literally.

We did have some discussion during a subcommittee meeting, but I guess I'd like you to address it. In particular, the example that I seem to recall, and I couldn't find it very quickly searching through my notes here, was something where an

applicant or a licensee said we would like to have these non-safety related signals available to operators on a safety-related display because they told the operators an integrated picture of the status of safety and non-safety systems, and the staff disallowed that because they said that is not a distinct safety benefit.

MR. JACKSON: Okay. That one there, I'm not familiar with that --

CHAIRMAN STETKAR: And I can't find it. I recall it because I remember during our deliberations we had some discussion about it.

MR. STATTEL: Well, our experience, and, you know, we've been working with NRO pretty closely as we develop this, our experience with the reviews has been very different for the operating plants versus the new reactor designs. It's actually a lot easier for the operating plants to make safety cases because they have like a baseline. So, relatively speaking, it's pretty, it's pretty easy or there's a success path for showing that a new design with new features actually provides a safety enhancement, and that's pretty quantifiable.

For the new reactor designs, they're pretty much establishing that baseline safety case,

and they have nothing to compare it against. So it's a lot more challenging for the new reactor designs, and that's part of the reason why we separated the requirements applicability for new and operating reactors.

Now, we did attempt to define what a benefit for safety was. The concern there was we didn't want to have disagreements, so an applicant could think it's a safety benefit and then the NRC reviewer would say, no, I don't think that's a benefit at all.

CHAIRMAN STETKAR: Yes. That's the type of discussion I recall.

MR. STATTEL: The type of benefits that we've seen in the operating plants for Oconee and for Diablo Canyon have been basically reducing reliance on operator actions, right, is one of them. We also see benefits, we've credited benefits for diagnostic features that basically identify faults in a system immediately, instantaneously when they occur, as opposed to the traditional way in operating plants, in the old analog technology from the 70s and 80s, it's very typical we have a surveillance test that we perform once a month or once a quarter. And, realistically, a fault can occur any time during that

quarter, and you don't have a means of identifying that until the end of the quarter. So having the ability to immediately identify a fault in the system really does provide a safety benefit there, and we've basically credited applications for those types of benefits, as well.

But we do review them, and they really have to be case by case. You know, we definitely have discussions with all the applicants with regard to is this a feature of the system, is it a benefit or is it just something you'd like to have, and we do evaluate them on a case-by-case basis.

MR. JACKSON: I think, overall, this was a challenging area in drafting rule language, and the challenge is is that digital technology brings a lot of benefits. There's a lot of functionality that you can bring to a system through using digital technology. But also you have to recognize that, due to its complexity and some of the interactions and stuff, there could be challenges to things, particularly with independence.

So you've got a kind of balance here of where you're trying to -- you want this nice functionality, but you also want to be able to ensure safety, as well. So you want to try to maximize the

ability to have this functionality but also minimize the risk of using certain design features, particularly with independence, which is kind of a good segue with what I'm going to talk about with new reactors because the next set of criteria that you'll see are, basically, they're consistent with what is in A and B, but they're more strict that you'll see.

So the first one here is that -- okay. So in (D)(1), this requires communications between the safety system and non-safety system shall be one way and enforced with a hardware device when the safety system is in operation. So, basically, what this does is this would allow communications from a safety system to a non-safety system. So, for example, if you want to send diagnostic information or information to the operators, you're still able to do that. But at the same time, it's blocking any kind of challenges you might get from a non-safety system failure back to the safety system.

And then in (D)(2), what this is saying is that it allows communications between a safety division or a safety system if those signals are required for safety. So, primarily, we realize that you'll need to do voting and certain things like that. So that provides that provision there.

MEMBER BROWN: Before you leave that, I mean, we've had considerable discussions in all the new reactor designs and others on relative to the sharing because of the voting issue. You obviously have to vote, and the concern of corrupt digital signals locking up or making non-operational all the voting units simultaneously since you have to obviously feed from one division to all voting units in order to do the voting. And I noticed you didn't, there was no explicit discussion of a diverse means of monitoring the processors for lockup such that -- and that's not covered by the analysis of serial data or any other communications type data. It's a functionality or a -- what I want to call it is a characteristic of computers to get confused and stop.

You have not addressed that in the new rule or in the conditions you've applied, yet we've utilized that and it's gone, you know, moved heaven and earth to try to get that across in all the new reactor designs, as well as to understand -- well, we actually haven't had a backfit where we've had to do that, at least not recently. I can't speak to Oconee because I just don't remember back six years or five years, whatever it was. I can only remember the Diablo Canyon routine where it, fundamentally, was an

analog signal that goes out to the analog voting unit.

So, anyway, you're not covering it here, and what's the rationale for not dealing with that now in the new rule since you had the opportunity?

MR. JACKSON: Okay. I think I'll take a shot at it and then ask Mike and Rich because they were more involved with the working group than I was. But I think the working group discussed that particular aspect there of having, basically, a hardwired way of --

MEMBER BROWN: A hardware-based monitor at the same time.

MR. JACKSON: Yes, ensuring that if a voting process are locked up that you would still get the reactor trip function.

MEMBER BROWN: Or a safeguards alarm, one or the other, just depending on the functionality.

MR. JACKSON: So I think when we looked at that, the group saw it as a very, I guess a very specific criteria, which we feel is covered by, for example, review system integrity. And that's one of the reasons why the system integrity clause was enhanced by the condition to be predictable and repeatable.

MEMBER BROWN: But that's if it's working.

MR. JACKSON: Right. But we didn't -- I think what we saw in the rule is that would be a very specific criteria there. We feel that the rule addresses the ability that it needs to operate with integrity and reliability but not the need necessarily to spell out a specific function.

MEMBER BROWN: Well, that's not a specific function. If you require it to be monitored, it's like anything else that you monitor. Well, go ahead.

MR. JACKSON: Well, I think some of the other thoughts, too, is that if you lost the ability, say all the voters lock up, that this is also similar to the common-cause failure, which is also addressed in the rule, as well. So you may have a diverse actuation system that is also going to provide a protective function.

MEMBER BROWN: Many folks don't recognize that as a common-cause failure. They don't recognize that it will even occur ever.

MR. JACKSON: Right. But we assume --

MEMBER BROWN: It's a little difficult if --

MR. JACKSON: Yes, I think --

MEMBER BROWN: -- if you've got a mind set out in the design world that says, well, you've got to

be kidding me, this never happens.

MR. JACKSON: Well, when they're doing their defense in depth and diversity analysis, they have to assume that the safety function doesn't occur from the primary system. So that could be failure to provide a reactor trip if one is required or a safety actuation if one has occurred.

MEMBER BROWN: Yes, but the diversity -- just to be contrary a little bit. Based on -- well, I want to make sure we mouse milk this to the nth degree here. If you look at some of the applications we've looked at in the new reactor world, there was not a one-for-one mapping of safety requirement, in other words trip functions, into the diverse actuation systems. They were based on a probabilistic risk assessment of the need for certain -- whether manual operations could take care of this or that. So there is not a one-for-one translation into the diverse actuation system evaluations. So, I mean, to use the diverse means, you know, that people do do is not a complete affirmation or solution to that particular circumstance.

All right. I got your answer. I just wanted to make sure we discussed that point since we've been over it fairly well in a number of the new

reactor designs. We will have to evaluate that --

MR. STATTEL: I would like to chime in here. So it kind of comes down to how prescriptive we need the regulation to be. For new reactors, in the proposed rule, we actually do put some restrictions. The voting function, for example, on new reactors per the new rule condition here cannot be done through communications at all. It has to be hardwired, basically relay type logic for transferring signals between the channels and the voting.

MEMBER BROWN: Where does it say that in here?

MR. STATTEL: That is actually in, for new reactors it's in clause III --

MEMBER BROWN: (D)(2)?

MR. STATTEL: D -- let's see.

MR. JACKSON: I think we required a hardwired --

MR. STATTEL: (D)(3), I believe it is.

MEMBER BROWN: It's only (D)(I) that says communication for safety and non-safety much be one way enforced by physical mechanism for safety to non-safety. It doesn't say from safety to safety.

MR. STATTEL: Yes, we would allow data communication for communication between --

MEMBER BROWN: From a safety processor that's calculating a trip, you would allow serial communications to a computer-based voting unit that takes data and evaluates it with headers and footers and all the other junk that gets tossed in to make it communicate with the other processors. So I don't think that's the case.

MR. STATTEL: Now, the other thing I'd like to point out, I think Oconee was a good example because in the Oconee system there was two different setups, one for the SFAS. They actually had computer-based voters, and there were two of them. In the (D)(3) analysis, which it kind of does provide a one-for-one comparison between the design and what the expectations are. The assumption was that both of those voters were to fail and freeze up, and the concern was not that we would have inadvertent actuations but that you would lose your safety function. It actually goes both ways.

For Oconee, they actually, for that system, they put in an emergency override switch. So, basically, they cut power. They just turned the computers off. And that was -- they would only do that -- it was manual. It was a manual switch --

MEMBER BROWN: You had to know what

happened while you're going through a casualty --

MR. STATTEL: Well, essentially, so it's a scenario where I have a safety injection, a high-pressure safety injection in progress. My pressure is going up, my voters are failed, I can't stop the injection.

MEMBER BROWN: How do you know your voters have failed?

MR. STATTEL: So, basically, the procedures were written in a way where the operators confirmed that they didn't have a condition where they required the safety injection and they could operate that emergency override switch that basically killed power to the computers. Now, that was for their SFAS system.

For their reactor protection system, they basically used the old relay logic, so there was no communications to the voters. The Oconee system uses relay logic, and there was really no --

MEMBER BROWN: There were five stable outputs out of the calculation unit into a voting, multiple voting --

MR. STATTEL: Right, it was a matrix. It was a standard matrix.

MEMBER BROWN: Well, that's a way to do

it, but they didn't have to do it that way. They could have used --

MR. STATTEL: Correct. And the reason I say that's a good example is because it shows you that there are more than one, there's not only one technological solution to --

MEMBER BROWN: Oh, Rich, I'm not disagreeing.

MR. STATTEL: -- technological solution to that problem. I think the rule establishes the performance and operational expectations for the system, and we don't want to restrict, you know, to one solution. That was not our intent. So we were very careful to basically define the criteria, the expectations, the goals that need to be met and not basically choose a technological solution.

Now, use of watchdog timers and monitoring functions, you know, yes, certainly, that has been accepted in several of the designs, including Oconee. But it's not the only solution, so that's why it's --

MEMBER BROWN: Computer-based voter. You know, you haven't really run through anything that really addresses a computer-based multiple voting unit type approach to solving that --

MEMBER CORRADINI: So can I ask a question

since you guys are having so much fun?

MEMBER BROWN: We're going to finish this right now.

MEMBER CORRADINI: So you basically want to outlaw just what you said, and you're saying the way it's written, it's not specifically outlawed.

MEMBER BROWN: They want it outlawed?

MEMBER CORRADINI: No, you want it outlawed.

MEMBER BROWN: No. I want to outlaw what?

MEMBER CORRADINI: The computer-based voting --

MEMBER BROWN: No, no, no, I don't want to outlaw -- no, no, it has nothing to do with that. It's just that if you have a software-based voting -- what we've done in the other plants, if you have a software-based voting system, one in each division, they're all fed by each division. One corrupt signal can lock them all up. That's fact, as long as you have a diverse means that monitors each of the voters and executes a downstream trip down to the other actuation --

MEMBER CORRADINI: And your point is that's not specifically required.

MEMBER BROWN: It's not addressed in here.

It allows, it's back to you're going to have to sit down and have that discussion in each and every time. They don't say a diverse means to monitor computer-based voting units. And you can say, well, there's a hazard analysis. If you go back to one of the other 5.5(I), which is AH5(I), it talks about you do a -- well, of course, it's a hazard -- oh, yes, safety system internal and external hazards. In other words, it's covered by the hazard analysis. So we will evaluate the use of the voting systems, computer-based, and we'll determine whether it does or does not need a diverse means of monitoring.

MR. STATTEL: I'm a little confused. You implied that that scenario that you just described is not a common-cause failure or would not be addressed in a (D)(3) analysis, and that's a little confusing to me because I don't know why --

MEMBER BROWN: I'm just, I'm going back to discussions we had in a couple of the new reactor design world where the issue was brought up and almost, we had arguments back and forth from the designers, not necessarily the staff, that this would never happen.

MR. STATTEL: Well, I'm not familiar with those discussions in the new reactor designs but --

MEMBER BROWN: And -- oh, one other thing, Rich. And that they had algorithms to ensure that no corrupt signals could ever get transmitted to another computer unit --

MR. STATTEL: Right.

MEMBER BROWN: -- which is baloney.

MR. STATTEL: Well, for the operating system designs, I can assure you that those scenarios are evaluated in the (D)(3) analysis, in the (D)(3) analysis.

MEMBER BROWN: For operating --

MR. STATTEL: For operating reactors. The ones I've been involved with --

MEMBER CORRADINI: Right. But I think what Charlie is saying, since I happened to be there when those discussions were held, I do remember those sorts of words going back and forth between the two, between us and the designers.

MEMBER BROWN: Two different designers, as a matter of fact, yes.

MR. WATERMAN: May I interject a comment here? Clause, paragraph B up there requires that any signal coming into a safety system or safety division must be able to be detected. So we're looking at that one safety division there, all that green stuff over

there, that could be A and it could B, C, or D. Any signal coming in must be able to be detected and mitigated for both current reactors. The idea -- I'll tell you the truth, Charlie. All the reviews I've done, I've always seen these watchdog detectors, and I just took it for granted that everybody is doing it. It just slid right by me as far as should we put something in that requires watchdog detectors on each computer. It's just the systems I've seen have all done watchdog detection or alerted the operator to a one-channel reset, things like that, and it just -- so it didn't end up in here off of any contribution of mine. I just haven't seen any systems --

MEMBER BROWN: Well, one of the designs actually, if you go read the topical reports and technical reports, there's actually the implication, based on the wording of the platform itself, that it utilizes software in order to, not just to send out a digital signal, a bistable signal that says I finished my cycle, it actually uses the software to determine whether the computer is locked up or not. It's just -- so in other words, they're lockstep together, which you could disable the monitor, as well.

I just, we needed to go through the discussion, okay? To have all the thought processes

put on the table to make sure your all's thoughts were thoroughly discussed.

MR. WATERMAN: Okay.

MEMBER BROWN: Okay?

MR. WATERMAN: Very good.

MEMBER BROWN: And are there any questions since I've been the one that's done this consistently? Do any of the other members have any additional comments to make? Okay. I think we ought to roll on here.

MR. JACKSON: Okay. So I'll move on to (D)(3). Now, when we had imposed the criteria in (D)(1), which is basically one-way data communication from a safety system to a non-safety system, we had to step back and think, well, is there any time that we would need information from a non-safety system to a safety system? By definition, with independence, the safety system shouldn't need information from a non-safety system, but we did consider that there were two cases. One was if you were using the diverse actuation system, at some point diverse actuation system has to tie into the safety equipment to actuate it. The other case is with anticipatory reactor trips, for example like reactor trip on turbine trip. There would be potentially some signal from the non-

safety system for anticipatory reactor trip. So the rule does allow for those situations there.

And then the criteria for (D)(4) is basically, it's applied to design certifications, standard and design approvals, and manufacturing licenses. And this basically says if, for the new reactor criteria, they want to take an alternative, that when they do that alternative then they need to identify all the direct and indirect data communication pathways to a safety division or a safety system from other systems.

So, basically, that concludes what we have for the independence criteria.

MEMBER BROWN: Okay. Any other comments? Let's roll on.

MR. STATTEL: The next section we'll discuss is the diversity and defense in depth clauses. So four new clauses are being introduced or proposed for the regulation to address the potential for software or logic implementation common-cause failure. These criteria were derived directly from the staff requirements memorandum on SECY 93-087, so there's really nothing new here. This would be the first time that these criteria appear in regulation, though.

CHAIRMAN STETKAR: Rich, before you embark

on the details here, I don't recall whether I asked during the subcommittee meeting or not, but the rule language specifically says, "Plant parameters shall be maintained within acceptable limits established for each design basis event in the presence of a single common-cause failure. The following requirements must be met when addressing digital system common-cause failures." The rule applies to both digital and analog. Why are we only concerned about common-cause failures in digital systems, and why are we not concerned about common-cause failures in analog systems?

MR. STATTEL: Well, the SECY paper was really restricted to addressing the potential for software --

CHAIRMAN STETKAR: Yes, and I understand that's not -- I understand what the SECY paper was. I'm asking in the broader sense. Since this is a rule that's being written for going forward with any reactor design, if I want to come in with a reactor that's got relays in it, this should apply.

MR. STATTEL: So what I would have to say about that is the IEEE 603 really doesn't address diversity, right? And since this is an incorporate by reference of IEEE 603, it was really not an issue we

had initially intended to incorporate, right?

Now, we do evaluate the diversity issue. Every license amendment that comes in, we do a (D)(3) analysis. We have, in our standard review plan we have -- obviously, BTP 719 provides specific criteria for the diversity analysis.

CHAIRMAN STETKAR: But do people who have to do that diversity analysis -- if I come in today and I want to submit a design, for whatever reason, presuming that I own a manufacturer who can give me long assurances that I can, indeed, procure safety-related electromechanical relays for the life of my plant, I can theoretically come in with a design that has safety-related electromechanical relays in my protection and safeguards actuation logic. There's nothing that prohibits me from doing that. I don't think I'm required to do a (D)(3) analysis for that, am I?

MR. STATTEL: And that really is the crux of the matter. So (D)(3) was not something that's covered in the standard and we're incorporating by reference that standard, so we weren't going to initially address (D)(3). However, it was identified by the new reactors folks that some of the applicants are basically claiming it's optional, doing a (D)(3)

analysis optional, regardless of the technology involved, you know. They were making claims that, yes, we don't have to go through every accident scenario and project this common-cause failure. So that's basically what resulted in the addition of these particular clauses.

So the NRC's position was, well, what do we do now? What is our current state of affairs? Our current state of affairs, every time we perform an evaluation of any I&C system, not just digital, like you mentioned, we do use the standard review plan, and the standard review plan has us pull up BTP 719 and we use that criteria for evaluating those systems. And in truth, all of that is guidance. None of that is really dictated by regulation.

MR. THORP: So what we've seen is that, we've seen the need for more comprehensive regulatory treatment of the need for diversity in defense in depth. And we have actually written a proposal for rulemaking that will establish that as a separate 10 CFR dot XX rulemaking. I think Steve and Art wanted to address some of the discussion here.

MR. ARNDT: To get to your original question, for all systems but particularly for I&C systems, whether analog or digital, we have a set of

requirements both in terms of the single failure criteria and the general design criteria. For example, GDC 22 directs the licensees to provide appropriate redundancy and diversity.

The SECY was the direction by the Commission on how we should interpret digital systems with respect to those requirements. So the requirement to do diversity analysis and redundancy analysis and everything else has always been there as part of the single failure criteria and GDC 22 and other regulations.

What the Commission did in that SECY was direct the staff to interpret that to include a special additional requirement for software-based systems, which we also interpreted for software developed systems, like CPLDs and FPGAs. The Commission was particularly concerned about software because software is unique in that it's not a physical entity and has unusual characteristics, as opposed to other kinds of systems, like analog systems. But the common mode failure is something associated with the design of the system.

Does that help?

CHAIRMAN STETKAR: No, but it's an answer. Thanks.

MR. THORP: But we realize, going forward, we want to -- in fact, over the last year, we've talked more and more about the need for --

CHAIRMAN STETKAR: My point is, obviously, we had the Salem reactor trip breaker failure years ago, and suddenly everybody got concerned about, my God, we can have common-cause failures of electromechanical devices. So there was a lot of hand-wringing. We went through all of the ATWS rulemaking. We established now non-safety related diverse trips for reactor trip breakers and, lo and behold, we solved that particular problem maybe.

And now I'm saying, going forward, we've now become sensitized to common-cause failure. Everybody is afraid of the boogeyman of software. Nobody knows what that can happen, so, therefore, you know, it can have some nondescript common-cause failure.

Going forward, if the staff were to have an applicant come in with an analog-based system, would the same principles of searching for common-cause failures and examining whether or not the applicant applied fundamental diversity and defense in depth principles to that design doesn't appear in the staff guidance.

Now, I'm not saying, this is not realistic, necessarily, because I can't envision somebody coming in with an analog-based system, but they could. My whole point is, you know, why do we necessarily restrict them to digital systems simply because that seems to be the current focus of everyone who's afraid of the software. And I understand the concern with the software. I'm not arguing about the software.

But, anyway, we've had --

MR. THORP: Your sense is we should treat this in a broader fashion.

CHAIRMAN STETKAR: If diversity and defense in depth is a good principle to examine for digital systems, it seems to be a good principle to examine for analog systems. And single failure criteria and redundancy don't satisfy it because that's not diversity.

MR. JACKSON: And I think, as John mentioned, that's something the staff is looking at.

CHAIRMAN STETKAR: Okay.

MR. JACKSON: The current rule package embodies what the current policy is.

MR. THORP: You know, you get to a point where you're trying to do an incorporate by reference

and you want to --

CHAIRMAN STETKAR: I understand --

MR. THORP: -- not diverse too far afield.

CHAIRMAN STETKAR: I understand the constraints you're working under.

MR. STATTEL: There's probably a few other things that we're not addressing in this rule, too.

CHAIRMAN STETKAR: Not too many actually.

MR. STATTEL: But we've tried to be fairly comprehensive.

MEMBER BROWN: Interestingly enough, I just went back and read all of these, if you just, with the exception of 6I where you have the word digital safety, there's not another mention of digital --

CHAIRMAN STETKAR: No, that's right. That's why I hung up on this one.

MEMBER BROWN: If you deleted that sentence -- I'm not asking you to. I'm just saying if you did, the words would apply --

CHAIRMAN STETKAR: Just delete the digital.

MEMBER BROWN: That's what I mean.

CHAIRMAN STETKAR: It's just the word.

MEMBER BROWN: The words are not -- if you

read every one of your all's --

CHAIRMAN STETKAR: But that is, on the other hand, that's a big deletion because that is a fundamental change because, in principle, if somebody does come in with an analog system or if they're going to replace an existing analog system with a new analog system, that could cause --

MR. STATTEL: I think what the SRM did, it changed, it really set software aside because it basically said the probability is one and treat it that way. Do your analysis, assume the failure. Don't even argue that it's not going to fail. Assume the failure occurs. And that really does set it apart from the mechanical, electromechanical type devices, how they are treated. And so, anyway, that's what it is.

MEMBER BROWN: Okay. Are we done with this one now? Thank you. Okay.

MR. STATTEL: So I wasn't going to spend a lot of time on the details of these because I know we've been through these in many previous meetings. But this slide really shows what these four criteria are, and I think you'll recognize them. The first one is demonstrate that vulnerabilities to common-cause failures have been addressed, evaluate to demonstrate

adequate diversity within the safety system for each design basis event in the accident analysis. If a postulated common-cause failure could disable a safety function, which is usually the case in the analysis, then a diverse means which is unlikely to be subject to the same common-cause failure shall be required to perform either the same or a different function. And, finally, a set of displays and controls located in the control room shall be provided for manual system level actuation of the critical safety functions and monitoring of parameters that support safety functions for cases where the manual operator actions are credited.

And, basically, we pretty much stuck to what the SRM says. So, I mean, I'm willing to have some discussions about that, but are we going to just move on to the next section?

MEMBER BROWN: Anybody else have any other comments? Let's move on.

MR. STATTEL: Okay. The final proposed clause pertains to documentation. 50.55a(h)(0) establishes requirements for maintaining documentation to support compliance with (h)(2) through (h)(8) requirements, which are the new conditions that we're imposing here. So, essentially, it just says that

they have to develop and maintain the documentation to support those analysis that are being introduced.

A couple words on the alternatives clause. Okay. So one unique aspect of 50.55a is its alternatives clause, which was formally 50.55a(83). And in the proposed version, it's becoming 50.55a(z), which is quoted here on this slide.

Normally, when a licensee does not follow regulation, an exemption path must be taken to avoid a violation or enforcement action. The process for taking an exemption from regulatory licensing requirements is covered under 10 CFR 50.11 and 50.12, exceptions and exemptions from licensing requirements.

When an applicant does not follow the requirements of 10 CFR 50.55a, however, they can use an alternative approach. Additionally, there's no special circumstances criteria associated with exercising this alternative clause. There are cases in which applicants have proposed alternatives in the past, so we've reviewed several of those. But in the past, the conditions that we describe here were not present.

So an example of that would be Oconee actually used the 1998 version of the IEEE 603 in lieu of '91, and we reviewed that as an alternative under

the alternatives clause. In addition, the EPR design, AREVA has proposed to demonstrate that their self neutron detector design is acceptable, even though it does not have the required redundancy needed to meet the independence requirements of IEEE 603, and they're utilizing this alternatives clause. There have also been cases where applicants have proposed an alternative to ASME code, several of those instances.

So the proposed rule, in the proposed rule, this clause is not changing. This is not a delta that I'm showing you here. But what's changing here is, in the past, we have not had the conditions. So each of the conditions we went through we had extensive discussions with OGC, so, basically, if an applicant chooses not to adhere to the criteria that's stipulated in the condition, they are allowed to utilize this alternatives clause. And that's just by virtue of the fact that those requirements are located in this incorporate by reference rule.

Okay. So I just wanted to make everyone aware of that situation. Any discussion on that?

Okay. And, finally, Mike Waterman from the Office of Research will now present --

MEMBER BROWN: Before we go on to the 1.153 -- that's where you're going, right?

MR. STATTEL: Yes.

MEMBER BROWN: I just wanted to bring up one other item that we had extensive discussions on in other ones, and that's relative to one of the clauses, 5.9, in the IEEE standard which did not change and which you all developed no new conditions. And this, effectively, is relative to controlled access, and the words there apply -- it says, you know, the generation station design has to -- and not in exact words -- has to support the ability to maintain controlled access. So you've got both procedural requirements for operators and anybody who's in the control room to keep people from going down, but the design has to support the ability to maintain that controlled access. And with the new configurations and computer-based systems and networks, all the data coming out is going into a network. The network is feeding the main control room.

Hanging out on the network is a little thing called a firewall, which is feeding off, in almost all the designs we've looked at, whether it be the management building or the corporate bus or the internet or whatever you want to call it, that that is a vulnerability that has been introduced which is outside the control of the procedural and that the

existing architectures, we've had to have extensive back and forth to try to get that to be a non-accessible, in other words a one-way hardware-based non-software controlled or actuated or set up device in order to -- in other words, part of the plant design to support controlled access.

And I'd say we've been relatively successful in that the designers have -- I'm trying to remember where somebody has not finally given in, but they have incorporated that thought process into their DCDs and/or their proposals. Now, you all have an opportunity now to say why you don't want to do that and make it as part of the rule since it is part of the overall architecture that supports the safe operation and not introduce a new vulnerability.

I mean, whether you like it --

MR. STATTEL: It is --

MEMBER BROWN: Let me finish. The old analog plants, nobody is going to come in via some line somewhere. I mean, people have to go down to the cabinets, take a key, open it up, play with clocks and whatever else they do, even if it was an embedded digital system that didn't communicate anything other than, you know, to no networks and still had to have a guy go down with a laptop, open the cabinets.

Now you don't have that. You have all the control signals and everything else is going in and out through these networks. So you didn't address it. Here's your opportunity --

MR. STATTEL: So the clause you're referring to actually predates all of the technology discussion that you mentioned here. The clause intention was, and we did research this, the intention of that clause was essentially, you know, if you put yourself back in the 1970s, they wanted to make sure that the right people had the access to do the things they needed to do. Not the other way around. They weren't thinking about intruders or outside people trying to get access into the plant. They were thinking about is the operator able to get to the points and do the things he needs to do? Is the I&C technician able to get into the system and take the voltage measurements to make sure that the system is operable? So can the operator make operability determinations? Can the maintenance technicians do the required surveillance to ensure operability? That's what that clause was written for, and that was the intent of that clause.

And in evaluating this, there's a couple of other issues, and I'll let Terry speak to this, as

well. Redefining that, even though the title of the clause is controlled access, and redefining that intent as far as cybersecurity or, you know, maintaining protective measures against a nefarious attack, it really creates some problems because you're kind of applying an interpretation that was never the intent of that clause.

So, now, are those concerns? Yes, they are. The cybersecurity concerns are there. We believe, well, our current policy is that they are addressed elsewhere in terms of programmatic approaches, and that's really why we have the rule, the rule for cybersecurity in 73 --

MEMBER BROWN: I'm well aware of that. The point being, though, that that's four or five years after the license and the design is approved and it's open to whatever you want. You make an interesting argument, well, gee, that was what it was before back in the old days. But what are you doing now? The rule and the standard was what it was before, and you have now taken the rule you've incorporated by reference and you say, well, gee, even the new standard doesn't deal with the new technology as well as either the new rule or the old standard; and, therefore, we've taken action to compensate for

that by incorporating conditions to meet the necessity of dealing wit the new technologies. And my point being is that you can say it was there because of the unique nature of having access, but, hold it, I now have a new unique situation and control of access is the same --

MR. STATTEL: But we don't want to lose the original intent either.

MEMBER BROWN: You don't, depending on --

MR. STATTEL: So we apply a couple of different things --

MEMBER BROWN: My point being is that you didn't do anything with that.

MR. THORP: Right. We purposely did not do anything with that. And I understand this issue has come before the Committee a number of times, and I'll have Terry speak to this in a second, but staff has acknowledged the concern and has identified, essentially, that where we stand right now with the Commission direction is that the cybersecurity reviews that we do are held within a cybersecurity program requirements of 10 CFR 50.73 and using Reg Guide 5.71. Those are ongoing.

Although operating reactors are already designed and they are already out there doing their

thing, it's my understanding that staff is going to develop a SECY paper to let the commissioners review this concern and determine whether the Commission wants to direct design-oriented reviews of cyber. So our intent is to proceed forward with this incorporate by reference and see where the other thrust goes with respect to that interpretation that you would like to see for the review of design.

Terry, do you have any other comments?

MR. JACKSON: Well, I was just going to say one of the challenges we have with this rule and with this standard is that the rule and the standard scope applies to safety systems. And I think the staff takes a great extent of effort to address non-malicious types of ways that could impact the safety system.

But part of the challenge is is when we're addressing some things that are kind of outside that scope where you have a non-safety system talking to a non-safety system, then the rule doesn't necessarily apply where the standard does. So that's the challenge that we had with this rulemaking with that particular concern.

But I think, as we had mentioned in other Committee members, that we understand the technical

issue and actually have an appreciation for it. So as John mentioned, that's why we feel that we have basically a policy issue that we need to go back to the Commission and say do you want us to address some of these design aspects or some of these kind of cyber aspects in a design review and let them give us a direction then on what they feel that we should be doing.

MR. THORP: Right. Rather than us, through manipulations of the incorporate by reference rule, presume to speak for them or to preempt their review and decision-making on this. So that's why we're not going to --

MEMBER BROWN: Now, I guess I would argue that you're not preempting anything by limiting communication to one way, regardless of whatever it is. Cyber, the use of that term implies maliciousness. It doesn't necessarily have to be, once you've communicated bi-directionally to a business network, funny things can happen coming back the other way, which are totally non-malicious and inadvertent --

MR. THORP: Right. Which is why we have a --

MEMBER BROWN: -- which can shut down

everything.

MR. THORP: Right. Which is why we have a significant emphasis in our reviews of the security development and operating environment to help identify and ensure that, to the maximum extent practicable, that you don't have means by which non-malicious or other unintentional things occur that essentially create the same problems and the same consequences as a malicious type of problem that's injected. So in some sense, there's some defense in depth in that respect by pursuing the SDOE process that we have in our design reviews for I&C systems.

MEMBER BROWN: Yes, but that's how the systems are developed, not necessarily what I'm doing going outside and connecting the network someplace else. Those are down within the reactor trip systems, safeguard systems. Their communications or control system signals coming back doesn't address this path that goes out, which can be non-malicious based on an inadvertent connection. So I just wanted to get your points.

MR. STATTEL: I would like to say there's an aspect to this that really differentiates new designs, forward-looking designs, versus the operating plants. The operating plants really aren't doing a

lot of modifications to their I&C systems, right? We've had, like, two major ones in the last six years. But, yet, they have a lot of digital assets in those plants that potentially could be vulnerable, right?

So for the operating plants, it makes a lot more sense to address the cybersecurity concerns programmatically through inspections. We require the plants to develop security plans. They identify what their critical assets are. They identify what the potentials are for intrusion, and they address those programmatically because we don't have shots at those. We don't get to do another design review of a system that was designed in 1992 and, yet, it has a security vulnerability.

So from the operating reactor perspective, I can say the 73.54 rule does a lot more to address cybersecurity concerns programmatically in those plants because, honestly, I think the more vulnerable systems are the ones that are installed and operating and running in those plants, the digital assets, as opposed to a brand new system that's being designed by today's standards is a lot less vulnerable.

MR. THORP: But in piggybacking on what Rich just talked about, for a major digital I&C upgrade like we're seeing at Diablo Canyon, we are and

have been accompanied by and joined by NSIR folks who are reviewing preparations for implementation of the cyber program rule and have come along with us in our audits as we look at this digital I&C upgrade in order to see for themselves what's being done with respect to cyber.

So those kinds of things are ongoing. Just a point that I wanted to be sure that that was understood.

CHAIRMAN STETKAR: Charlie, let me interject here. We have time marks that we have to hit, and we do have --

MEMBER BROWN: We're just about done.

CHAIRMAN STETKAR: -- public that are -- that's fine. We have three more slides to cover, and we have to hit some time marks here.

MEMBER BROWN: Okay. I wanted to get the points out. Mike, do you want to go ahead with your comment, and you'll take care of the public?

CHAIRMAN STETKAR: No. I was going to say we do have public interest in the next topic on our agenda, so we need to --

MEMBER BROWN: Oh, yes. Mike, it's your turn.

CHAIRMAN STETKAR: -- be cognizant of that

time.

MR. WATERMAN: This next part of -- this is Mike Waterman. I'm in the Office of Research, and my task was to write a reg guide that accompanied the rule and I was late on that reg guide. And it looked like an onerous task until I realized I could just piggyback on the efforts of all these other people.

But Reg Guide 1.153 provides guidance for implementing requirements of the rule. It's a reg guide that -- typically, reg guides endorse standards. So if you looked at the old reg guide, and I'll get into that in a minute, that's essentially what it did.

The public and other stakeholders are presented the opportunity to comment on draft federal regulations by responding to Federal Register notices. In the case of 10 CFR 50.55a(h), the current one, the Federal Register Notice is made up of references to standards and the Commission's intent regarding the underlying basis of the regulation. And this information is published in the Federal Register Notice in the discussion section, and the regulation itself is put into the Code of Federal Regulations.

The FRN discussion is maintained by the National Archives and Records Administration through the Office of the Federal Register. And the Office of

the Federal Register maintains these Federal Register notices on a 20-year rolling cycle, if you will. When a Federal Register notice is older than 20 years of age, it is transferred over to the Federal Depository Library System. The Federal Depository Library System consists of the Library of Congress, the regional federal libraries, and things like that.

So if you have a Federal Register notice that has the Commission's intent and that Federal Register notice is older than 20 years of age, you go off to the Library of Congress if you want to find out what the Commission's intent was, right now the way things are. And why would a Federal Register notice be older than 20 years? Well, the Federal Register notice that went out for incorporating IEEE Standard 279-1971 is pretty old. It's older than 20 years. And if you go to the ops of Federal Register now to find out what was the Commission thinking when they put in 279, you're not going to find it there. And it seemed like that was, you know, that was almost a travesty because if you really want to know what the heck does this regulation mean, you can't dig it up anymore, other than going to the congressional library or you could go to a, I believe there's a dot com company, HeinOnline I think is what it's called, dot

com and you can get it from there if you subscribe to them.

But what occurred to me is, you know, are they going to be here next year? How about five years from now? Ten years from now? If this rule lasts for 20 years, are they going to be here 20 years from now so somebody can actually find out what the heck were we thinking about when we put 603-2009 into the rule?

So accompanying that regulation was Reg Guide 1.153 Revision 1. And what 1.153, the current version, now does is it endorses those two standards. It doesn't really endorse them. What it says is that all of you GDC plants and 279 plants, you can use IEEE Standard 603-1991 from now on. It gives them permission to do that. And it also endorsed a couple of other standards. And that's it. It only has about one page of guidance.

So what we have is we have a regulatory guide that essentially mirrors the regulation. Not a lot of guidance there. The real guidance, what I consider real guidance, such as statements of consideration and the discussion section of the Federal Register notice, is often the Office of the Federal Register for IEEE Standard 603-1991 or it's often the congressional library for 279.

So the proposed revision to 10 CFR 50.55a(h), in addition to IEEE Standard 279-1971 and 603-1991, includes 603-2009. Further, where in the proposed 10 CFR 50.55a(h) will reference these standards, regulations have been added to apply additional conditions.

Notice to the proposed reg guide will provide the Commission's intent. What we're doing is taking all that discussion section and moving it over into the reg guide verbatim. If, as a result of public comments, we change the regulation, we'll have to change the discussion. When the discussion changes, the reg guide will change. But it will capture pretty much verbatim what is in that discussion section, so it's up in the reg guide. As compared to where we're sitting right now where we're just pointing at a couple of standards, we're now going to have all of that Commission's intent and references to standards up in the reg guide.

So that's it. There are advantages to that, and I seem to be missing my -- there are advantages to that.

CHAIRMAN STETKAR: You've got 30 seconds, Mike.

MR. WATERMAN: This slide is going to

summarize some of the advantages. First, because the FRN provides the underlying basis of the regulation in its discussion section, that discussion section is a commitment that the Commission levies on the NRC staff that says, NRC staff, this is what we mean and this is the only way you can interpret this regulation.

So by putting it up into the reg guide, we have consistent interpretations between stakeholders and the NRC staff. Everybody is working on the same sheet of music.

The NRC website, the reg guide is going onto the NRC public website under the reg guide section. That's the logical place for telling the public what the heck do we mean by this regulation, right? So when somebody comes to the NRC on our website and says I want to see a regulation on 603-2009, 10 CFR 50.55a(h), they look at that regulation, and it would seem logical that they would go what does that mean that they would stay on our website to find out what it means. Right now, what they have to do is they come to the website to get our regulation, but they go to the Office of the Federal Register to find out what we means. So they have to leave our website and go to the Office of the Federal Register, look up the reference, dig out the discussion section out of

there. It just seems like a pretty inefficient way of doing it, especially when it's only going to last there for 20 years.

And that 20-year thing, there's no time limit on the availability of our underlying basis when we put it in the reg guide. We have reg guides on our public website now that are over 40 years old. So going this route allows us to maintain control over what the Commission means by that regulation. It just seemed like a logical way to go.

MEMBER BROWN: Okay. Thank you, Mike. John, you finished?

MR. THORP: I think we are. I'd like to thank the Committee for your good questions and the good discussions that we've had. And if we have any other final questions or discussion, we're prepared to try to address them.

MEMBER BROWN: You'll have to deal with John if you have more questions. Okay. I want to thank you all. It was a good discussion. We appreciate it. Very thorough. And I think we've got all the questions answered, and I'll turn it back to you, John.

CHAIRMAN STETKAR: One procedural thing. I'd like to ask for if there are any members of the

public in the room who'd like to make any statements, and let's see if we can get the bridgeline open. I don't know if there's anyone out there.

While we're doing that, thanks again. You crammed a lot of material into two hours, which is really good. Appreciate it. I appreciate the discussion, too. I mean, you know, we've had a lot of discussion about these topics, as you all know, in this forum and in other forums. So it's good to start focusing down on some closure.

Just to help us out, because we're a low-budget operation I have to explain this every time, if there is someone out there on the bridgeline -- I hear a phone ringing, so that means it is open.

MR. LEWIS: Hi. My name is Marvin Lewis.

CHAIRMAN STETKAR: Hi, Marvin.

MR. LEWIS: Yes, I just have a question and it might be an improper time or whatever, but what it is is about the electromagnetic pulse. Now, I don't care whether we're talking electromagnetic pulse coming from a coronal mass ejection on the sun or an electromagnetic pulse because North Korea gets whatever, okay, and sets off a nuclear bomb in the stratosphere.

We were talking about electromagnetic

interference and other electromagnetic problems. I was wondering if the nuclear power plants are hardened against an EMT event.

CHAIRMAN STETKAR: Okay. Marvin, thanks a lot. In this kind of forum, we actually don't have exchanges with the public, but we do note your comments and your concerns and we'll certainly have an opportunity to get back to you. Make sure that your contact information is available to Christina Antonescu, our staff member. And offline we will reply to you.

Any other comments?

MR. EPSTEIN: This is Eric Epstein checking in from Three Mile Island. We did file comments in opposition --

CHAIRMAN STETKAR: Eric, you're a little bit early. You're in for the Peach Bottom EPU, though; is that correct?

MR. EPSTEIN: Yes.

CHAIRMAN STETKAR: Okay. Hold off for about 15 minutes because we're just finishing up the first topic on our agenda here.

MR. EPSTEIN: I'll just call back.

CHAIRMAN STETKAR: Okay. Thanks a lot. We'll be on for Peach Bottom in about 15 minutes. Is

there anyone else on the bridgeline who would like to make a comment relative to the IEEE 6203 -- whatever it is -- 603-2009, 10 CFR 50.55a(h) topic?

If not, thank you all. Thanks for the public comments, and we are recessed until 10 minutes to 11.

(Whereupon, the above-entitled matter went off the record at 10:35 a.m. and resumed at 10:50 a.m.)

CHAIRMAN STETKAR: We are back in session. The next topic on our agenda is the Peach Bottom extended power uprate, and we'll be led through that by Dr. Joy Rempe. Joy, it's yours.

MEMBER REMPE: Thank you, Mr. Chairman. Our subcommittee on power uprates reviewed the Peach Bottom Atomic Power Station Units 2 and 3 extended power uprate license amendment request on June 10th, 2014. Subcommittee members had the opportunity to review the staff's draft SC, the licensee's power uprate safety analysis report, staff requests for additional information, and the ICC responses. And at this time, I believe that the consensus of our subcommittee is that this EPU application is ready to be forwarded to the full committee for consideration at today's meeting.

Many of the topics that we reviewed during our subcommittee meeting are similar to matters that we reviewed in past EPUs. However, there are two topics that were of special interest to our subcommittee. The first topic is the licensee's decision to implement plant modifications that allow Exelon to eliminate Peach Bottom's current reliance on containment accident pressure and analyses for LOCA, anticipated transients, and Appendix R related special events.

The second topic pertains to the approach taken by Exelon to provide confidence in the testing of vibration replacement steam dryers that will be installed at Units 2 and 3.

So today we're going to hear presentations on both of these topics and other issues of interest. And as you notice, some of the presentations do contain proprietary information, so part of our session will be a closed session. And at this point, I'd like to turn the meeting over to the staff, and I believe that Ms. Louise Lund will begin the presentations.

MS. LUND: Thank you. Good morning, Chairman and ACRS members. My name is Louise Lund, and I'm the Deputy Division Director for the Division

of Operating Reactor Licensing in the Office of Nuclear Reactor Regulation. We appreciate the opportunity to brief the ACRS full committee this morning on Peach Bottom Units 2 and 3 extended power uprate application.

Today, Exelon and the NRC staff will present selected topics based on feedback from the ACRS during the subcommittee meeting on June 10th. These topics include the plant modifications, elimination of credit for containment accident, pressure and steam dryer analysis.

The proposed EPU power level of 3,951 megawatts thermal represents an increase of approximately 12.4 percent above the current licensed thermal power level of 3,514 megawatts thermal. Since Peach Bottom had already implemented a 5 percent stretch power uprate in the mid 1990s and a 1.62 percent measurement uncertainty uprate in the 2002, the proposed EPU represents an increase of approximately 20 percent above the original licensed thermal power level of 3,293 megawatts thermal.

Our review of the proposed EPU for Peach Bottom was completed using the EPU review standard RS001. This review standard has been used for the 17 EPU reviews approved since 2005.

There are no open items in the NRC staff's draft safety evaluation. There are also no open licensing actions associated with or linked to this EPU application.

Unless there are any questions, I would like to turn it over to Rick Ennis who is the NRC project manager for the Peach Bottom EPU review.

MR. ENNIS: Thank you, Louise. Good morning. My name is Rick Ennis. I'm the NRC project manager for Peach Bottom in the Office of Nuclear Reactor Regulation, Division of Operating Reactor Licensing.

As Louise mentioned, today you will hear presentations from Exelon and the NRC staff regarding the proposed EPU for Peach Bottom Units 2 and 3. I'll present some background information regarding the NRC staff review, and then I'll discuss the agenda for today's meeting.

Exelon submitted the Peach Bottom EPU in September 2012. Following the NRC staff acceptance review of the application and submittal of supplemental information by Exelon in February of 2013, the NRC staff accepted the application for detailed review, as documented in a letter dated March 8th, 2013.

The NRC's current timeliness goals for EPUs is 18 months after the staff accepts the license amendment application for detailed review. As such, based on the March 8th, 2013 letter, the NRC staff established a forecast review completion date of September 8th, 2014. Completion by this date would support Exelon's implementation of the amendment in the fall 2014 outage for Unit 2. Unit 3 would be implemented during the fall 2015 outage.

With respect to the agenda, Exelon will first provide an overview of the plant modifications associated with the EPU, and this overview will include the modifications being made to eliminate the credit for containment accident pressure for the emergency core cooling pumps net positive suction head analyses. Exelon will then discuss the elimination of containment accident pressure in more detail.

Following Exelon's presentation, it's my understanding the ACRS will open it up for public comments.

MEMBER REMPE: Yes.

MR. ENNIS: Okay. And after the public comments, we'll have to go into closed session due to the proprietary nature of the information that will be discussed. And during the closed session, Exelon will

discuss an overview on the replacement steam dryers. That will be followed by an NRC staff presentation regarding our review of the steam dryer analyses.

And unless there's any further questions, I'd like to turn it over to Exelon.

MEMBER REMPE: Okay, thank you.

MR. BORTON: Hi. My name is Kevin Borton. I'm the licensing manager for power uprates for Exelon. This is our agenda for today, just a brief introduction and some background. And as Rick stated, elimination of containment accident pressure and replacement steam dryer during a closed session.

Before I get started, I just want to introduce some other people that we brought down with us today to this meeting. My name again, Kevin Borton. I'm the licensing manager. Craig Lambert who is over here to my right, he is our vice president of power uprate. Mike Massaro is our site VP at Peach Bottom. John Rommel next to me here is the power uprate engineering director. Ken Ainger over here on this side is our project manager and director for EPUs. Jim Armstrong here off to my right is our regulatory assurance manager. Dave Henry to my far left here is the senior manager design engineer for Peach Bottom.

And we have folks from operations. Jim Kovalchick. He's been assigned to EPU integration. He's the manager of operations. And Tony Hightower, who's been with the project since its almost very beginning, is our shift supervisor supporting power uprates.

I'd like to turn it over now to Mike Massaro.

MR. MASSARO: Good morning again. My name is Mike Massaro. I'm the site vice president at Peach Bottom. Some background on Peach Bottom. It's a GE BWR-4 with a Mark I containment, and we got our operating licenses issued in '73 and '74 and they were renewed in 2003 and now carry Unit 2 until 2033 and Unit 3 until 2034.

We've already gone over the license power level. Currently, we're at 3,514, and we're proposing an EPU to 3,951 megawatts thermal.

Next is an overview, a pictorial overview of some of the modifications going on in the plant. We're tracking approximately 29 modifications to support the EPU implementation on each unit, and I would propose to give you just a brief overview of each of them as we go through, not of every one but the ones that support reliability and plant

operational margin. And if there are questions on any of these, since I just plan to touch on them briefly, please stop me as we go. John will get into more detail about some of the modifications that support CAP elimination.

We are replacing our high-pressure turbine replacement. We're doing a high-pressure turbine replacement. This is to support improvement margin on the turbine and accommodate the increase in steam flow. It's essentially a replacement of the rotating element. This will be -- I should mention going into this that Unit 2 has -- both units are on two-year refueling outage cycles. Unit 2 has a refueling outages on even years, so this year will be a Unit 2 refueling outage in the fall, in November. Unit 3 has odd years, so next year will be Unit 3 refueling outage.

So high-pressure turbine replacement has not been performed on either unit. That will coincide with EPU uprates. So we are planning on performing a high-pressure turbine replacement this outage on Unit 2. That would include the rotor and essentially diaphragms inside the existing case.

Main generator modifications. This includes replacement of the rotor. We have already

rewound on both the units. The rotor has been replaced on Unit 3 in the last refueling outage, so last year we replaced the rotor on Unit 3 to accommodate EPU. We gained that margin. Along with that, we've also replaced the exciter and the exciter doghouse we call it or enclosure. So those modifications have been completed and give us that additional margin on Unit 3 and have been done successfully.

This was also completed on Unit 3 last year, which is essentially just an upgrade of the isophase system. Again, a successful modification.

Feedwater heaters. We have completed a study on all the feedwater heaters, looking at things such as tube plugging and wall thinning, and concluded that five feedwater heaters would be suitable for replacement. We've completed two of those on Unit 3 last year very successfully. We have one scheduled this year for Unit 2 and the remaining two next year on Unit 3 as we enter in EPU.

Reactor feed pump turbine upgrades. This is a replacement of the turbines. We're a three train feed and condensate system, and this will coincide with EPU. So this will be a replacement of the turbine, not the feed pump itself. And that will be

on each of the units, three per unit, again, as we go for EPU. This fall, we'll do the first unit, Unit 2.

Next, motor-operated valves. We've completed a review of our motor-operated valve margin. We do that on a regular basis; but, to support EPU, we identified eight valves that require margin improvement, and they will have margin upgrades through the outage and, again, in the next outage for Unit 3. That typically requires a gear change type of modification, which we've completed in the past on other valves very successfully and without incident.

We will be adding an additional main steam safety valve on each unit. We currently have two dresser valves. This will add a third dresser valve of same manufacturer at same set point, 1260 psig, by removing a blank flange on the Charlie main steam line and essentially installing the safety valve on that line.

Main steam piping. This is new supports and modifications to the main steam piping. We completed this modification on Unit 3 again successfully last outage. We'll implement essentially the same modification on Unit 2, which will be supports both inside and outside the drywell out to the turbine stop valves.

MEMBER BANERJEE: Has the SSV already been installed or will it be installed?

MR. MASSARO: The SSV will be installed on Unit 2 this outage as part of the EPU and again on Unit 3 next outage as part of the EPU.

MEMBER SKILLMAN: Mike, what clairvoyance allowed that flange to be available to you? Is that just margin from GE on early design? Is that what that was?

MR. MASSARO: Evidently, I'm looking around --

MEMBER SKILLMAN: That's a curiosity question, not a challenge. I'm just curious.

MR. MASSARO: Yes, it was a blank flange. It's been there since initial construction, and we just took the opportunity to use that flange.

MEMBER SKILLMAN: You were just taking advantage of it?

MR. MASSARO: Yes.

MR. ROMMEL: There are several others there, and we just took advantage of this one. Yes.

MEMBER SKILLMAN: Thank you. Thanks.

MEMBER REMPE: Did I miss -- but what is the designation of the light blue versus the black text in all these slides?

MR. MASSARO: I actually, I had actually intended to, since we had already given the ACRS Subcommittee an overview of these, I thought that I might just go into a couple of these in more detail and kind of touch on the ones --

MEMBER REMPE: Okay. I just was curious.

MR. MASSARO: It probably didn't work all that well. Reactor water cleanup modifications, we'll be modifying it. We have done some of the modifications. There were essentially five modifications on our reactor water cleanup system. This is to improve efficiency. We completed a portion of those on Unit 3, again without issue. And those will be completed coincident with EPU on Unit 2. They don't have to be done at exactly the same time as EPU, so we're marching through those. Many of those modifications are online modifications.

Condensate pump and motor upgrades. Here we are replacing both the condensate pump and motor with higher capacity equipment. The motors will be rated to 5,000 horsepower from the current 4,500, and this is to support increased feed and condensate. They will fit in the existing pump bowls. We expect that to be a pretty direct replacement of similar kind.

Condensate filter demineralizers. We currently have ten per unit condensate filters, if you will. We'll be adding two on each unit of similar capacity, so it will essentially increase the capacity of the demineralizer system by 20 percent.

ATWS re-circ pump trip system. This will be essentially moving the current ATWS trip to the drive motor breaker for the MG sets to an interposing breaker that is between the generator and the re-circ pump motor. This is to get more timely trip signal to the re-circ pumps to post down more timely after the initiation of the signal.

And, finally, replacement steam dryer. We have not initiated this, obviously, on either unit. This will be done as part of the EPU.

The next modifications that are associated specifically with CAP credit elimination, you can see those on the board. John will be talking about those as we go so --

MEMBER CORRADINI: Can I take you back to the last slide? I think I understand -- the second to the last one, re-circulation pump trip. So I think I understand why you want to -- does that affect anything else in terms of accident progression that you now have a faster coast down of the circ pump? I

don't remember this one from the subcommittee so I'm . . .

MR. DICK: This is Michael Dick with Exelon. Actually, there's two effects, and one is actually a little bit more. The worse effect is is for the LOCA analysis, whereas that, by relocating the trip from the MG set drive motor to the pump motor inlet, actually it causes the coast down to be faster, obviously, which is a worse effect for the LOCA analysis. And we actually took that into account with our analysis that we presented in our license amendment and showed that it had a small effect on large break peak cladding temperature but had no impact on the licensing basis PCT because Peach Bottom is a small break --

MEMBER CORRADINI: Right. That's what I remember. Thank you. Thank you very much.

MR. MASSARO: All right. With that, John, I'll turn it over and move into CAP credit elimination.

MR. ROMMEL: Okay. My name is John Rommel. I am the power uprate engineering director for Exelon, and we're going to spend the next couple of slides just talking about how we eliminated the reliance on containment accident pressure.

As part of our initial strategy for EPU, we looked at and investigated the possibility of eliminating the need for containment accident pressure credit. We considered it an opportunity to improve our margins and effectively remove some concerns that existed in the industry.

If you refer to this diagram, you've got the simple equation for MPSH available there. The term in question that we're all looking at is that H atmosphere term that Kevin is pointing to, and our current license will allow to take credit for that, the increase in that during an accident. And what we've done is to eliminate that and keep that at its pre-accident conditions.

CAP is credited at Peach Bottom for both accidents and special events. And the maximum amount of CAP credit we took was 6.1 psig. Different events have different amounts, but that was the maximum we took and that was during our large break LOCA in the long-term event.

When it was all said and done, we concluded that we had a practical design that was available to eliminate CAP credit at Peach Bottom. Thus, as part of our submittal, we eliminated that. And the next couple of slides, will go through some of

the details on how we got there.

There are four key steps in eliminating the CAP credit. Since we had to do it for both special events and accidents, it wasn't a one-shoe-fit-all type of solution, so we had to do different things for different events. And we'll go through that in some detail here.

The first step, though, was increasing the RHR heat transfer capability, and we did that via two different methods. One was we put in some cross-ties on the RHR system and the HPSW system, and the second was we increased the allowable heat transfer from our heat exchangers. As part of our test data for our Generic Letter 89-13 program, we saw that the actual filing was less than what we, that we were seeing in the plant was less than what we were considering in our analysis. So we took credit for some of that margin in our analysis.

The next step was to reduce the RHR pump flow. This allowed us to increase the -- excuse me -- reduce the required MPSH available, required MPSH, without significantly impacting the peak cladding temperature results. As Mike indicated, we're a small break limited plant, and reducing the RHR flow doesn't really impact the small break analysis.

CHAIRMAN STETKAR: John, I didn't have the opportunity to attend the subcommittee meeting. How did you reduce the flow? You just have fixed throttle valves --

MR. ROMMEL: Yes, we have some fixed throttle valves. And, actually, in the slide we'll look --

CHAIRMAN STETKAR: Okay, okay. Sorry. Never mind.

MR. ROMMEL: That's okay. The third step was we had to use the condensation storage tank as a water source during special events. The extra inventory helps reduce the pool temperature, as well as adding extra height to the pool, both of those increasing the available MPSH. We'll go through some several modifications that we did to make that happen. And then the last thing we did was we increased the boron enrichments to 92 percent from about 62 percent. This --

MEMBER BANERJEE: Can I just interrupt?

MR. ROMMEL: Sure.

MEMBER BANERJEE: The K value, is that based on experience in operating the plant now?

MR. ROMMEL: Yes, yes. Our Generic Letter 89-13 program requires us to go test and verify that

value.

MEMBER BANERJEE: And how much of the gain, you said this before but just remind us how much of the gain is coming from this K value being brought in line with your measurements?

MR. ROMMEL: Maybe Mike knows the specific answer, but it's part of, it's all part of one piece, it's all part of --

MEMBER BANERJEE: Is it 20 percent, 50 percent? What is that number?

MR. DICK: This is Michael Dick with Exelon. Previous to the EPU analysis, the K value that was used, I believe it's, if I recollect, it's 263. And we raised it through the analysis to 305. So, essentially, it's about 20 percent.

MEMBER BANERJEE: Twenty percent. Okay. That's a good answer. Thank you.

MR. ROMMEL: Okay. So go to the next slide. This slide here just shows how the different actions we took impacted the various event analyses and in-grade into the overall strategy to eliminate the need for containment accident credit.

As you can see, the cross-ties for RHR and HPSW are really only for the accidents and that the condensate storage tank actions are really for the

special events. The heat exchanger change and the RHR pump changes are more systematic changes, and they affect all the events.

Okay. This slide gives a simple overview of the RHR and HPSW across time modifications. We're going to leave this on this slide as I go through the details up on the screen, so you can see that as we go through the details.

One of the big differences at Peach Bottom than some of the rest of the plants is that Peach Bottom has four RHR heat exchangers, two per division. Our original analysis only credited one, so one of the key elements in increasing the heat transfer capability was to figure out a way to use that extra heat exchanger on each division.

So if you go through -- okay. To take advantage of the extra heat exchangers, we added a cross-tie, and Kevin can show you there, between the two RHR systems right downstream to the pumps with a normally closed valve, the one in the middle there. The two other valves were just maintenance valves but the normally closed MOV.

We also added control valves upstream of the heat exchangers to allow balancing of the flow, and that was answering the question that you had

earlier where you have some throttle valves there that we control the flow with.

CHAIRMAN STETKAR: They're controlled, but they're not --

MR. ROMMEL: They're control valves.

CHAIRMAN STETKAR: -- operator control? Okay.

MR. ROMMEL: Okay. And then on HPSW, we added, we upgraded the valve there in the middle that was only used there previously for outage purposes to a valve that can be opened against full flow and pump differential pressure. This allowed the HPSW pump to supply cooling water to the extra heat exchanger. The combined effect of this was to effectively increase the heat transfer capability by, roughly, 65 percent, in addition to the increase in the fouling allowable.

With these modifications, along with the reduction in the pump flow and the reduced fouling, we successfully reduced the post-action pool temperature to a point where MPSH available was always greater than MPSH acquired and, thus, effectively eliminating the need for CAP credit for accidents. And this, again, was really just for the accidents more than anything.

Okay. If you go to the next slide,

there's a pictorial of the modifications for the condensate storage tank which are really for the special events. First, we added a stand pipe to prevent draining and ensure adequate water level in the CST. Next, key lock switches were installed in the control room to prevent inadvertent valve actuation which could result in swapping from the suction from CST to the suppression pool.

MEMBER CORRADINI: Can we just go back?

MR. ROMMEL: Sure.

MEMBER CORRADINI: I know you guys said this, and now I don't remember. Explain to me the need for the added or the benefit of the added stand pipe? I'm sorry. Can you just remind me?

MR. MASSARO: It protects the CST inventory in special events from a drain down from the hot well makeup reject line.

MR. ROMMEL: Basically, we elevated it.

MEMBER CORRADINI: Well, that I understand, but I'm trying to understand the event that would suck it, that you protect --

MR. ROMMEL: Go to that valve. An inadvertent opening of that valve right there.

MEMBER CORRADINI: Oh, okay. Thank you. Thank you very much.

MR. ROMMEL: Third, we raised the torus high-level set point where swapping the HPSW suction from the CST occurs.

MEMBER BANERJEE: But you raised it to get additional head; isn't that it?

MR. ROMMEL: No, we raised it so that the swapping, that we stayed on the condensate storage tank for a longer period of time. There is a benefit of extra head, but the real was we wanted to use the condensate storage tank for a longer period of time and not go into a re-circulation mode.

MEMBER CORRADINI: You just delay, you just delay the time into re-circulation?

MR. ROMMEL: Correct.

MEMBER CORRADINI: Okay.

MR. ROMMEL: And, finally, we made some procedural guidance changes to allow us to make up to the CST from the refueling water storage tank. This gave us just an added source of water.

So all these changes, along with increasing the enrichment of the boron-10 combined with the other RHR changes we talked about previously, resulted, for special events again, MPSH available being greater than MPSH required for all special events. Thus, in conclusion, for all events, both

accidents and special events, we came up with a solution where our available MPSH was always greater than the required. And, therefore, we won't require containment accident pressure credit for Peach Bottom.

MEMBER BANERJEE: Could you just go back over this reduction in RHR flow that you alluded to? I figured that was for the special events --

MR. ROMMEL: No, no, no, it helps them all for the RHR pump. We reduced the design flow here. Just give me a second. I got the numbers here. We reduced the design flow from 10,000 gpm down to 8,600 gpm. What that does is it reduces the required MPSH --

MEMBER BANERJEE: Oh, I see. Got it.

MR. ROMMEL: Instead of needing this amount, you need less amount to prevent decavitation. Now, since, again, we're essentially a small break limited plant, they really had, this change had lower effect under peak cladding temperature analysis. While it impacted the large-break analysis, it had nowhere to impact our limiting condition.

MEMBER REMPE: During our subcommittee meeting, we discussed a little bit about how long it would take for the operators to implement the cross-tie, and could you, for the rest of the full committee

members, just go over that a little bit?

VICE CHAIRMAN RAY: And, also, normally, a lock closed valve or something like that is intended to ensure against the effect of a single failure propagating to both trains, for example. I'm completely unfamiliar with this, and I'm just looking at what you're presenting just now. Could you also, she asked about the operator action, but could you also talk about whether there's any implication of that valve now being part of the accident sequence changing the single failure assessment of a system?

MR. ROMMEL: I'll let Tony answer both of those questions.

MR. HIGHTOWER: This is Tony Hightower, Exelon operations. To answer the single-failure question first, we're making two modifications to the valves. One is the RHR cross-tie valve, and that cross-tie valve operates within an RHR subsystem. So if that RHR subsystem is affected, we rely on the other RHR subsystem for the event.

The other aspect to that is that RHR cross-tie valve is only used during an event after which a single failure has already occurred. So our procedural guidance will limit us to using that RHR cross-tie to events that have already included a

failure of a kV bus, an emergency bus, or a diesel generator that supplies --

VICE CHAIRMAN RAY: Okay. So that's part of the consideration in opening the valve --

MR. HIGHTOWER: Yes.

VICE CHAIRMAN RAY: -- is an assessment of whether you're exposing part of the system that was isolated, just something that is inoperable or failed somehow.

MR. HIGHTOWER: And we've simplified it to a symptom-based criteria which will require a single failure to have occurred. The approach to the HPSW cross-tie is --

CHAIRMAN STETKAR: So just to make sure I understand, that's the RHR cross-tie and that's within, that's within a particular division --

MR. HIGHTOWER: Yes.

CHAIRMAN STETKAR: -- so you're not talking about interdivisional effects?

MR. HIGHTOWER: Yes.

CHAIRMAN STETKAR: Okay.

MR. HIGHTOWER: The HPSW cross-tie, however, is between, is used between two divisions. And that is also going to be operated only after a single failure, at least one single failure of a

safety-related component.

To operate that valve, our procedures will require that a 4 kV bus has failed, an emergency bus has failed, or a diesel has failed. And that also would ensure that a single failure has already occurred. And from a design and licensing analysis perspective, we don't have to assume the second single failure.

MR. BORTON: And, Joy, I'll answer your question, too.

MEMBER REMPE: Yes, there were some questions, and I tried to recount what I know from what I read, but I think it would be good to have you --

MR. BORTON: I provided some information to the staff. So our design, our licensing basis shows that we use CAP credit up to 78 hours.

MEMBER REMPE: Oh, that one, yes. That's good, and that's what I have in the letter or the draft letter. But the timing required for the operators to implement this cross-tie, my understanding is that you can get it started in the same amount of time you would have done without the cross-tie, right?

MR. HIGHTOWER: Yes. The analysis assumes

that we place suppression pool cooling in service early in the event. The analysis assumes that the RHR cross-tie is placed in service following placing suppression pool cooling in service. It assumes that we place torus cooling in service at one hour following initiation of the event. So that makes it feasible for operators. We started work on the procedures, and it's a simple operation consistent with other RHR component manipulations that we already have in our procedures.

MEMBER BLEY: Let me, let me push a little bit on the single failure built into the procedures, and it's hard to think fast enough here to get it right. But the thing I'm a little concerned with is, you know, from a licensing point of view, that sounds like the normal thing, thinking about single failures. The real world and your PRA, too, looks at combinations of other failures.

I suspect there are combinations of other failures, pumps or things out for maintenance, that could get you in this same spot, such that it would be, you'd need to open this valve. And I'm just wondering if you've shoe-horned yourself in the procedures into requiring specific single failures you thought of ahead of time, rather than giving you the

capability to do this when, functionally, the system needs it to work.

MR. HIGHTOWER: And we did look at that as part of our strategy, developing our strategy. And failure of a diesel or a 4 kV bus is what would drive us to need to use that valve. It's --

MEMBER BLEY: That's one failure that could lead you to need that valve. You could have others, I suspect. The things that are driven by that diesel could fail themselves. I mean, if we've got a procedure that says, unless the diesel or the bus failed, you don't open that valve, it might not be the best thing for you.

MR. HIGHTOWER: The failure that we're looking at where we would need that cross-tie valve is a failure of HPSW pump and a RHR pump concurrently. So it is a certain combination of failures that would require us to have that flexibility. We do have two HPSW pumps and two RHR pumps in each subsystem, so if those combinations of failures haven't occurred we don't need to use a cross-tie. So we did go through a rigorous evaluation of --

MEMBER BLEY: So I haven't seen the procedure. Now, if the procedure is linked out to all the combinations you just described, that's probably

good.

MR. HIGHTOWER: The procedure is a practical application of the outcome of our evaluation that we did.

MEMBER BLEY: Well, in any case, we haven't seen the procedure in detail, so I hope we're not somehow trapping ourselves when the real world gives us a case you didn't lay out inside the procedures.

MR. HIGHTOWER: Certainly.

VICE CHAIRMAN RAY: But, nevertheless, I want to be on the record saying this is a good thing.

MEMBER BLEY: Oh, yes, it's a very good thing.

MEMBER SKILLMAN: John, in your discussion, you've used the term "special events" a number of times. Would you explain the difference between accident and special event, please?

MR. ROMMEL: Kevin, you can go to the one slide that has the table. That's probably the best way to go through that. So the DBA LOCA and -- the first two columns are DBA LOCA and obviously an accident. The second one is a small steamline break, obviously an accident. And then you have events for Appendix R, which is a fire, ATWS event, and an SBO,

all considered special events. And they have different, obviously different transients that you have to evaluate.

So I guess that's the difference between the two. And, you know, we needed to have different solutions to make them work analytically for each one, and that's why the whole series of changes versus just one shoe type fits all.

MEMBER SKILLMAN: Okay. Is the term "special event" described in your license, or is that just one that you're using in slang in this discussion, or is that one that has some formality in your documentation?

MR. ARMSTRONG: This is Jim Armstrong, regulatory assurance manager at Peach Bottom. Special events are clearly a category in our license. You know, you have accidents and then you have special events that you're required to analyze for, so these are the three special events we're required to analyze.

MEMBER SKILLMAN: Thank you.

CHAIRMAN STETKAR: John, I'm very quickly trying to find my list, and I can't. Is Peach Bottom converting to NFPA 805 risk-informed fire protection, or are you staying with the Appendix R?

MR. ROMMEL: We're staying with Appendix R.

CHAIRMAN STETKAR: Okay, thanks.

MEMBER BANERJEE: And you do need to increase the boron for the ATWS?

MR. ROMMEL: Correct. We're going to increase it to 92 percent, and it's about 62 percent right now.

MEMBER REMPE: Okay. At this point, because of the fact that we have to close the session for proprietary information, we're going to take a break and open up the phone lines and let a member of the public who's requested the opportunity to talk speak. Are the phone lines open so he can speak? Mr. Epstein, can you hear us and can you respond back? Is there anyone --

CHAIRMAN STETKAR: I'm sure he can hear us. I doubt that the phone line is actually open.

MEMBER REMPE: Okay. I was getting different information --

CHAIRMAN STETKAR: We're checking on it now.

MEMBER REMPE: But is there anyone in the audience, while we're waiting, that wanted to make a comment? Because this is going to be the only time

for public input during this session. Okay. So we're going to have to just wait for the phone lines then.

CHAIRMAN STETKAR: No, we can't go into closed session with the phone line open, and we do need to provide the opportunity for public comments. So we're going to wait. We're on the record here, so just put us off the record so you don't pick up all of the extraneous comments and we'll go back on the record.

(Whereupon, the above-entitled matter went off the record at 11:29 a.m. and then resumed at 11:30 a.m.)

CHAIRMAN STETKAR: We are now back on the record, and Joy?

MEMBER REMPE: Okay. You're good, too? Okay. So, Mr. Epstein, this is your opportunity to provide comments. We have you scheduled for five minutes.

MR. EPSTEIN: Okay. Can you hear me?

MEMBER REMPE: We can.

MR. EPSTEIN: Yes. I guess I'm at a loss here because I filed comments at the subcommittee and have received no feedback or responses. So my comment is threefold. One, has the subcommittee reviewed my comments? Has the Committee reviewed my comments?

And will we be receiving any input to the testimony I delivered?

CHAIRMAN STETKAR: Mr. Epstein, the answer to your first comment is -- this is John Stetkar. I'm the chairman of the Committee. The subcommittee does not speak for the Committee. So I'm sure that the subcommittee received your comments, but, unfortunately, that's kind of irrelevant to the current proceedings.

The more relevant issue is, yes, indeed, the full Committee did receive your comments. We have them and they will be made part of the record of the proceedings of this meeting. They will be appended to the record of the proceedings.

And I've read your comments. I can tell you that the ACRS typically does not address environmental issues. However, because your comments were submitted as part of this meeting, the NRC staff, I'm sure, will review them and address them in the context of the environmental issues associated with the site.

So I can give you those assurances. I can't give you an answer to your specific questions because, as I said, we don't do that. A, we don't do that in this forum; and, B, we typically, at the ACRS,

do not become directly involved with environmental issues, which the majority of your comments addressed those environmental issues.

MR. EPSTEIN: Well, I guess I would suggest, for future reference, you know, because we spent a lot of time putting the comments together and we made a trip to D.C. So to be told that the comments that I made to the ACRS subcommittee was irrelevant I find deeply --

CHAIRMAN STETKAR: They're not irrelevant, sir, except for the fact that the subcommittee does not speak for the ACRS. The subcommittee's function is to gather information for further deliberation by the full committee. The full committee is the operative body; so, therefore, communications with both the public and the NRC Commission.

So we certainly appreciate the effort that you've made to both come to Washington and address the subcommittee because we do, in the subcommittee meetings, provide that opportunity for members of the public, and we do take those statements very seriously during the subcommittee meetings. The only problem is the subcommittee cannot speak for the full committee, so that's why you have this opportunity to make oral statements in the full committee meeting so that your

oral statements are on the full committee meeting record. And as I said, your full written comments will be included in the record of this meeting, so they will not be lost.

MR. EPSTEIN: Well, let me ask you something just in terms of political mechanics. Are you going to vote today up or down to approve the EPU or what? I mean, because if you're going to get back to me with comments and today you're going to vote one way or the other on the EPU, you know, I'm a little confused on how that works.

CHAIRMAN STETKAR: We'll have to be a little bit cognizant of time here. The ACRS does not vote to approve or disapprove the EPU. We simply draft a letter report with our recommendation to the Commission. The Commission will make the final determination.

So if the answer to your question is do we plan to write a letter report to the Commission during this meeting, the answer to that question is, yes, we do. I cannot get --

MR. EPSTEIN: I don't want to take up any more of your time because, frankly, you know, I just want to state for the record that I would appreciate if the NRC did formally respond to the comments

because it's very disheartening as a member of the public to put that much time and effort into comments not to get a response. And just for your edification, we will be suing at the DEP regarding the company's request for a water quality permit. That's fair play that I apprise you of that.

But I guess, I guess this thing I'm still wondering is will the NRC respond to the testimony or will it simply --

CHAIRMAN STETKAR: I'll let the staff speak for that right now. As ACRS, I can't guarantee you things one way or the other, but perhaps the staff would like to weigh in.

MR. ENNIS: This is Rick Ennis with the NRC staff. Consistent with the guidance for this type of license amendment, the NRC had previously published a draft environmental assessment and finding of no significant impact, which we published in the Federal Register for public comments. We did receive some comments, and we did resolve those comments and issue a final environmental assessment and finding of no significant impact, which we also published in the Federal Register.

So as far as this license amendment, we have completed our environmental review. So we

wouldn't, we wouldn't, in the course of this review, address any other environmental comments at this time.

CHAIRMAN STETKAR: And we now have that statement on the record of this meeting also.

MR. EPSTEIN: Yes, I don't want to waste your time or my time. Gentlemen and gentlewomen, have a great day. Disappointing. But we'll check with you down the road.

CHAIRMAN STETKAR: Great. And thank you very much for your comments and your time. We do appreciate that very much.

Is there anyone else on the line who would like to make a statement? And as Dr. Rempe mentioned, if you're on the line this is your only opportunity because, from this point forward, we will be closing the line.

MEMBER REMPE: Because of proprietary information that will be discussed.

CHAIRMAN STETKAR: So hearing nothing, we will close the bridgeline in both directions. And we'll have to change the record. The other thing that I'll ask both the licensee and the staff to confirm that every one in the room is cleared to hear the proprietary information. So staff and licensee, make sure that you know everyone here.

Make sure that we have, the bridgelines are closed.

MEMBER REMPE: But while we're in between records, clearly -- right? We're not on either record right now?

CHAIRMAN STETKAR: We are.

MEMBER REMPE: We are on one or the other records? Okay.

CHAIRMAN STETKAR: We have not closed the meeting. As soon as I have confirmation that the bridgeline is closed -- just make sure that we have the bridgeline closed.

Just for our purposes, because of the number of people who are identified as being connected, could we ask each person who's on the bridgeline currently to both state your name and your affiliation, please?

(Phone line introductions.)

CHAIRMAN STETKAR: Okay. We seem to finally be in a good situation here. We are now entering closed session for the record.

(Whereupon, the above-entitled matter went off the record at 11:42 a.m. and then resumed at 2:00 p.m.)

CHAIRMAN STETKAR: We are back in session,

and the next topic on our agenda is review of the mPower design-specific review standard Chapter 7, instrumentation and control systems. And we'll be led through that topic by Charlie Brown.

MEMBER BROWN: Okay. This is kind of a wrap-up session. I mean, we have had a couple of meetings, subcommittee meetings, and they have published this before, this DSRS chapter for public comments. We've seen those and incorporated them. We had another meeting after that, and now they are hoping that we will complete this review today at the full committee and they will be able to pilot this for their first opportunity.

So I want to make sure, did you have any opening remarks, or do you want to segue right to Tim? Tim, have at it.

MR. MOSSMAN: Thank you. Good afternoon. My name is Tim Mossman. I currently serve in the Office of New Reactors in the Instrumentation and Controls Branch 2, which is led by Ian Jung, who is seated to my right. Also with me today is Joe Ashcraft, who is one of our senior engineers in the branch who has logged a significant amount of time in the development of the Chapter 7 DSRS.

Before I begin, I want to note that,

previously, the full committee was briefed on DSRS Chapter 7 by Milton Concepcion, who, along with Joe and many of the other I&C staff in our branch, did much of the hard work on this document. Milton has since left the agency for a position in the private sector, but we do appreciate the work that he put in on this product.

In addition, I wanted to point out our project management staff from DARR, Division of Advanced Reactors and Rulemaking, who have provided significant support to us in the development of Chapter 7 and helping us coordinate with the other chapters in the DSRS.

Also with us today is some of our folks from DCIP, vendor quality, Paul Prescott and Mary Anderson, who have worked on the quality section.

Today's agenda is as follows: I wanted to kind of give you a brief overview of what the objectives of Chapter 7 were. I wanted to introduce Section 721 on quality, which was not completed 18 months ago when we last briefed the full committee, although it was completed in time to go out in the version that went out for public comment. I wanted to go over the ACRS formal recommendations that we received approximately a year and a half ago, as well

as some other comments that we got recently from the subcommittee in May and how we considered those and then wrap up.

Okay. Since we previously briefed Chapter 7 of the DSRS to the full committee, we've only included a brief overview of the major changes to the I&C section. The major change to Chapter 7 was to reorganize the SRP content from a system focus to focus on I&C design principles and design attributes in the DSRS. In addition, we took the opportunity to remove redundant staff guidance and non-applicable information. The SRP has a lot of staff guidance for review against IEEE 279, which is very applicable for operating plants but will not be applicable to newer plants or the SMRs.

Staff also had a number of lessons learned from other design certification reviews that we attempted to reflect in the guidance. One of the most notable ones resulted in the inclusion of appendices on hazard analysis, systems architecture, and simplicity, which we expect will enable applicants to better communicate their designs to staff, facilitate our review, reduce the number of RAIs, and make this a smoother process.

MR. JUNG: I just want to take this

opportunity to visually show -- I shared this some time ago. This is the DSRS. Both are double-sided. And this is SRP as it is right now. And removal of redundant and non-applicable information really focused, so all the information here that's applicable to new reactors are incorporated. And, actually, one of the sections has actually a complete matrix that talks about how this was transferred here. That's been scrutinized by the committee, so this is complete.

So I just want to highlight from a simple user-friendly staff guidance perspective, this will provide clear mapping areas to look at, which area to look at. Any design or any system related to I&C, just looking at the table of contents will show, oh, I need to address this, I need to work on determining the predictable repeatable behavior.

I just want to highlight even a simple restructuring of the guidance, I think we made a significant difference.

MEMBER SCHULTZ: And you haven't had a chance to test drive this yet, but have there been tabletop exercises with staff to go through the document to validate what you just told us about ease of use?

MR. JUNG: Not quite there yet. We were really hoping to pilot this with mPower. But I think, overall, this has been scrutinized by the applicant, both the mPower, addressed most of their comments, and staff has been working on it. They are trained by being part of the development.

So I think they're excited about this. And in addition, as Tim mentioned, to incorporate a better way of doing it, those appendices on the concepts of simplicity, architectural design information, and hazard analysis. Even additional tab is in addition to this here. So I think this will be a great platform that we can continue to build up on our guidance.

MEMBER SCHULTZ: We share your excitement, and thank you for the demo.

MEMBER BROWN: Let me -- along that line, you said you had talked or NuScale has been involved in looking at this, as well. Have you thought about how you're going to translate this thing that says mPower at the top to say NuScale? And the second part of that question is, aside from the FMR applications, we had mentioned in one of our letters that we ought to be giving some thought to this at even reorganizing what I would call new reactor, like big reactors,

review plan along the same organizational setup. Did you all give anymore thought to that at all, or is it downstream?

MR. MOSSMAN: In answer to the two questions, one, we have provided a draft of the, we're working on the draft of the NuScale DSRS Chapter 7, and it will look remarkably similar to the mPower 1 by design. We tried to make the Chapter 7 as common to SMR as possible, so that, eventually, it might get to a point where it's just an SMR DSRS or SMR, SMR SRP or something to that effect.

We've talked about applicability to other reactors, and I think, if an applicant came in expressing interest in having us review against the DSRS, we'd have to discuss that. We'd certainly give it serious consideration, but, at this time, I think we're really focused on trying to get it to an SMR review first before we expand it out. But it's something we would consider.

MEMBER BROWN: There was an ISG we put together for licensing. I can't remember what the number is. Six, seven, five? And that's structured a little bit relative to this fundamentals approach and what detail will you need. So I'm just trying to think ahead. Whether anybody new is going to come

forward in today's environment and decide they want to design a new reactor is going to be interesting, to say the least. But I just, the fundamental format and the focus on fundamental principles up-front and then identifying details I think is a good way to get a more coherent and integrated view of what somebody is submitting. So, yes --

MR. ASHCRAFT: I would just like to add that some of our last signed certifications for the large light waters, they revamped their sections and wanted to add in principles discussions and so forth. So even though we wouldn't use this, this would have, those appendices would help us even in that respect of when they came in.

MEMBER REMPE: So when I was reading this, since we're talking about how you're going to apply it, I noticed that it -- well, I know 10 CFR 50.34 specifies instrumentation requirements for beyond design basis accidents, and you've accommodated that somewhat in this section. And I'm not quite sure that was one of the thoughts that crossed my mind, so if you could educate me what happened on any plant that's come in for construction permit after '97 and how that was implemented. But if you go into 10 CFR 50.34, it requires that you have instrumentation that would

survive severe accident conditions, and I was wondering how you're going to do that or has it been done? Because where's the cutoff frequency, for example? And you don't do it to a meteor strike or whatever, and how do you do that?

MR. JUNG: One of the sections in 7.213 has a section on displace and monitoring, and it incorporated the existing guidance regarding Regulatory Guide 1.97, which endorses IEEE 497 with clarifications. So in 497, it talks about the variables for various types of scenarios, manual actions, automatic actions, and variables.

The tougher variables we have known to be important. I think many of them are covered. But as you know, because of the post-Fukushima, some action items, because of the timing and because of the ISGs and other guidance being developed, you know, working with them in operating reactors, some of those areas are not specifically covered. So even for some of the COL combined license reviews we are seeing, they're creating separate chapters, Chapter 20, of that nature, to address post-Fukushima items that's encompassing some of the new topics that came from the Fukushima accident.

So we didn't want to inject those moving

targets in our guidance. This project started just about a year after Fukushima event so --

MEMBER REMPE: I understand you don't want to put the details here. I'm just wondering what's in your mind and what you're going to do. Reg Guide 1.197 is for design basis conditions, and so there may be other sensors and then what kind of conditions the sensors have to survive. And perhaps it will be a lot easier with the small modular reactors and all, but it's just -- one answer you might have given me is, oh, I'm going to use a risk assessment and we're going to look at, you know, some of the risk dominant events or something. But I just am not sure what you're thinking, and I would be interested in what you're thinking.

MR. MOSSMAN: A couple of things. And I think it was kind of what we got from our chairman here at the subcommittee on 7.213 about the tie to the operating experience and the Fukushima orders. And so we did actually put some additional language of the 7.213 to make that tie stronger to --

MEMBER REMPE: I didn't know you discussed this already.

MR. MOSSMAN: And so we attempted to strengthen that tie to make sure that the Fukushima

orders or other relevant operating experience does get reflected and that display is monitoring.

In addition, and I'm not our agency expert on IEEE 497 or Reg Guide 1.97, but I talked to our representative to that committee. He said that their next, the next revision to IEEE 497 is going to have expanded guidance on --

MEMBER REMPE: I heard that, too.

MR. MOSSMAN: -- essentially, beyond design basis events, although I think they're calling it something else. And the way the DSRS is written is we do not endorse a specific version of the IEEE standards that are guidance or the reg guide. It's whatever version is in place six months prior to submission. So as that gets evolved, the DSRS should be able to automatically pick that up if we go ahead and endorse that.

CHAIRMAN STETKAR: By the way, one thing in response to some of the things Ian was saying, we just had an opportunity recently at the subcommittee level to see Chapter 20 for one of the new design centers in terms of response to the Fukushima orders, and that chapter was entirely silent on survivability of instrumentation in severe accident. It had a lot to do with designing spent fuel pool level

transmitters until level gets to the top of fuel in the spent fuel pool but was entirely silent on any severe accident type qualification for instrumentation. So it's not going to be resolved in that format for either the currently certified designs or any of the designs that are in the review pipeline, unless things change.

MEMBER CORRADINI: If they were to change, where would they change? I'm trying to understand. We're not supposed to care about only technical things, but, from a process standpoint, I'm still confused because what John is speaking about is true, that, basically, it's what you'd expect to be, I want to have level instrumentation, I want it to be of a particular quality and accuracy. But then, after that, it basically is the spent fuel is determining the environmental conditions that they must perform in.

So if you're going to go beyond the design base, what process does the staff have to understand what I'm going to specify beyond the design base?

CHAIRMAN STETKAR: And that's, I mean, we saw spent fuel, but, more importantly, it's containment parameters, things like temperatures and pressures and what all you might to look at what's

going on inside the containment and what may or may not be left of the core. And it's entirely -- I mean, you know, the Chapter 20 thing, we're entirely silent on that.

MEMBER CORRADINI: I was going to say, except for spent fuel and orders in spent fuel level indication, is there anything in terms of Fukushima-related activities that actually suggests any sort of additional instrumentation?

MEMBER REMPE: It's reactivity that ACRS . . .

MEMBER CORRADINI: Some members of ACRS recommended that.

MEMBER REMPE: The committee passed it.

MEMBER CORRADINI: Some members recommended that.

CHAIRMAN STETKAR: The simple answer is no.

MEMBER CORRADINI: I didn't think so because the only reason I'm asking is that, I mean, let's just take something that we know is out there but there is no instrumentation because I have a hydrogen plant. So is there a process by which staff is going to start saying, okay, I must have a thermocouple and a pressure transducer that must

quality to this temperature and pressure and radiation level so that it survives the extreme environment to actually measure something?

So my question is, okay, now show me the process that determines the right temperature and pressure and radiation level. That, to me, is tough.

MR. CARUSO: Mark Caruso with the staff. I'm trying to pass that -- we have something that might help. I think, you know, this is really an evolving area. We had some discussion of this when talked about Chapter 19 the last time where we have incorporated guidance about our interaction with this group when we look at the severe accident analysis.

But I think the most important thing that's happened recently is the Commission has directed the staff and the SRM to modify, when we put in the design certification rule, you know -- there used to be a clause in there that said if there's a changed process for anything that's required for X vessel severe accident mitigation needs to be captured in Tier 1 and this change process applies. Well, they opened that up to all things that would apply to severe accident mitigation and directed the staff to ensure that, when the rule is written, that it accounts for that and to make sure that in their

reviews that the items that are important to those features are captured in Tier 1, which would then open you up to ITAACs and additional review, I mean a review on a level that, say, we did for the BiMAC.

So I think this is an evolving area. I think the Committee and subcommittees have been at the forefront of asking these questions because they asked the same kind of things to us. So I think that's what happened there is a significant development in this area because it opens up a door for us in our review through the severe accident analysis and assistance from them to identify features and identify what it takes to make sure these things do what they're supposed to do and to get them captured in Tier 1 of the DCD. So I don't know if that helps or not.

MR. ARNDT: As you know --

CHAIRMAN STETKAR: Identify yourself.

MR. ARNDT: I'm sorry. Steven Arndt from the staff. One of the Tier 3 activities in the post-Fukushima agency activities was to look at severe accident instrumentation at the recommendation of the Committee, and that is an ongoing research project, as you're familiar with the Tier 3 designation.

The other activity that Tim mentioned earlier is the revision of the IEEE standard, and that

is, if that includes the kind of instrumentation that we're referring, then that would logically flow into the reg guide and then into the standard review plan.

So all of those activities are going along in parallel. How much of it actually gets into a guidance and/or regulation depends a lot on cost benefit analysis, what we find out from the research, and where the technical community goes.

MEMBER REMPE: Out of curiosity, what happened with -- we were talking about this the other day, and what happened with AP1000, did it happen before the 10 CFR 34 was passed or was it after? And if it was after, did cost benefit kind of dominate on what was done?

MR. ARNDT: I can't speak to that.

CHAIRMAN STETKAR: First of all, it's Part 50, and AP1000 is Part 52.

MEMBER REMPE: CFR 50.34? Is it --

CHAIRMAN STETKAR: I just --

MEMBER REMPE: -- action. And it says anything that has a construction permit after 1997 needs to consider design basis --

CHAIRMAN STETKAR: But AP1000 does not have a construction permit. That's the whole point. It's licensed under Part 52.

MEMBER REMPE: Oh, so both of them have to do --

CHAIRMAN STETKAR: I'm not sure how. The applicants actually do address the post-TMI issues, but I'm not sure --

MEMBER REMPE: Yes, that's what --

CHAIRMAN STETKAR: I know they do address those issues in their application, so it's not silent.

MR. MAGRUDER: This is Stu Magruder from the staff. I can address your question. Part 52 has a requirement for any new application to address all the TMI requirements, so that's how we get the 50.34(f) requirements.

MEMBER REMPE: So since you only have one more slide, can I pull the string a little further?

MR. MAGRUDER: Of course.

MEMBER REMPE: What did they do? Did they do cost benefit, or how did they address it with AP1000 to say we have instrumentation that will survive severe accidents?

MR. MAGRUDER: I don't know. I'd have to ask Ian or Joe or somebody about the specifics of I&C, but, from a licensing perspective, that's how we get the --

MEMBER REMPE: Yes, I figured it was done,

and I just was curious. And if someone could give me some information later, I'd appreciate it.

MR. MAGRUDER: Okay.

MEMBER REMPE: Thanks.

MEMBER POWERS: You probably just avoided all that Idaho stuff.

MEMBER BROWN: You're going to make some other mention of this later in your slides, if I'm not mistaken. I had taken a quick look through, and you do mention a change that was made to 7.213. It's generic in nature, but, yet, it has some comment relative to -- without being specific -- the analysis or what information you expect. So I would suggest you let him grind through the slides, okay? Even though there's only 11 slides and you want to take as much time as you could.

All right. Go ahead. You're still on -- oh, you've now transitioned to slide four.

MR. MOSSMAN: Slide four. As I mentioned, Section 721 of the DSRS, which is entitled "Quality," it's I&C quality, was under development late in the calendar year 2012 when staff previously briefed this committee. However, this section was completed and included in the DSRS version that was released for public comment, so our public comments did reflect

review of this section.

The new section on I&C quality incorporates the review guidance that was contained in the SRP, including the material from BTP 714. One of the driving goals behind developing this section was achieving greater coordination with NRC's vendor quality staff. The regulatory basis for I&C quality are the same as the regulatory basis for quality of other safety-related components in nuclear power plants, specifically 10 CFR 50 Appendix A GDC 1, 10 CFR 50 Appendix B, and 10 CFR 50.55a(a)(1).

Staff's expectations are that we can achieve a review that is more efficient by leveraging existing staff expertise in quality, that's largely our DCIP folks, while ensuring that the I&C technical staff are able to focus on aspects of quality that may be unique to I&C systems.

Next, I was going to walk down the formal recommendations that we received late in 2012 from the full committee. There were four formal recommendations. The first recommendation was fairly straightforward, and this was one of the easiest ones to address, was to release Chapter 7 and we released the entire DSRS for public comment, which we did.

Staff received a number of formal comments

from the public on the DSRS. Approximately, 2,000 in total from the public were provided. That was on the entire DSRS, which were considered by the staff. A hundred and nineteen of those comments were directed specifically to Chapter 7. Generation mPower, NEI, and NuScale provided the majority of public comments on Chapter 7 with one comment being submitted from an individual at IAEA.

While the majority of the comments were editorial in nature, we did receive approximately three dozen technical comments. Of the technical comments, approximately half of those were just requesting clarification on particular positions or statements in DSRS Chapter 7.

We believe we successfully resolved all the comments. We did not consider any of the technical comments to be showstoppers, nor did any of the resulting comment resolutions change our approach to Chapter 7.

If there's any particular public comments you have questions about, we're happy to discuss. But, generally, they were fairly benign relative to the direction we're going.

MR. JUNG: I'll just note that, after that letter of recommendation we received, the staff

formally responded to it. We are just updating that we have executed the commitments to be made in the response letter. So it was good to go back and read through on what has happened since then.

MR. MOSSMAN: Recommendation two is one that Charlie just kind of ghosted a little bit ago. The thought was that the DSRS Chapter 7 may be applicable to more than just the mPower SMR. It may be applicable even up to and including large reactor designs. Staff agreed that it certainly may have applicability beyond the mPower design. We certainly hope it does, given the time and effort we put in on it.

However, those opportunities will need to be identified on a case-by-case basis. And right now our primary focus is on getting Chapter 7 a trial run before making any wholesale changes to other I&C review guidance because we want to go through a learning cycle on what we put together.

The guidance, ultimately, the guidance very likely will be migrated to another DSRS in the very near future and possibly may be migrated to other guidance documents, as appropriate. So we agreed.

The third recommendation had to do with a very specific design implementation to be applied to

reactor designs to comply with control of access. Staff acknowledges the Committee's concern and recognizes that the issue addressed by ACRS Recommendation 3, control of access, has wider equatability that just to the mPower design and its corresponding DSRS.

As such, as detailed in the staff's letter to the ACRS dated April 3rd of this year, the staff intends to develop a correspondence to the Commission to seek their guidance on how to proceed with this issue. Staff does not perceive that there's any technical disagreement with the Committee regarding what the Committee wants to accomplish via the recommendation. I think we're in very good agreement with what we want to accomplish.

I think the issue is simply where the confirmation of adoption of the appropriate defensive architecture boundaries should occur as to whether it should be via cybersecurity inspections under the cybersecurity program, or do we augment that with review in licensing space with the design certifications. And we will keep ACRS informed as to our progress on this correspondence.

MEMBER BROWN: For members and since you've heard all of the dialogue in the previous

meeting this morning, I don't see any sense in grinding through that dialogue again. The issue is the same. The back and forth is, roughly, the same. And we will have to evaluate how we go forward with what they intend.

MEMBER CORRADINI: And your opinions are the same?

MEMBER BROWN: My thought processes, as coherent and cogent as they are, are still the same, yes.

MR. JUNG: I just want to, Member Schultz asked us at the subcommittee meeting. If you look at the slides, staff is developing a SECY paper for more of a, not just that issue, more other, other technical issues. So this is an opportunity just to share. The staff, mPower, DSRS, and some of the rulemaking efforts you've seen this morning, it's sort of looking at what we've seen is the immediate changes to the regulatory framework to address the lessons learned.

But we are continuing, the staff has continuously seen new challenges even now. One of the topic is such as embedded digital devices. These digital devices are going into execute features of the safety systems, pumps and valves, MCCs, protection for turbine missile issues. You've seen cases. It's in

bits and pieces, but, I think, for new reactors in particular, we'll probably see a significant, if not most of the mechanical electrical equipment in the future, we expect to see an introduction of these devices. And given the current framework being structured based on traditional protection system, I&C is going to continuously challenge us.

So we are looking at those issues and also, recently, there was an issue of -- of course, non-safety systems themselves are also employing a significant number of digital systems where some of the failure modes may result in a plant condition that is not analyzed under safety analysis or it could introduce your secure actuation scenarios or conditions that's beyond the analyzed.

So it has become somewhat challenging in those areas. So we are looking at it broadly and looking at not next five years but looking at 15 - 20 years. If you don't start now, rulemaking takes about five to ten years. So we are looking at for the future. That's one option. It's an options paper we are developing for the Commission. So at the end, the Commission might say just address this particular issue the ACRS has addressed or it could be look into a more broader setting where the global I&C

instrumentation challenge and some other examples. Is there a way to really take a global leadership and maybe including harmonization? And also we're looking at the 2008 policy statement on reactors. It clearly talks about simplify systems, inherent safety systems, easy to explain to the public, easy to analyze for safety and conformance to the regulations.

So we are looking at that as an opportunity, rather than missing this opportunity. So we'll brief the Committee in the future on that aspect, but the staff is working hard to develop a logical SECY paper to the Commission with a certain set of recommendations. It's still in the works. In the next several months, we are working on the paper.

MEMBER BROWN: Just before you go to this, just a little bit -- flip back. I didn't use this this morning because we were running out of time, so I will just -- I did receive from another former member, as a matter of fact, who does excellent research a note about a hacker that broke into a control system network for a public utility through their vulnerabilities and their remote access at their utility. He used brute-forcing techniques. In other words, he made attempt after attempt after attempt. Finally got the password. They were compromised.

They were configured for remote access capability that was bi-directional, had passwords and stuff like that, which they lost them. And this came out of Homeland Security, and this ICS, that's industrial control systems, identification noted that tools even as common as Google and other search engines give people who are skilled the ability to go in and find and pull out passwords and other access information in order to do this.

So you'll have to understand my reluctance to accept or -- not accept -- to agree that we can take another five years for the SECY paper and SRMs and the constant back and forth of what, you know, legal and everything else that needs to be done when a simple design architecture inclusion in our design documents, which is totally separate from any malicious cyber thought process, just a fundamental design, like you put a diode between the safety system and stuff going somewhere else, is pretty easy to do and doesn't require hordes of PhD theses in order to come to a conclusion.

So just bring this particular item up. I've summarized two pages of stuff in about ten sentences to note that. And on the embedded device things, that's another interesting issue, depending on

how those, it was a power supply. The analog systems takes an analog in place of power supply. Those do come now with embedded software in them, and if that embedded software has an external connection that goes into the network, you have no idea what could be done with even something so simple as a power supply.

So I just wanted to make you aware that this sleeping dog is not just laying here. I'm speaking about myself. I'm not speaking for the Committee. I'm speaking for myself.

MR. MOSSMAN: I completely appreciate where you're coming from, and I think, to the best of our ability as a staff, we have attempted to engage vendors jointly as both, whether it be NRR, NRO, I&C staff, along with the NSIR cyber staff, to give a single message to the vendors about defensive architectures, about what's essentially prescribed that ought to be in there cyber security plan, and if it's not it's not going to get approved, which features a lot of one-way communications.

And the message we've tried to give to vendors, and I think they've been very receptive of it, is, even though the cyber provisions apply to licensees, not to vendors, because it's an operational program, the message to vendors is please set your

licensees up for success, not failure, and that if you do the right things in design your licensees will have a much easier time complying with the cyber provisions and making sure that those protections not only are in place in day one but for the life of your facility.

And so I think we've gotten pretty good feedback from the vendors from that message, and we've been actively reaching out. We even actually had an agreement or an engagement with a -- a foreign regulator came over, and we actually gave him a joint briefing with the same message.

MEMBER BROWN: Well, we've had some success with the designers, over and above the fact there's no requirement, that they have eventually used the word caved and have incorporated that feature in the designs to enable us to at least write a letter that said something.

Anyway, I just wanted to bring that up to say, just to let you know that this is really not an abstract and as off the wall as it sounds. That's all. So you can proceed.

Oh, I'm sorry. I didn't --

MR. CALDWELL: I'm Bob Caldwell. I'm a deputy division director for the Division of Engineering at NRO.

MEMBER BROWN: Oh, okay.

MR. CALDWELL: And we do understand your concern, and we are going to take it back. And I'm previously from NSIR, so I'm familiar with the situation.

MEMBER BROWN: Okay. Thank you very much. And I'm sorry I missed you out there.

CHAIRMAN STETKAR: That's what I'm here for.

MEMBER BROWN: Are you trying to tell me something? Okay, Tim. Have at it.

MR. MOSSMAN: We're in agreement with you. We want to achieve the same thing. So recommendation four had to do with a very particular, a very specific section of Appendix B, which was on system architecture, DSRS Chapter 7 Appendix B which addresses system architecture to augment what kind of diagram should be provided. And so staff agreed in the letter, and we responded about a year and a half ago. We agreed with the recommendation. We did augment item three of the relevant information section of Appendix B. The additional text emphasized that the purpose of providing this information was to facilitate staff review on the fundamental design principles and design attributes in Section 7.1 and

7.2.

You can see in the little box at the bottom of the slide, the words in black were the ones that existed when you last looked at the DSRS a year and a half ago. And the new content is in red.

MEMBER BROWN: I'm looking at it right now.

MR. MOSSMAN: Okay. In addition, Regulatory Guide 1.206, combined license applications for nuclear power plants which contains guidance on development of a complete design certification application, is currently under consideration for revision. The current version was released in 2007. Any revision to Reg Guide 1.206 would also include lessons learned from the development of DSRS Chapter 7. And I happen to know a guy who is our point guy on Reg Guide 1.206, so I don't have to go far to make sure those lessons get incorporated.

MEMBER BROWN: Okay.

MR. MOSSMAN: In addition, as was noted, we briefed the digital I&C subcommittee back in May of this year, and we had a lot of discussions amongst ourselves. Based upon the discussions we had at that meeting, the following were some of the changes we made to, additions that we made to the DSRS Chapter 7

in response to the subcommittee.

The one at the top on independence, I believe Chairman Stetkar had noted that there may be possible situations where prior decisions regarding actuation of the safety function may be conditional. And so we added a statement in there that, in the event that there are some conditional priorities, that those should be identified and justified.

On the bottom left, 7.213 displays a monitoring. And we augmented that to make sure that we had a stronger tie to the Fukushima-related orders, as well as instructing staff to circle back with the operating experience folks to make sure any relevant recent operating experience is reflected in the staff review of 7.213.

And then --

MEMBER BROWN: These were in addition to the ones we reviewed during the -- you've added --

MR. MOSSMAN: Yes, yes.

MEMBER BROWN: Okay. That's what I thought.

MR. MOSSMAN: Yes, so these were new since May.

MEMBER BROWN: Since May. Okay, thank you. I know we discussed these, and we went over

comments during the meeting?

MR. MOSSMAN: Yes, yes.

MEMBER BROWN: Okay, got it.

MR. JUNG: Just as usual, we went through all of the transcripts.

CHAIRMAN STETKAR: By the way, those were not ACRS comments. Those were subcommittee comments. So be careful how you characterize those.

MR. MOSSMAN: They were discussions, and we felt there was enough merit to go back and tweak some words.

MR. JUNG: I was going to take this opportunity, I was looking at the 7.213 related to Member Rempe's discussion on the -- I assume that she is here.

MEMBER REMPE: I thought I'd confuse you and sit over here.

MR. JUNG: I'm sorry.

MEMBER CORRADINI: You can stay there if it's okay with him.

MR. JUNG: I can elaborate a little bit more later, but I think the current section goes through all the sections of the 50.34 section related to variables, including severe accidents. I'm just going to read one section. There are multiple

sections.

MEMBER REMPE: Is this from the IEEE standards you're reading or --

MR. JUNG: No, that's DSRS.

MEMBER REMPE: Okay.

MR. JUNG: So it says the reviewer should note that the position regarding 1.97 expands the guidance for type C variables beyond what is stated in IEEE Standard 187. And then it talks about working with the severe accident technical staff and the PRA for assistance in identifying the necessary information. And then the reviewer should consider the following attributes: the variables monitored and range and accuracy of information provided to monitor these variables should conform with the severe accident analysis submitted under, pursuant to 10 CFR Section 52.47(a)(23).

The instrumentation provided for monitoring severe accident conditions should be designed to operate in the severe accident environment -- that's what Mr. Stetkar was talking about -- for which it is intended and over the time span for which it is needed.

MEMBER CORRADINI: Can you repeat that, please?

MR. JUNG: These instrumentations should be designed to operate in the severe accident environment for which it is intended and over the time span for which it is needed.

MEMBER CORRADINI: Which instrumentation, though? That's what I --

MR. JUNG: These are instruments that include in both accident prior to core damage, as well as post-core damage severe accident conditions.

MEMBER CORRADINI: But the instrumentation identified is what I was trying to understand. It can't be all instrumentation --

CHAIRMAN STETKAR: Well, the licensee or applicant has to identify what instrumentation is needed.

MEMBER CORRADINI: So if they don't identify any, they don't have to qualify any?

CHAIRMAN STETKAR: Well, they have to identify post-accident monitoring instrumentation. That's a requirement.

MEMBER REMPE: And they'll have to come up with some --

CHAIRMAN STETKAR: What particular instruments it is --

MEMBER CORRADINI: I mean, we have a

little bit of time, so just to go over the point. I don't remember anything in AP1000 or ESBWR that was identified.

CHAIRMAN STETKAR: The ESBWR, there was a lot of discussion. I don't remember how they resolved it. I did a quick check on AP1000, and I think it's really vague and hazy. They refer you back to Chapter 19, which is the PRA, and they identify, I think, although I haven't done enough reading here in realtime, instrumentation that's supposed to survive.

MEMBER REMPE: I thought they also did some cost benefit analysis --

CHAIRMAN STETKAR: That I didn't get far enough. But I --

MEMBER REMPE: I was kind of wondering how this was --

CHAIRMAN STETKAR: I think, as the designs have, the design reviews have matured, certainly the later ones are identifying that inventory of instrumentation. There's a lot of give and take between the applicant and the staff.

MEMBER CORRADINI: So you've seen there was stuff identified?

CHAIRMAN STETKAR: I don't know for ESBWR because I know there was quite a bit of discussion in

terms of the staff requesting the list and push back saying we can't identify that list yet because we don't have our I&C system developed and, once we develop the I&C system and the HFE, which is all backed, then we'll provide the instrumentation. But I could be mis-remembering that.

MEMBER REMPE: Doesn't there also have to be some SAMGs involved or some sort of --

CHAIRMAN STETKAR: But that's all, that's all post -- any procedures are post-COL.

MEMBER REMPE: Yes.

MR. TANEJA: This is Dinesh Taneja from the I&C. You're correct about the ESBWR being DAC. But we spent considerable time on the USAPWR because they elected to provide us with variables, and we've gone through their EOPs, which are preliminary, and we've talked with them, but we did not get into the SAMG area. That, again, is a Chapter 19 area. But we did, you know, Reg Guide 1.97 is performance based where they have to demonstrate the instruments that they need to mitigate or monitor design basis events. So, you know, we spent quite a bit of time with them in developing that parameter list.

MEMBER CORRADINI: But I guess, just to make sure I'm clear about my curiosity, my curiosity

is about something that's either being built or is certified, not to be certified, and to what instruments are identified. So the ESBWR --

CHAIRMAN STETKAR: My recollection for ESBWR is it was punted off into DAC space.

MEMBER CORRADINI: For AP1000? For AP1000?

CHAIRMAN STETKAR: That was before -- I don't remember. I was doing a quick search here, and I don't --

MEMBER CORRADINI: I'm kind of curious because I don't remember anything.

CHAIRMAN STETKAR: I don't remember a list, and that's why I did a couple of quick searches here and I couldn't find one. But I'm trying to listen to presentations and search at the same time, which means I'm not doing well on either.

MR. MOSSMAN: Oh, yes, the last one was the bottom right, seven to eleven on multi-unit stations. Although we didn't anticipate for mPower having shared systems, we added some stronger language in there to consider failures in non-safety systems, and it actually kind of goes to head to other SMR designs we might get that it might be more applicable for. So it may or may not do much for the mPower

review, but it sets us up for --

MEMBER BROWN: That's just a stake in the ground.

MR. MOSSMAN: It does. Okay. And then one last item, part of the formal recommendation letter that we received 18 months ago had some discussion on lockup conditions, reviewing lockup conditions. And so we just extracted -- this was some verbiage that was already, it's already in the DSRS on 7.21 under independence that addresses --

MEMBER BROWN: You all had -- this was incorporated in the version we reviewed. I mean, I recognize this.

MR. ASHCRAFT: This is Joe Ashcraft. I think why we just put this slide is you had made a comment in the May meeting that, hey, I put the words, you know, and these were some of the words that we didn't find in that previous slide, but they were already -- they're actually in a stronger place in the DSRS.

MEMBER BROWN: Okay, all right.

MR. MOSSMAN: All right. In summary, we think the DSRS Chapter 7 is ready to be piloted for review of a digital I&C design. We have interacted with numerous stakeholders throughout the process and

have generally gotten very good feedback and positive contributions. We believe we've achieved the objectives we set out to accomplish via this guidance, which would be an accomplishment of a more efficient and effective licensing review, guidance that will support a more efficient and effective licensing review, and we look forward to piloting it.

CHAIRMAN STETKAR: I have a question. One issue that you didn't cover in the presentation and one change that was made from the earlier draft that the committee saw and the current version is that you've, in the introduction, you've developed a framework that categorizes SSCs or, in this case, instrumentation and control issues into four categories that are designated as -- A1 is safety-related risk significant; A2 is safety-related non-risk significant; B1 is non-safety related risk significant; and B2 is non-safety related non-risk significant.

Those four categories are remarkably the same as categories RISC one through four in 10 CFR 50.69, except they're renumbered and renamed. And in particular, A1 is risk one; A2 is risk three; B1 is risk two; and B2 is risk four. So we can't even keep the numbers straight.

So that leads to a point of confusion. But that's not where I'm headed with this. The confusion is confusing, and we ought not to have confusion. But that's -- I can accept being confused.

The more important issue is that the guidance now says that a, the highest level of review will be applied to both A1 and A2 categories, which are the safety related, regardless of risk significance. And then let's call it a less stringent review but more stringent than completely non-safety related non-risk significant will be applied to the B1 category so that we apply the most stringent review to anything that's given the name safety related, regardless of its risk significance. And then the non-safety related but risk significant issues get enhanced review compared to things that are both non-safety related and non-risk significant.

The structure, regardless of the names that we give these things, is good because the intent of the design-specific reviews were to be both design specific and risk informed so that part of this increasing efficiency and focus on the things that are most important to real plant safety for that particular design would achieve the highest attention during the review process.

This doesn't do that. This says that, regardless of the risk significance, if something is given the name safety related, I do a very in-depth review of it. And anything that's not safety related but risk significant gets a lesser review. That doesn't seem consistent, so I'd like you to address that. We had some discussion over this.

And the reason I bring it up here is, in the context of digital I&C, it's important. But as a practical matter, this is the first section of the design-specific review standard that's being issued. So at this higher level, in terms of organizing the review and how you think about performing the review, it will be the template that I'm assuming will be followed by all other chapters, whether I'm looking at, you know, pumps and pipes and valves or, you know, whatever.

MR. MOSSMAN: We had a lot of discussion about this topic post-subcommittee meeting.

CHAIRMAN STETKAR: And that's why you didn't have a slide on it.

MR. MOSSMAN: It probably is fertile conversation for an entire session on its own. But I think the one, your one thought at the end, I'm not sure I can speak generically to any of the other

chapters in the DSRS as to how they will address the categorization and how it influences their review. And I think that was one impression that I think afterwards we probably felt folks might have walked away with is that the Chapter 7 is the way it will be treated throughout the rest of the DSRS and not necessarily true.

For the I&C section, at this point in time, our regulatory framework and our guidance is not really set up to address relaxation of safety-related items. And at this point in time, heading into the mPower review, I don't know that we anticipated having, I don't know that we can point to an A2 system to even know --

CHAIRMAN STETKAR: But categorization is a different issue. At one level, I'm more concerned because I can hear the people who are looking at the Chapter 6 systems, the Chapter 9 systems, the electric power systems, everything else, saying those same words. At this point in time, we're not set up to do this, so we're going to keep status quo. And it was my impression that wasn't the intent of risk-informing and streamlining the, the whole purpose of developing this risk-informed streamline review process for the small modular reactors.

So by you saying that, well, at this point in time, in Chapter 7, we don't know how we would do that, the other chapters are just going to mimic those same words. You know, unfortunately, you're first off the block.

MEMBER BLEY: Yes, but, in any case, it seems to, while we haven't written anything for a while on this, but we have written related things, so it's almost a spot for the whole committee but certainly for me. Taking something that's analyzed to be risk significant and giving it less review intentionally makes no sense from a safety point of view to us, or to me for sure. And, you know, you can argue about, well, if it's safety related, we got to do it. Well, that's okay. If you have to, you have to. But to say that you'll take a thing that you know is more important than something else and give it less seems contrary to good practice. It just really does. And that really bothers me quite a bit.

And I would hope, I wouldn't hope -- the idea that Chapter 7 doesn't speak for all the other chapters is even more disturbing to me because we ought to be getting consistency throughout this thing. So that's really bothersome. I'm sorry, Mike. I cut you off.

MEMBER CORRADINI: Oh, no, no. So I guess I don't appreciate, since I've never been a reviewer, what more or less review means. So explain to me what that means. If I'm a reviewer and I get those directions, what am I supposed to do? Spend ten hours here, eight hours there, six hours there? I'm not sure exactly what that means. Can you help me?

MR. JUNG: Member Corradini, that's a generic question that actually all the different disciplines discussed with the projects branch in trying to understand. So I would refer to Stu, if you want to kind of --

MEMBER CORRADINI: Because I'm kind of in agreement with what John and Dennis were saying, which is it really kind of seems kind of counterintuitive or maybe even wrong to do it that way. But I'm not sure what that entails, so I have no way of feeling how wrong that might be.

MS. STAREFOS: This is Joelle Starefos. From a larger picture, we understand that concern and we've done a lot of work in developing the introduction part two to the SRP to give guidance on what this means to the reviewers and how to actually develop the DSRS.

One of the lead PMs on that project is

Mike Jones, and he's at the microphone. I'll ask him to just make a few statements on that.

MR. JONES: Yes, hi. Just a couple of clarifications, I guess. First, there is a difference in treatment between A1 and A2 in the guidance. A2 allows you to start to consider alternative approaches to taking a look at meeting the design requirements, and so A1 is not the same as A2 in the guidance. So if you look at the diagram that's included in the introduction, it gives you a place to start to use a different approach and start to use some risk informing if you think it's appropriate.

MEMBER BROWN: Are you talking about the DSRS?

MR. JONES: I'm talking about the SRP introduction part two, which is where this risk-informing approach --

CHAIRMAN STETKAR: But we're talking specifically here about DSRS, and we were instructed earlier to not confuse that with the SRP because the staff didn't know from one direction how this particular guidance was eventually going to get into the SRP or not. So please don't confuse the Committee by bouncing back and forth between the SRP and this. We're addressing this specific review standard and

guidance.

MS. STAREFOS: This is Joelle Starefos. Let me just try to clarify for a moment. The SRP is our standard review plan for all of our normal guidance. In order to do the DSRS and develop it as required or requested by the Commission, we had to develop what we called introduction part two of the standard review plan. That was our avenue to allow all of this DSRS to occur, and that gave us our direction on how we were going to do everything that the Commission had requested during and throughout the SECY paper interactions.

So what Mike is sharing is the overall guidance to everyone in allowing this to happen this way --

CHAIRMAN STETKAR: I understand that. But I will quote verbatim for the record Section 3A. I'm in Section 7.0. And in this guidance, it says, "For SSCs determined to be safety related and risk significant (A1) and safety related non-risk significant (A2), the level of review will involve detailed analyses and evaluation techniques to satisfy the acceptance criteria contained in the DSRS." It does not differentiate between A1 and A2, regardless to whatever, an introduction to section whatever you

cited in the SRP. This does not follow through on that. So if this is contrary to the intent of the SRP, it is then contrary to the intent of the SRP.

MR. JONES: This is Mike Jones again. I understand your comment. I think what the I&C folks are saying is that this differentiation between A1 and A2 is going to be difficult in the realm of I&C SSCs.

CHAIRMAN STETKAR: That's a different issue because that says if I look at pump A versus pump B I might not be able to -- that's throwing the individual SSCs or the elements into boxes. If I can't populate box A2, that distinction doesn't change how I think about reviewing box A2 if I could populate it. And this says, if I can populate that box A2, I must treat it the same as box A1. I don't care if box A2 is empty. I don't care. It says I don't, I don't need to care about it.

So from a pragmatic sense, if they say that they don't know how you can differentiate between A1 and A2 in the particular context of digital I&C, I can accept that. That's fine. I can accept that. But the guidance should still be set up saying that if you could do that, if some clever, creative applicant comes in and says I've done a very, very detailed analyses and here's my justification for

differentiating between A1 and A2 and if the intent is to provide less stringent review guidance for A2 compared to A1, this doesn't do that. So you're essentially precluding or, in some cases, providing a disincentive for somebody to come in and try to do that. Why would I, as an applicant, try to even justify it if I don't think I can get any benefit from it?

VICE CHAIRMAN RAY: Well, maybe there is no justification for it.

CHAIRMAN STETKAR: That's a different issue.

VICE CHAIRMAN RAY: Well, I know that. But they're both in A.

MR. CARUSO: Excuse me. This is Mark Caruso from the staff. I feel like I'm hearing fingernails across a blackboard here. And I was heavily involved in developing this process. I guess I'm not, I know that there are some issues with the I&C DSRS on this topic specific to them, and I don't know what they are. I can't really speak to that.

But I want you to know that what Mike was saying is we have, we wrote down guidance, general guidance for the development of DSRS in this SRP introduction zero that talks about this whole process

of how the staff should do it. And there it's very clear that the treatment of A1 versus A2, B1, B2, is as you would want to it to be, and it says it in SRP-0. It tells the staff generally. And I know from all the work that's been done on the other DSRSs, Chapter 9, Chapter 6, chapter whatever, that that is being followed.

CHAIRMAN STETKAR: Okay. We haven't seen those.

MR. CARUSO: Well, you have not seen those, but I want you to know that the general approach here is not to treat A2 the same as A1. The general approach to the staff is to look for opportunities in A2 because they're not risk significant to find ways to, you know, rely on perhaps operational programs as a basis for showing down the line that something is okay, rather than spending a lot of time reviewing. But, you know, as we've all said, you know, there are a number of things that you have to still do, especially with respect to design.

So, anyway, I just wanted to make that clear because I didn't think that was getting through.

CHAIRMAN STETKAR: No. And as I said, this is the only chapter that we've seen so far of the DSRS. So it's our only solid frame of reference in

terms of, you know, our state of knowledge at the moment.

MR. TANEJA: Just, you know, a little bit of background on this particular introduction section. When we were writing that, Milton Concepcion and I, we had a long discussion on the actual design. Now, if you have a safety-related system, A1, A2, regardless, when we look at the I&C systems we have a safety-related platform and you have a non-safety-related platform, typical designs that we have seen so far.

So if I have an A2 system, I would still put that instrument or that system by my safety-related platform. So I really have single treatment of safety-related platform.

So, really, it's very difficult for me to distinguish, you know, how I do A1/A2 because I'm using single platform predictor of all safety systems. That's really what the thought process of --

MEMBER BROWN: When you say platform, do you mean like the reactor trip system will use a Common Q platform?

MR. TANEJA: Correct.

MEMBER BROWN: And another ancillary system that feeds that or does whatever is a still safety, it's called safety related, but it uses a

Common Q but it's not as risk significant. Does that -- I'm trying to get, I'm trying to understand your use of the word platform.

MR. TANEJA: Platform is like -- let's say we are using Common Q as an example, right? So I have a Common Q platform, four divisions, displays associated with them. Now, if I say post-accident monitoring, it's an indication only. Is it critical, not critical? That's a different issue. But I will be putting those instrument indications on my safety-related displays, not on my non-safety system.

So my treatment of that safety-related platform is a single treatment. I'm going to apply the rigorous review criteria to make sure that that platform is a solid fundamentally-safe platform, which will support all my safety-related function in the plant. That was the thought process that went into, and it was very difficult for us to say, when it comes to I&C, how can we, you know, degrade A2s because I'm running it on the same platform. That's why. I just wanted to --

MEMBER BROWN: So the pan, the pan is not a safety related --

MR. TANEJA: It is safety related.

MEMBER BROWN: Oh, okay.

MR. TANEJA: But, you know, I don't know if somebody wants to make an argument that it is A2.

MEMBER BROWN: It's A2, yes. But it --

MR. TANEJA: Yes, but I will still be on that.

MEMBER BROWN: It would still be using a Common Q platform for it?

MR. TANEJA: Right.

CHAIRMAN STETKAR: There's a couple of things here, and, obviously, this is kind of a charged issue. But one is consistency in the guidance throughout the regulatory, all chapters, same basic philosophy. And if the basic philosophy is that one should treat A1 differently from A2, that should be reflected consistently in all chapters.

If the population of A2 is zero for whatever reason, that's okay. That's fine, that's fine. There's no problem with that.

The other is communications with potential applicants and licensees to say that, if we want to provide incentives for people to use the principles of risk assessment and performance to help streamline the entire review process, we don't necessarily want to provide disincentives by saying, well, look, we've created these four categories, but there's absolutely

no incentive for you to go to try to do this assessment. Maybe somebody can come up with a really clever way of justifying why something in the digital I&C safety-related arena could be an A2. That might be a challenge to them. It might be a challenge to the staff to review it. But we don't necessarily want to preclude that based on our experience to date or some preconceived notions about what might happen in practice or what has happened in practice so far.

So that's the other part of the coin is to keep, if we're establishing this framework, let's establish it and make sure that everybody understands what it means.

MR. CARUSO: John, Mark Caruso again from the staff. I wanted to say one more thing, and I think it relates to what you just said but more so from your comments in the beginning about the confusion about the boxes being named differently. Remember that this framework that we're talking about is strictly for the staff to use to help organize its review. We are not, in any way, shape, or form, asking applicants to do any kind of bidding of SSCs in boxes. We are not asking applicants to do a de facto 5069 assessment. We are only asking applicants to do what they've done in the past, which is, A, categorize

their SSCs as to whether or not they're safety significant in accordance with 50.2 of the regulations; and, B, to have a wrap program and to assess all SSCs with their wrap program and identify a list of SSCs that they consider to be risk significant.

We'll take that information, staff will take just that information and it will be the one to see what goes in the boxes. And one of the things that we, when we were first rolling this out and putting it out there, we were meeting with mPower, and they were under the impression that we were asking them to do 5069. So as far as the confusion goes, it's a two-edge sword.

CHAIRMAN STETKAR: Yes, I understand that there's some intention there, and that's right. On the other hand, if they voluntarily want to come in and classify those things that way --

MR. CARUSO: Sure, if they wanted to. But I --

CHAIRMAN STETKAR: Not formally under the 5069, but if they want to say, well, we believe that we differentiated even within the safety-related category based on this risk significance, and we would expect from the staff differentiation in the level of,

you know, do I get 37 RAIs because I'm in A1 but only six because I'm in A2, that's up to them.

MR. CARUSO: And we've had discussions with at least one vendor about them wanting to do that but with three boxes. So in any case, I was getting the impression that maybe you thought we were asking them to do this kind of bidding, and we're not.

MR. MAGRUDER: This is Stu Magruder from the staff, and I want to follow up on this discussion. A couple of take-aways. One is I think we can look again at Chapter 7. I understand now more clearly your point, Dr. Stetkar, and we can look and see if we can write it in such a way that would not preclude somebody from doing it separately. Like you said, if we want to leave it open, if somebody can think of a good way to do it, I think we should be open to it because, you're right, we want to maintain the same philosophy throughout the entire document that there's a --

CHAIRMAN STETKAR: And from Mark said, if other chapters already have established that hierarchical philosophy, it seems that it should be reflected consistently. And if you already thought that process through in the SRP section that we can't seem to find --

MEMBER BLEY: I just pulled down SRP 7.0 and the SRP introduction, and it ain't in there. So it might be a new version that's not up on the website yet.

MR. MAGRUDER: No, it's on the website. I can show you. It's at the very bottom of the page.

CHAIRMAN STETKAR: We can do that offline.

MR. MAGRUDER: But the other takeaway I have is I think the staff needs to work with the Committee and come back at a future date and go through how we're approaching this categorization for an actual design, whether it's mPower or NuScale, give you some examples, talk about how reviewers are doing things differently, and --

CHAIRMAN STETKAR: You know, that would come out, in principle, in the piloting part, but if the pilot is going to be performed sort of within this version of the framework, you won't necessarily challenge that aspect of the piloting under at least Chapter 7. And, again, unfortunately, for many good reasons, Chapter 7 is first off the block because that's obviously, in many cases, the most difficult part of the review, the most complex. It's been the source of many, many concerns in the new reactor licensing and certification process, so it's good to

get this on the table as early as possible. The other chapters might have been easier to assess from a piloting --

MEMBER BLEY: I just want to clarify one thing I had said. I can understand, for practical reasons, there might be cases where either you cannot distinguish A1, A2, B1, B2, or, even if you can distinguish it, you would want to apply the same review. That's not what we're talking about. What we're talking about is that structure that's there for those cases where you can distinguish them and would apply a different review, it ought to be consistent with the ideas of safety and risk.

MEMBER BROWN: We're going to be writing on a letter on this, so we need to have you to the primary progenitors of this to be on the same page and have an idea of what you want to do when we proceed. I tried to find part two of the introduction with what I had, and I didn't --

CHAIRMAN STETKAR: You couldn't find it either.

MEMBER BROWN: Well, I didn't go on the internet to find it. I was looking --

CHAIRMAN STETKAR: That's okay. We can, I'm sure the staff --

MEMBER BROWN: I have one remaining question. The way this reads in item three on page seven of the introduction, according to what you pointed out, the introduction to NUREG 800, introduction part two describes the licensing review philosophy and framework to be applied by the staff for new IPR and COL applications under Part 52 with the incorporation of risk insight classified as follows, and that's the table. That's in the DSRS introduction item three, page seven.

Then it goes on to the next page where it goes 3A, and 3A then, whatever part two says is part two, but now it says specifically for A1 and A2 they will involve detailed analysis, as you said. So I don't know if there's an inconsistency between part two and what it says and what it says here because I don't know what's in part two. That's my concern after listening to the -- is there an inconsistency within the DSRS relative to what part two says, relative to what 3A says, because that literally, as you pointed out, is very specific that they will be detailed and B1 and B2 will be somewhat less detailed because they're non-safety related only. I'm just looking --

CHAIRMAN STETKAR: I didn't see an -- you

know, when I read those sections, I didn't see that kind of, if you want to consider it a --

MEMBER BROWN: Between part two?

CHAIRMAN STETKAR: Right.

MEMBER BROWN: Well, I don't know that's in part two. I couldn't -- I didn't know what that was.

MEMBER BLEY: I just got part two. That's where it's supposed to be.

MEMBER BROWN: Okay.

CHAIRMAN STETKAR: Anyway, we can do some --

MEMBER BROWN: We can look around on that. All right. We'll just have to come to some conclusion. Anything else from anybody else on this issue? Did you want to say something else?

MR. JONES: Just one last comment.

MEMBER BROWN: Name again just to make sure?

MR. JONES: It's Mike Jones.

MEMBER BROWN: Okay.

MR. JONES: And, again, the use of the methodology that's in the new part two introduction gives each reviewer and each group and each discipline a tool to risk-inform their particular review. And so

if, in fact, I&C has taken a look at this and said we've taken that opportunity and we don't see a practical way to implement that, they've, in essence, done what they could do under the new methodology.

CHAIRMAN STETKAR: And I think I'll just speak for myself because that's all I can speak for. I wouldn't have a problem with that if it was presented that way. We recognize the framework and, for practical reasons, in this particular area, we don't feel that we can distinguish between A1 and A2. It's not a problem.

MR. JONES: So it may just be a language issue here. I think they've done their best to try and apply the general guidance, which is consistent with what you were looking for. Maybe we have to dress it up better.

But the last thing is the whole methodology here, the whole use of DSRSs and this conformed methodology, is optional. Nobody is required to do this. Applicants are not required to use it. They can -- use Westinghouse, for example. They may say we don't want application engagement.

CHAIRMAN STETKAR: That's fine. I mean, that's their decision. The staff then performs the review based on however the applicant wants to submit

their application. But if there are applicants who are interested in heading down this pathway, you know, I think, collectively, we need to be sensitive to that notion and make sure that we apply it consistently and that we don't somehow provide disincentives to that whole process.

MR. JONES: One last comment. Whether you apply this or not, the acceptance criteria for the SSCs don't change. It's giving you a different method to decide whether you've satisfied the criteria or not, but the acceptance criteria themselves don't change.

MEMBER BLEY: I'm going to toss in a last thing on this, too. I did get a chance to look at part two. I can't find the words in the text yet, but the picture and the words on it, if we're consistent with that, I'd be much happier than I am with what I read. But I've got to look at it some more. That's the first look.

MEMBER BROWN: Okay. Are you ready for your summary page? Did we finish with that?

CHAIRMAN STETKAR: I let them get through with everything before -- I was looking at this slide when I brought up the topic.

MEMBER BROWN: John, in spite of the fact

that we started 15 minutes late, I am turning this back over to you 20 minutes early. That is management of the first degree. I'm expecting some action in return.

CHAIRMAN STETKAR: I'm eternally thankful. Do we have, by the way, because we have to do this, any one in the room who'd like to, members of the public in the room who'd like to make a comment? And, Christina, if we can get the bridgeline open, if there's anyone out there who would like to say anything. I think we may be open. If there is anyone out on the bridgeline, just do us a favor and say hello or utter some words so we know that it's open. Is there anyone out there?

PARTICIPANT: Yes.

CHAIRMAN STETKAR: Thank you very much. Trust me, if you've not gone through this process, we have no way of knowing that the bridgeline is open in this direction without someone saying something. Now, given the fact we know it's open, is there any member of the public or anyone else on the bridgeline who would like to make a comment?

PARTICIPANT: Nothing here.

CHAIRMAN STETKAR: Thank you very much. Hearing nothing, thanks very much to staff. You've

covered the material, and I think we had a fruitful discussion. And with that, we are in recess until -- come back at ten minutes to four. I'll give you 20 minutes, but we have a lot of things to cover.

(Whereupon, the above-entitled matter went off the record at 3:27 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

John Thorp (NRR)
Richard Stattel (NRR)
Michael Waterman (RES)
Terry Jackson (NRO)

Agenda

- **Describe Reasons for this Rulemaking Activity**
- **Describe changes made to IEEE Std. 603**
- **Describe Proposed 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**
- **Discuss Draft Reg. Guide to update RG 1.153 which is 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 discussion between the NRC staff and applicants over the existing applicability statements (Clarification of applicability is needed)**

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

Maintenance Bypass (in Clause 6.7 of IEEE Std. 603-1991) Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features **shall** continue to meet the requirements of 5.1 and 6.3.

EXCEPTION: 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).

EXCEPTION Clause of Section 6.7

Maintenance Bypass (in Clause 6.7 of IEEE Std. 603-2009) Capability of a safety system to accomplish its safety function shall be retained while sense and command features equipment is in maintenance bypass. During such operation, the sense and command features **should** continue to meet the requirements of 5.1 and 6.3.

NOTE: 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:

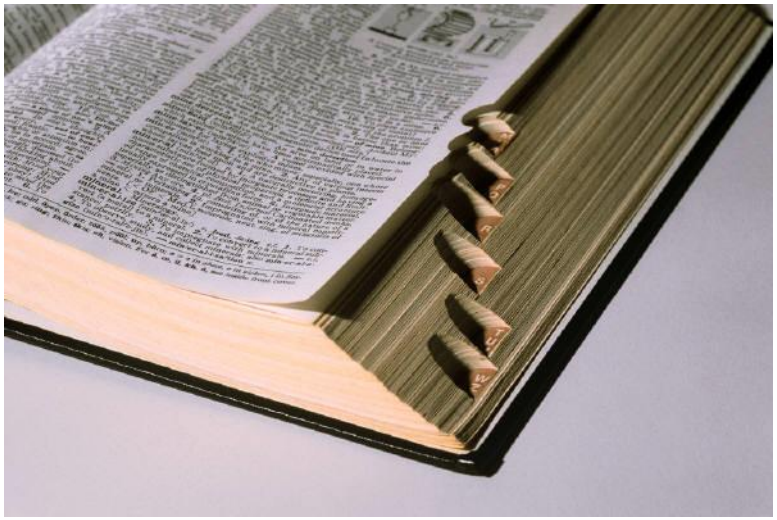
1. Provides definitions for several terms used in various standards and within the proposed regulation.

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.

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***
- ***Predictable***
- ***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:

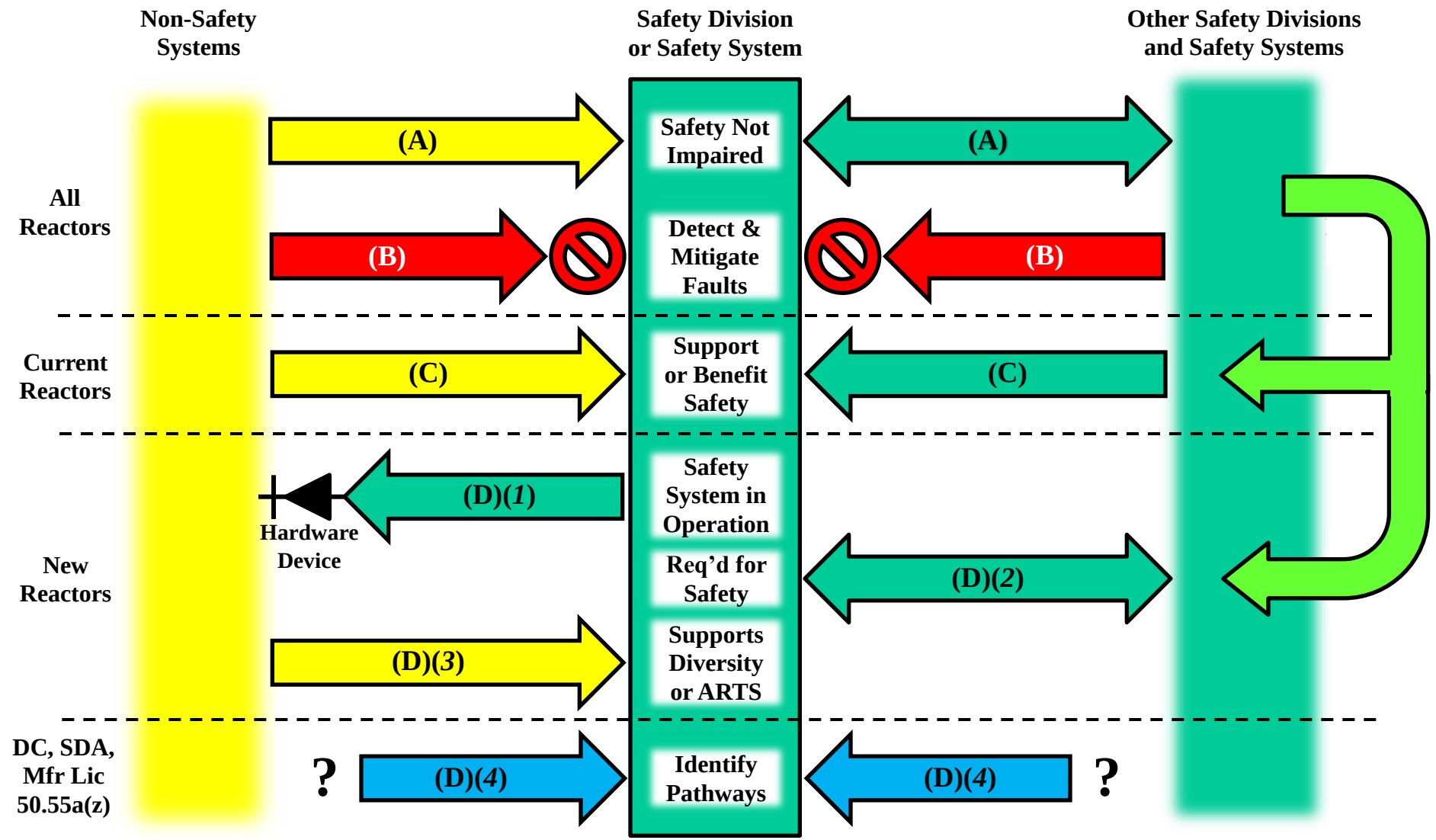
In order to assure the integrity and reliable operation of safety systems, safety functions shall be designed to operate in a predictable and repeatable manner.

Independence

General Independence Requirements 10 CFR 50.55a(h)(5)(i) & (5)(ii)

- **Address independence between**
  - **Redundant portions of safety systems – (5)(i)**
  - **Safety systems and other systems - (5)(ii)**
- **Analyze**
  - **Safety system internal and external hazards**
  - **Extent of interconnectivity**
  - **Impact of failures and degradation**
- **Digital communication independence extended to include other signal technologies**
  - **5.6.3.1.a.2.ii**
  - **5.6.3.1.b**

Specific Independence Requirements
10 CFR 50.55a(h)(5)(i)



Diversity & Defense-In-Depth

Defense-In-Depth Criteria

Staff Requirements Memorandum to SECY 93-087

I. Demonstrate that vulnerabilities to common-cause failures have been addressed.

2. Evaluate to demonstrate adequate diversity within the safety system for each design basis event in the accident analysis.

3. 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.

4. 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.

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

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), (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.

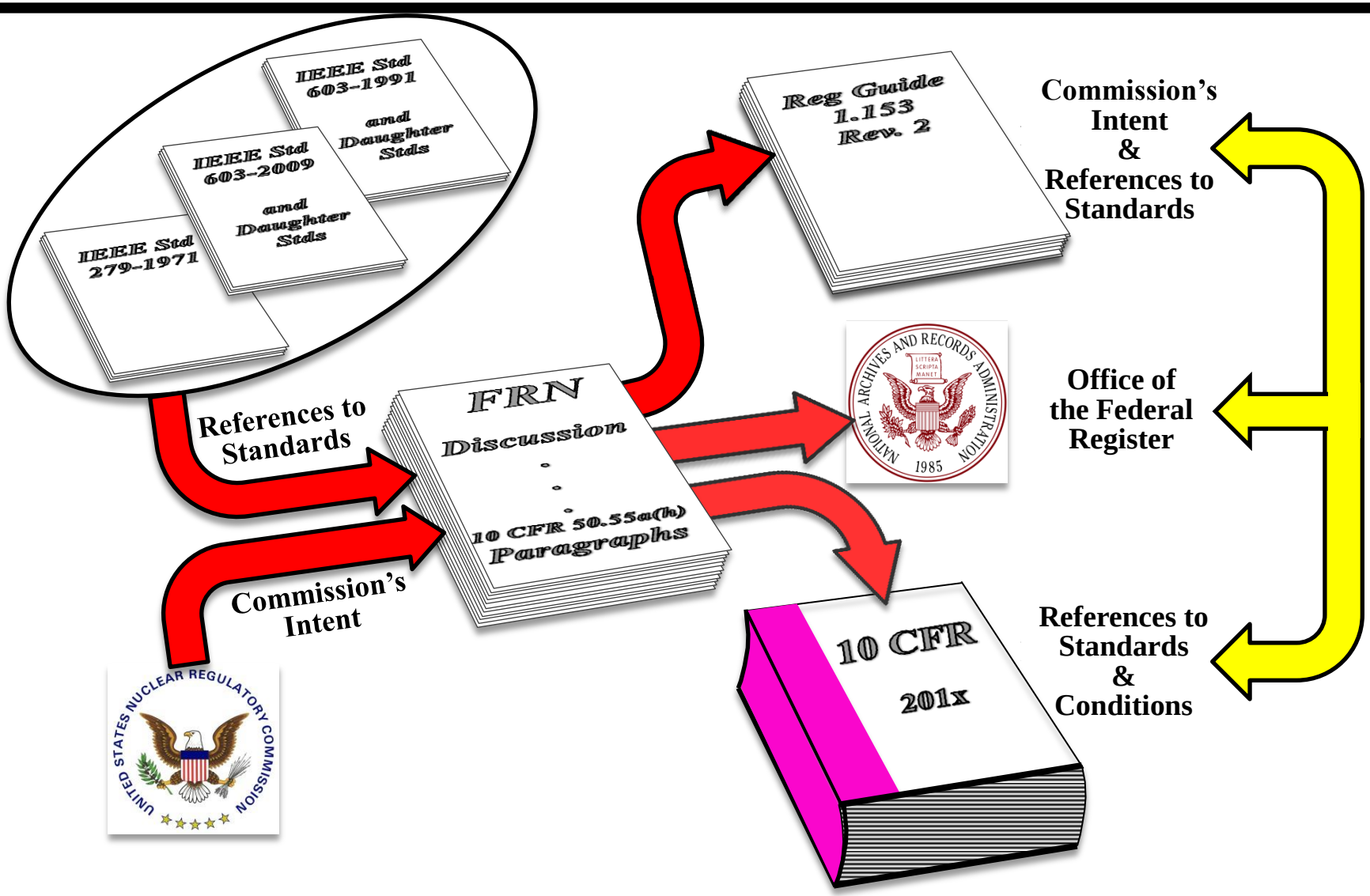
Draft Reg. Guide 1.153

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).

10 CFR 50.55a(h) and Reg Guide 1.153



Draft Reg Guide 1.153

- **10 CFR 50.55a(h) FRN provides the underlying basis of the regulation**
- **Consistent interpretations**
- **NRC website is the logical repository**
- **NRC website thereby provides Commission's**
  - **definitions of terms**
  - **reasoning behind Rule paragraphs**
  - **NRC Staff commitments on applying the Rule**
- **No time limit on availability of underlying basis**

END

Peach Bottom Atomic Power Station Extended Power Uprate

Advisory Committee on Reactor Safeguards

July 09, 2014

Exelon Generation®

Introductions

Peach Bottom Atomic Power Station (PBAPS) Extended Power Uprate

Agenda

- Introductions
- EPU Project Overview
  - Background
  - Modification Summary
- Elimination of Containment Accident Pressure (CAP) Credit
- Replacement Steam Dryer Overview
  (closed session)

Key Team Members Present

- Kevin Borton - Power Uprate Licensing Sr Manager
- Craig Lambert - Power Uprate Vice President
- Mike Massaro - PBAPS Site Vice President
- John Rommel - Power Uprate Engineering Director
- Ken Ainger - EPU Project Management Director
- Jim Armstrong - PBAPS Regulatory Assurance Manager
- Dave Henry - PBAPS Sr Manager Design Engineering
- Jim Kovalchick - PBAPS Sr Manager Operations, EPU Integration
- Tony Hightower - PBAPS Operations Shift Supervisor

EPU Project Overview

Background

Modification Summary

Mike Massaro

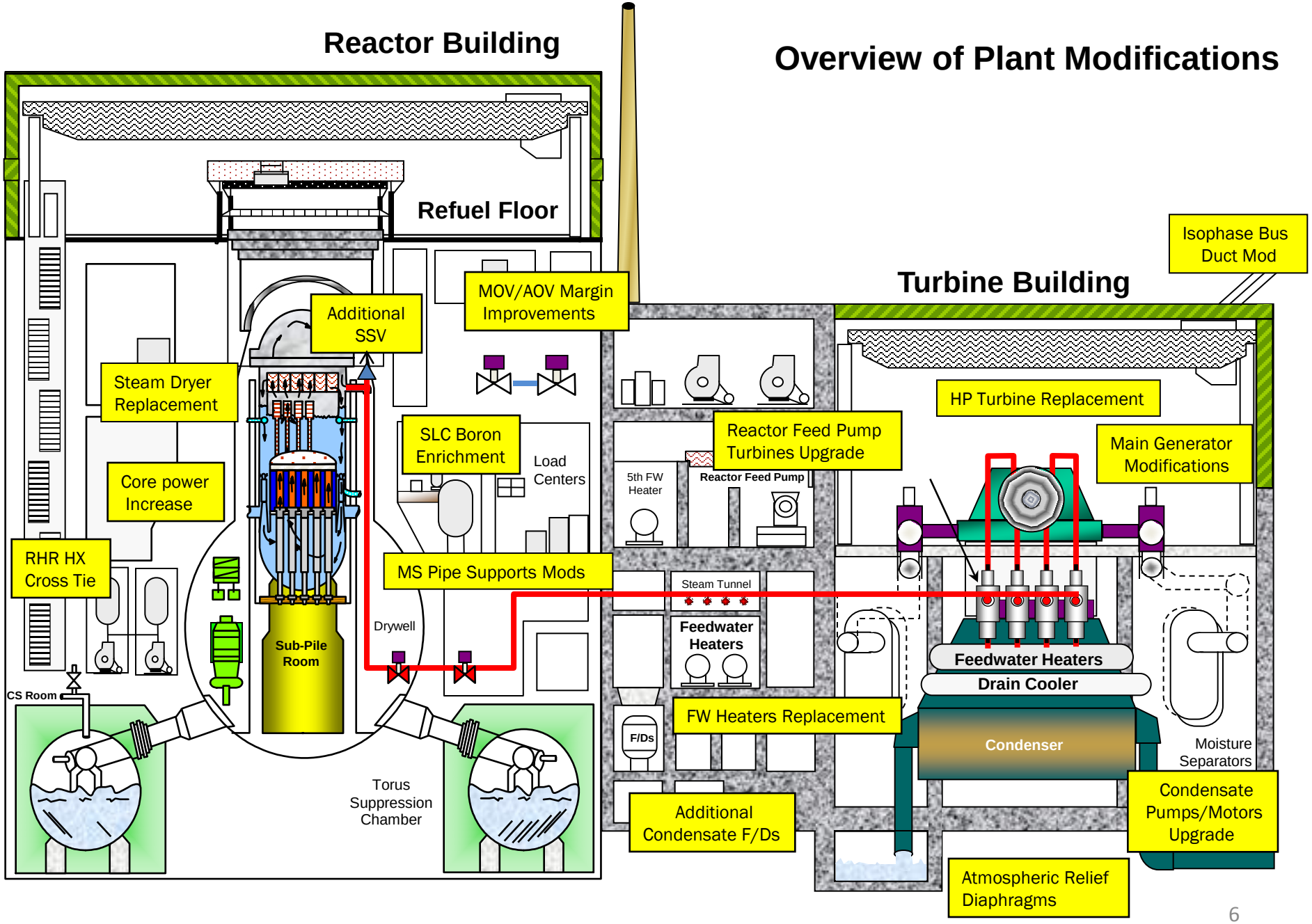
PBAPS Site VP

Background

Peach Bottom Atomic Power Station Overview

- GE BWR 4 Mark I Containment
- Operating License issued 1973 (U2) and 1974 (U3)
- Commercial Operation commenced 1974
- Renewed License issued in 2003 (U2 and U3)
- Licensed Thermal Power History
  - Original Licensed Thermal Power (OLTP) 3293 MWt
  - Stretch Uprate in 1994 and 1995 3458 MWt
  - MUR power uprate in 2002 to CLTP 3514 MWt
  - Proposed EPU (20% OLTP, 12.4% CLTP) 3951 MWt

Overview of Plant Modifications



Major Modification Summary

Modifications to Improve Reliability and Operating Margins

High Pressure Turbine Replacement
Accommodates increase in steam flow at EPU
Improves operating margin for Main Turbine Control system

Main Generator Modifications
U3 rotor replaced in 2013, U2 rotor to be modified for new rating
Restores generator margin at higher MVA at EPU

Isophase Bus Duct
Several portions of existing IPBD will be replaced
Restores IPBD margin at higher MVA at EPU

Feedwater Heaters
Replace five (1 on U2 and 4 on U3) to restore margin at EPU conditions
Other FW heaters analyzed and verified to be acceptable for EPU

Reactor Feed Pump Turbine Upgrades
Accommodates higher blade stresses at EPU
Improves reliability

Major Modification Summary

Modifications to Improve Reliability and Operating Margins (continued)

Motor Operated Valves
MOVs affected by changes in EPU response were evaluated
Improves margin at EPU conditions

Additional Main Steam Spring Safety Valve (SSV)
One additional SSV on each unit
Increases margin for ATWS analysis at EPU

Main Steam Piping
New supports and support modifications
Assures margin to Code requirements at EPU conditions

Reactor Water Cleanup
Flow diffusers to be installed on all four RWCU demineralizers
Improves efficiency to maintain chemistry limits at EPU conditions

Major Modification Summary

Modifications to Improve Reliability and Operating Margins (continued)

Condensate Pump/Motor Upgrades
Impellers to be replaced and larger motors installed
Improves margin at EPU conditions

Condensate Filter/Demineralizer
Two additional demineralizers to be installed on each unit
Maintains chemistry limits and operational flexibility at increased FW flowrate

ATWS-Recirculation Pump Trip
The ATWS-RPT relocated from MG sets to Recirculation Pump motor breaker
Provides faster coastdown time for Recirculation Pumps to support ATWS analysis

Replacement Steam Dryer
Replacing steam dryers to improve structural margin
Improves Moisture Carryover (MCO) performance lowering in-plant radiation doses

Major Modification Summary

Modifications Associated with CAP Credit Elimination

RHR Heat Exchanger Cross-Tie
Includes new cross-tie valve allowing two HXs to be supplied from one RHR pump
Increases RHR heat removal capability

HPSW Cross-Tie
Replaces existing cross-tie with valve able to open against full flow differential pressure
Increases RHR heat removal capability

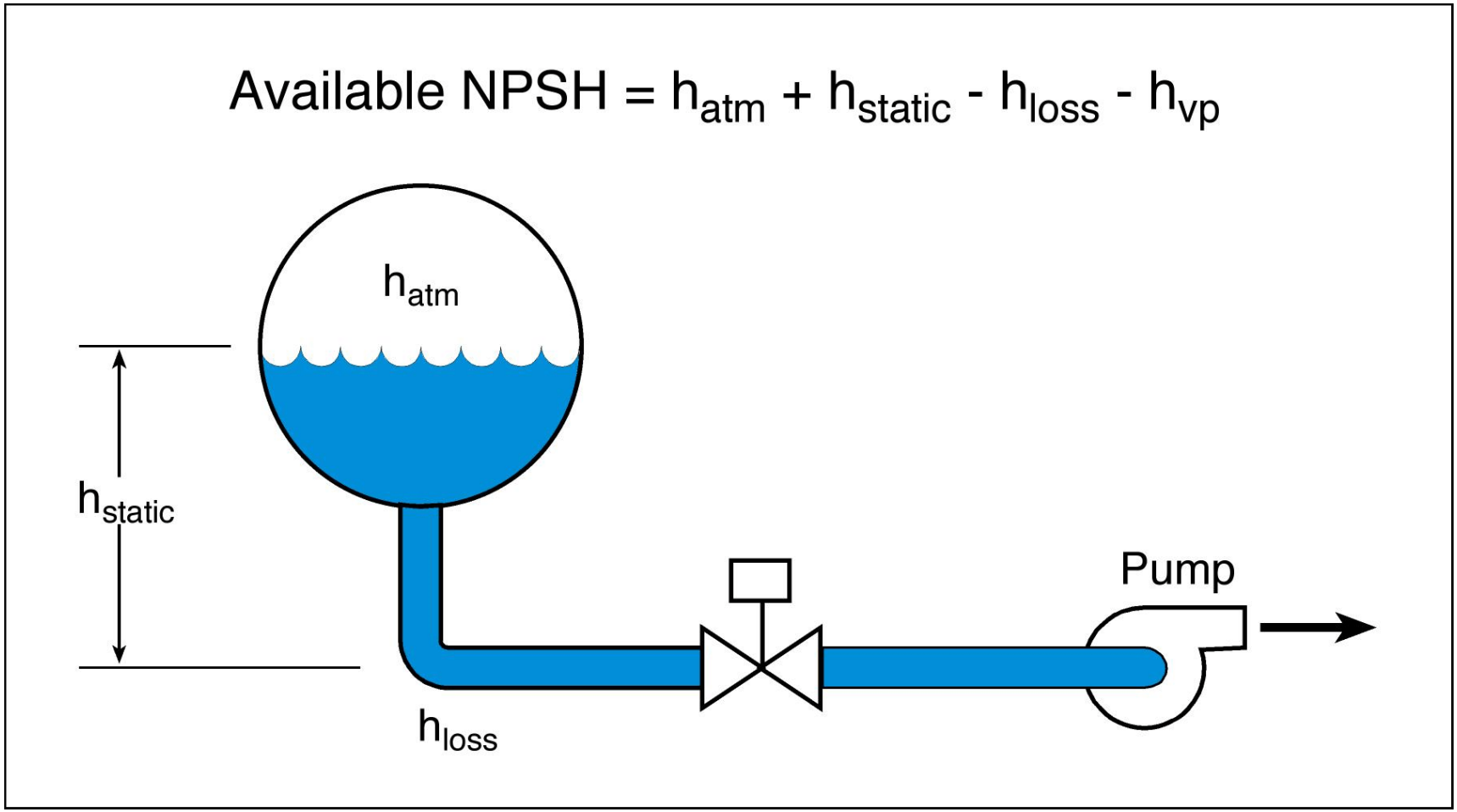
Condensate Storage Tank
Provides protected CST volume and safeguards against fire-induced swapover to torus
Allows crediting of CST as suction source

Standby Liquid Control System
Boron-10 enrichment increased to 92 atom percent in SLC Storage Tank solution
Lowers Suppression Pool temperature during ATWS

Elimination of Containment Accident Pressure Credit

John Rommel
Power Uprate Engineering Director

Elimination of CAP Credit



Elimination of CAP Credit

- Opportunity to improve margins and remove concerns associated with Containment Accident Pressure (CAP) Credit
- Became key project goal
- Credible options existed to eliminate CAP Credit at PB

Elimination of CAP Credit

Actions to Eliminate CAP Credit

- Increase Residual Heat Removal (RHR) system heat removal capability
  - RHR and High Pressure Service Water (HPSW) cross-tie modifications
  - Increase RHR Heat Exchanger (HX) K-Value
- Reduce RHR pump flow
- Credit Condensate Storage Tank (CST) as suction source for special events
- Increase Standby Liquid Control (SLC) system Boron-10 enrichment

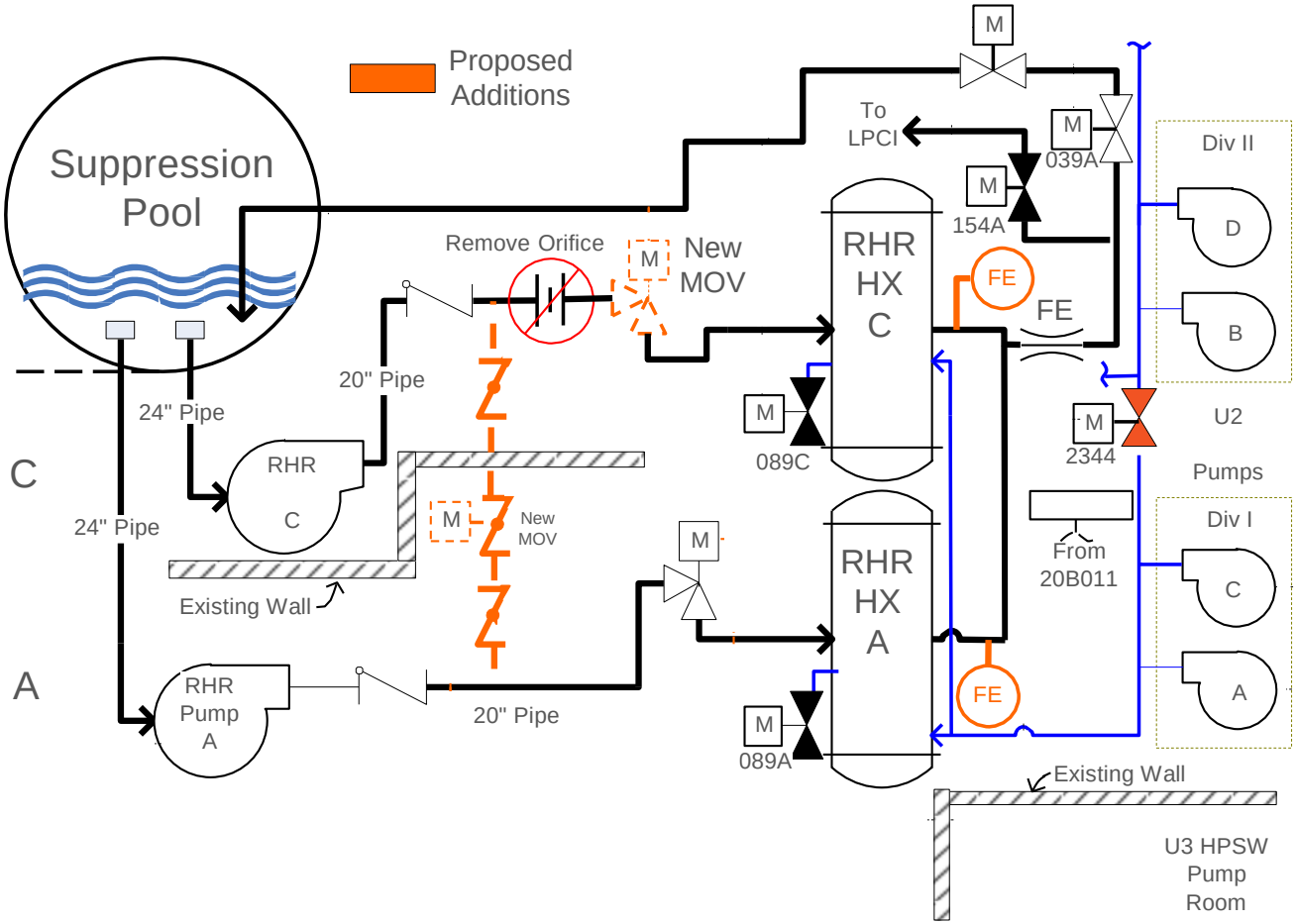
Elimination of CAP Credit

Methodology

Modification or Analytical Change	DBA-LOCA	SSLB	App R	ATWS	SBO
RHR HX Cross-tie and HPSW Cross-tie mods	X	X			
Increased single RHR HX K-Value from 270 to 305	X	X	X	X	X
Reduced RHR flow rate from 10000 gpm to 8600 gpm	X	X	X	X	X
Credit CST as HPCI and/or RCIC suction source			X	X	X
Increase SLC Boron Enrichment				X	

Elimination of CAP Credit - Accidents

U2-DIV I RHR and HPSW Cross-Tie

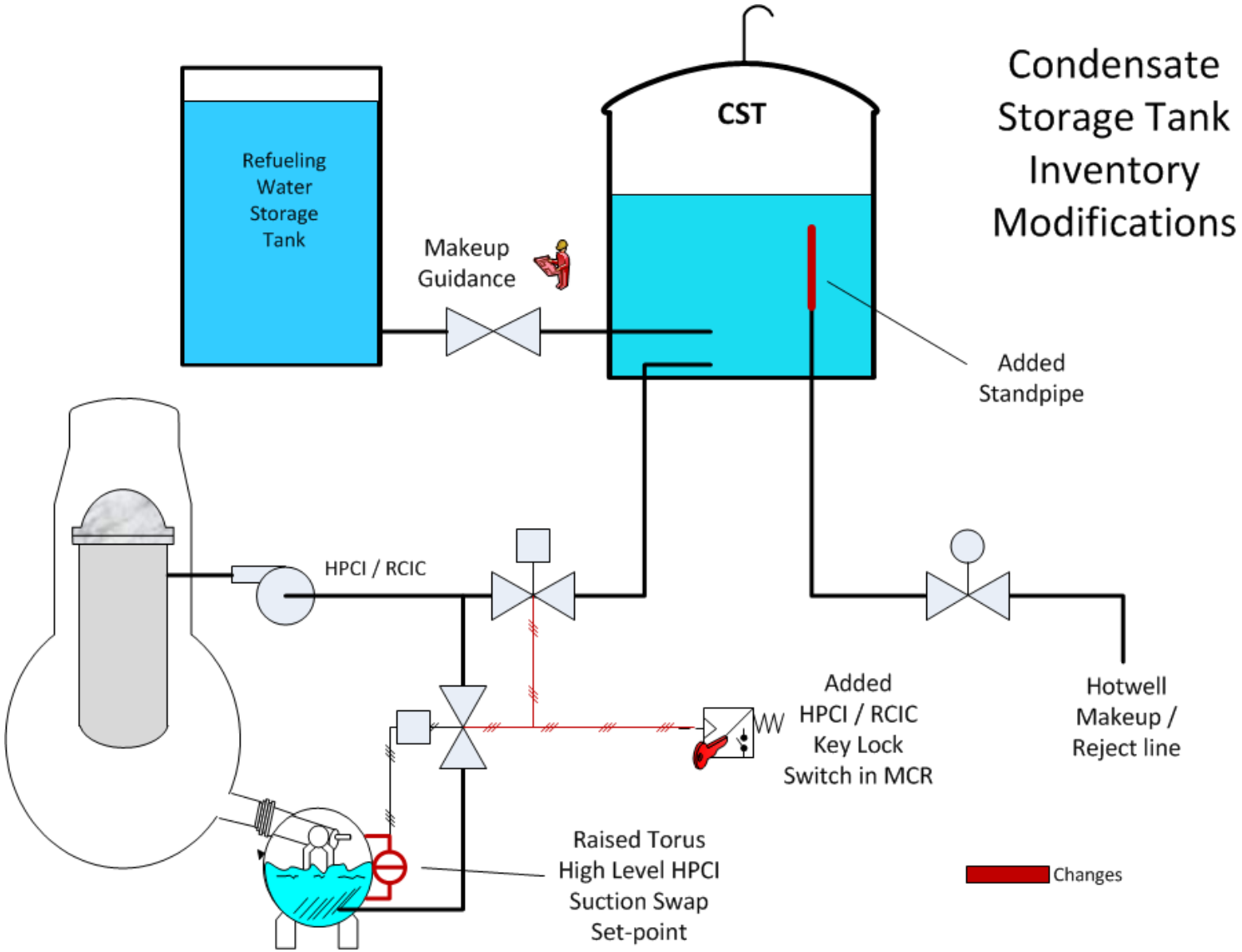


Elimination of CAP Credit - Accidents

RHR/HPSW Cross-tie Modifications

- Modifications will:
  - Allow two RHR HXs to be supplied from one RHR pump
  - Improve rate of Suppression Pool cooling
  - Lower peak Suppression Pool temperature, increasing NPSHA
  - Lower required RHR flow, decreasing $NPSHR_{eff}$
- Modifications consist of:
  - New cross-tie line with a normally closed cross-tie isolation on discharge of RHR pumps
  - New flow control valves upstream of each heat exchanger to balance flow
  - Replacement of existing HPSW cross-tie valve with one that can be repositioned against the full flow and differential pressure of a single HPSW pump

Elimination of CAP Credit - Special Events



Elimination of CAP Credit – Special Events

CST Modifications

- Modifications will:
  - Ensure adequate inventory in CST
  - Ensure that HPCI /RCIC pump suctions remain aligned to the CST
  - Produce additional heat capacity in Suppression Pool
  - Lower peak Suppression Pool temperature, increasing NPSHA
  - Provide additional volume (height) in torus, increasing pump NPSHA

- Modifications consist of:
  - A standpipe to protect the CST volume
  - Installation of key lock switches in the Control Room to prevent inadvertent suction source swap
  - Raising torus high level setpoint to prevent premature automatic switch of HPCI suction to Suppression Pool
  - Revised procedural guidance to ensure adequate CST inventory makeup from RWST

Elimination of CAP Credit

Conclusions

-For all events

- NPSHA > $NSPHR_{eff}$

-No CAP Credit is required

CLOSED SESSION

Replacement Steam Dryer - Exelon

Acronym List

- ATWS – Anticipated Transient Without Scram
- BOP – Balance of Plant
- BWR – Boiling Water Reactor
- BWRVIP – Boiling Water Reactor Vessel Internals Program
- CD – Condensate System
- CLTP – Current Licensed Thermal Power
- CLTR – Constant Pressure Power Uprate
- CPR – Critical Power Ratio
- CRDA – Control Rod Drop Accident
- CST – Condensate Storage Tank
- DBLOCA – Design Basis Loss of Cooling Accident
- EPU – Extended Power Uprate
- HP – High Pressure
- HPCI – High Pressure Coolant Injection
- HPSW – High Pressure Service Water
- HX – Heat Exchanger
- MASR – Minimum Alternating Stress Ratio
- Mlbm – Million pound mass
- MNGP – Monticello Nuclear Generating Plant
- MOV – Motor Operated Valve
- MPS – Minimum Recirculation Pump Speed
- MS – Main Steam
- MSIV – Main Steam Isolation Valve
- MSL – Main Steam Line
- MWT – Megawatt Thermal
- NPSH – Net Positive Suction Head
- NPSHA – Net Positive Suction Head Available
- NPSHR – Net Positive Suction Head Required
- $NPSHR_{eff}$ – Effective Net Positive Suction Head Required
- NSSS – Nuclear Steam Supply System
- OLTP – Original Licensed Thermal Power
- PBAPS – Peach Bottom Atomic Power Station
- PORC – Plant Operations Review Committee
- PRFO – Pressure Regulator Failure Open
- psia – pounds per square inch absolute
- psig – pounds per square inch gauge
- RCIC – Reactor Core Isolation Cooling
- RCPB – Reactor Coolant Pressure Boundary
- RHR – Residual Heat Removal
- RIPD – Reactor Internal Pressure Difference
- RPV – Reactor Pressure Vessel
- RSD – Replacement Steam Dryer
- RTP – Rated Temperature and Pressure
- RWST – Refueling Water Storage Tank
- SBO – Station Blackout
- SRV – Safety Relief Valve
- SLC – Standby Liquid Control
- SSLB – Small Steam Line Break
- TS – Technical Specification
- VPF – Vane Passing Frequency

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACRS Full Committee Meeting

NRC Staff Review of Extended Power Uprate for Peach Bottom Atomic Power Station Units 2 and 3

July 9, 2014

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Opening Remarks

Louise Lund

Deputy Director
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Background

- **Peach Bottom Proposed EPU:**
  - **3514 to 3951 Megawatts Thermal (MWt)**
  - **12.4% increase**
- **EPU Review done with Review Standard RS-001:**
  - **RS-001 used for 17 EPUs since 2005**
- **No open items in draft safety evaluation**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Introduction

Rick Ennis

Senior Project Manager
Division of Operating Reactor Licensing
Office of Nuclear Reactor Regulation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Review Schedule

- **September 28, 2012 – Application submitted to NRC.**
- **February 15, 2013 – Exelon submits supplemental information.**
- **March 8, 2013 – Application accepted by NRC for review.**
- **September 8, 2014 – NRC forecast for review completion based on 18 months from date of acceptance.**

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda

- **Plant Modifications**
- **Elimination of Credit for Containment Accident Pressure**
- **Steam Dryer Analysis**

U.S.NRC

UNITED STATES NUCLEAR REGULATORY COMMISSION

Protecting People and the Environment

ACRS Full Committee Meeting mPower DSRS Chapter 7, I&C July 9, 2014

Tim Mossman
Joe Ashcraft
Ian Jung
Office of New Reactors

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Agenda

- Objectives of DSRS Chapter 7
- Development of Section 7.2.1, Quality
- ACRS Recommendations
- Other ACRS Comments Resolved
- Summary

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Objectives of DSRS Chapter 7

- Reorganize review guidance
  - Fundamental design principles
  - Safety focus and efficiency
- Remove redundant and non-applicable information
- Incorporate lessons learned from large light-water reviews
- Introduce the use of hazard analysis

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Development of Section 7.2.1, Quality

- Section added after 2012 ACRS meeting
- Goal to enhance coordination between I&C reviewers and quality assurance (QA) staff
  - Strategy uses qualified QA staff to review QA programs
  - I&C reviewers focus on aspects of quality that may be unique to I&C systems

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACRS Recommendation 1

Full Committee Letter 12/18/2012

DSRS Chapter 7 should be issued for industry and public comment

Summary Formal Public Comments

- Comments on Chapter 7 primarily received from Generation mPower, NEI, and NuScale
- The full DSRS received nearly 2000 comments
  - 119 comments received on Chapter 7
- None of the resulting comment resolutions altered the staff's approach to Chapter 7

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACRS Recommendation 2

Full Committee Letter 12/18/2012

DSRS provides a review standard that is likely to be applicable to large reactor designs…[and] other…SMRs.

The staff agrees that Chapter 7 of the DSRS may have applicability beyond the mPower review.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACRS Recommendation 3

Full Committee Letter 12/18/2012

A specific design implementation should be applied to comply with control of access

Control of Access

- Staff acknowledges the Committee's concern and position
- Resolution of this recommendation has wider applicability than just for the mPower DSRS and involves policy-level issues
- The staff intends to develop a SECY paper regarding a number of I&C technical issues which would address the ACRS recommendation

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

ACRS Recommendation 4

Full Committee Letter 12/18/2012

DSRS Chapter 7, Appendix B, Instrumentation and Controls System Architecture, should be augmented

System Architecture

DSRS 7.0 APPENDIX B

3. Diagrams of the overall architecture should illustrate the I&C system architecture principles and concepts (as addressed in Item 1 above). The staff review should ensure that sufficient detail is provided as follows:

   A. Physical architectures to include

      i. All of the safety systems and relevant control systems

      ii. Connections between the above systems

      iii. Identification of signal / data barrier devices

   B. Functional block diagrams to include

      i. Major components from sensor(s) to actuation device(s), including various channels / divisions used for signal / data processing, voting unit(s) and actuation devices

      ii. Signal / data flow paths

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Other ACRS Comments Resolved

DSRS 7.1.2 - INDEPENDENCE

III.9 Priority modules should be safety-related. A command initiating a safety function should have the highest priority and should override lower priority commands. Any instance in which a command initiating a safety function does not have the highest priority should be identified and the conditions that justify the reduction in priority should be explained. All requirements that apply to safety software should also apply to priority module software. The priority module software should be stored in the nonvolatile memories to prevent online alteration.

DSRS 7.2.13 - DISPLAYS AND MONITORING

I.6 Severe accident and PRA evaluations in the application to confirm that information displays conform to analyses of severe accidents and any applicable Fukushima-related orders.

In addition, operating experience staff should be consulted to determine if any operating experience relevant to displays and monitoring may inform the staff's review of this section.

DSRS 7.2.11- MULTI-UNIT STATIONS

III.2.D Failure or undesirable behavior of non-safety I&C systems shared among multiple units do not impair the ability of the I&C systems to perform credited safety functions in individual units.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Other ACRS Comments Addressed

7.1.2 INDEPENDENCE

III.3 For designs that implement sharing of data between trip processing units and voting unit processors, or among voting unit processors, the reviewer should confirm that the proposed design includes provisions to cope with a trip processing unit or voting unit processor experiencing a lock-up condition (also known as hang or freeze), whether the processor controls a reactor trip or engineered safeguards system function. Such design provisions should include the following:

A. Any voting unit processor or trip processing unit experiencing a lock-up condition will produce an alarm in the main control room and send a trip signal to all voting unit processors or trip processor units for that channel/division.

B. If any two or more voting unit processors or trip processing units experience a simultaneous lock-up condition, an alarm will be displayed in the main control room and a reactor trip will result.

C. The means used for ensuring that a trip signal is produced from either a trip processing unit or voting unit processor that experiences a lock-up condition should be completely independent among safety divisions, should be hardware-based, and completely independent of software.

U.S.NRC
UNITED STATES NUCLEAR REGULATORY COMMISSION
Protecting People and the Environment

Summary

- DSRS Chapter 7 is ready to be piloted for a review of digital I&C
- Staff has interacted with numerous stakeholders throughout this process
  - Overall, staff received highly positive feedback from the stakeholders
- Staff achieved the objectives for the guidance, which will contribute to more efficient and effective licensing reviews