Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, November 21, 2019

Work Order No.: NRC-0681 Pages 1-245

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

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL I&C SUBCOMMITTEE

+ + + + +

THURSDAY

NOVEMBER 21, 2019

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

The Subcommittee met at the Nuclear Regulatory Commission, Two White Flint North, Room T2D10, 11545 Rockville Pike, at 10:00 a.m., Charles H. Brown, Jr., Chair, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR. Chair

RONALD G. BALLINGER, Member

DENNIS BLEY, Member

VESNA B. DIMITRIJEVIC, Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member

JOY L. REMPE, Member

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

CONTENTS

Opening Remarks 4

Introductory Remarks 13

Draft BTP 7-19, Rev.8 17

Industry Perspectives on Common Cause 150
Failures (CCFs) in Digital Systems

EPRI R&D Perspectives on Digital I&C 205
Reliability and Software CCF

Public Comments 242

Closing Remarks 243

P R O C E E D I N G S

10:02 a.m.

CHAIRMAN BROWN: (Presiding) The meeting will now come to order.

This is a meeting of the Digital I&C Subcommittee. I'm Charles Brown, Chairman of the Subcommittee.

ACRS members in attendance are Dennis Bley, Joy Rempe, Ron Ballinger, Walt Kirchner, Jose March-Leuba, Vesna Dimitrijevic, Myron Hecht, and I'm here.

Christina Antonescu of the ACRS staff is the Designated Federal Official for this meeting.

The purpose of the meeting is for the staff to brief the Subcommittee on Revision 8 to Branch Technical Position 7-19, the Guidance for Evaluation of Diversity and Defense-in-depth in Digital Computer-Based Instrumentation and Control Systems.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act. The NRC implements FACA in accordance with its regulations found in Title 10 of the Code of Federal Regulations, Part 7. The Committee can only speak through its published letter reports. We hold meetings to gather

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

The rules for participation in today's meeting have been announced as part of the notice of this meeting previously published in The Federal Register. The rules for participation in all ACRS meetings was announced in The Federal Register on June 3rd, 2019.

The ACRS section of the U.S. public website provides our Charter/Bylaws, agendas, letter reports, and full transcripts of all full and subcommittee meetings, including slides presented at the meetings. The meeting notice and agenda for this meeting were posted there.

Portions of this meeting can be closed as needed to protect proprietary information, pursuant to 552b(c)(4), as stated in The Federal Register notice and in the public meeting notice posted to the website.

Members of the public who desire to provide written or oral input to the Subcommittee may do so and should contacted the Designated Federal Official five days before prior to the meeting, as practicable.

We have also set aside 10 minutes for comments from members of the public attending or listening to the meeting via the phone. We have not received any written comments or requests for time to make oral statements from members of the public regarding today's meeting.

A transcript of the meeting is being kept and will be made available on the ACRS section of the U.S. NRC public website.

We request that participants in this meeting please use the microphones located throughout the meeting room when addressing the Subcommittee. Participants should first identify themselves and speak with enough volume and clarity, so that they can be readily heard.

A telephone bridge line has been established for the public to listen to the meeting. To minimize disturbance on the public line, it will be kept in a listen-only mode. Also to avoid disturbance, I request that attendees, including myself, put their electronic devices --

MEMBER REMPE: Is that electronic?

(Laughter.)

CHAIRMAN BROWN: This is an electronic device, yes. It's only 19 years old. Yes, I can

text, barely.

Where was I?

I request you put your electronic devices like cell phones in the off or noise-free mode.

We will now proceed with the meeting. And before I call on Mr. Benner to introduce himself and his staff, I will call on Member Bley, who has some opening comments also.

MEMBER BLEY: Yes. Thanks, Charlie. I appreciate it.

I just wanted to get some things out. So, maybe it will help you in the presentation address some of these issues that I want to flag before you get there.

One is a logic issue and one is a matter of your text. On the logic issue, and you're not the only group we've had this same conversation with, to me, if something is safety-significant -- that's A1 and B1 in your nomenclature -- it's been shown by analysis to actually have an impact on safety.

And A1 is both safety-related and safety-significant, and certainly deserves high attention. B1 I don't understand, and never have, why it would be mixed with A2, which is safety-related, but not safety-significant. It's not a real contributor to

safety, but it's there for things that we really want. But why you would treat B1 and A2 together and A1 separately, I don't understand. Since both A1 and B1 are safety-significant, they're big contributors to safety, I don't see why they aren't treated the same. That's the logic piece.

The textual piece is in your procedure for carrying out the D3 analysis for A1. That's Section B3. This is my opinion. In your efforts to be very precise and not be misunderstood, you have made the language to me incomprehensible. If you simplified the language a great deal and stuck with your figure, and linked it to the figure more closely, I think it would be much easier for people to use. And you keep referring back to the positions and you go back and forth and reiterate things over and over again, to the point I lose track of what I'm supposed to do when I'm reading it. So, just those two things.

CHAIRMAN BROWN: Dennis, which part of 719? Was that Section 3?

MEMBER BLEY: Yes.

CHAIRMAN BROWN: Is that the DID assessment you're talking about?

MEMBER BLEY: Yes.

CHAIRMAN BROWN: That's item Section 3?

MEMBER BLEY: B3, and especially B3-1, which applies to the A1, the ones you want to be most careful about. I just find the procedure so convoluted. And clearly, it's an effort to be precise.

CHAIRMAN BROWN: Okay. I will amplify your comment. This is my comment on B3.

MEMBER BLEY: Okay.

CHAIRMAN BROWN: The entire Rev. 7, Section 3.1, of the acceptance criteria has been deleted and so wordsmithed in the rest of the document as to be unintelligible. R.7, Section 3.1, is a high-level, integrated set of information. Only Items 1 and 2 from R.7 are incorporated and they are watered-down. They are shortened considerably.

MEMBER BLEY: We didn't talk to each other.

CHAIRMAN BROWN: That's right, we didn't.

The entire Section 3.1 should be included as a preamble to the new acceptance criteria writeup. That whole old Section 3.1 had a wide-ranging, overall picture of what we mean by an assessment. I have no problem with the stuff after that. It's just that there's no context provided for what we're doing, which was in the old. So, I'm just echoing that the

assessment turned out, in my own mind, to be somewhat confusing.

The other new Section 3.12, "Use of Testing to Eliminate Further Consideration of Common Cause Failure," I could say -- and these are my opinions; this is not the Committee opinion; this is not the Subcommittee opinion; this is mine only -- it's written up pretty nicely. There's a lot of information. It's an expansion from the Rev. 7 version. But, by the time anybody finishes reading it and determining what they ought to do, anybody that concludes they're going to try to get stuff resolved by testing is out of their minds.

MEMBER BLEY: Yes.

CHAIRMAN BROWN: It's so hard and so difficult. That was another perception.

MEMBER BLEY: We'll get to that when you talk about it, but, to me, I put a big "X" through that. You have the right words if it's simple enough, but hard to get anything simple enough that you can fully test it.

CHAIRMAN BROWN: Exactly. Very few systems are going to be simple enough to use testing, and yet, there's a lot of emphasis. On 3.3, "The Defensive Measures," the acceptance criteria referred

to NR-approved methodologies as bases for crediting defensive measures. And I searched through the entire document trying to find where are defensive measures identified. They aren't, or at least I couldn't find them.

And then, in Section 3.2.2, "Crediting Manual Operator Actions," the critical paragraphs from Rev. 7, Section 3.5, paragraphs 3 and 4, are not there anymore. They were deleted or eliminated. And they provided valuable clarification and "what do we mean examples" which are valuable in the manual action assessments.

And then, under the acceptance criteria, Item A, the last sentence, it said, "for complex," and then, that's the beginning of the last sentence. The whole concept of less than 30 minutes is not existent in this document at all, as it has been historically in terms of, if an operator has less than 30 minutes to respond, then you have to give some real thought to what you're doing. And that's gone. I couldn't find anything on that.

And since we're still on 3.8, which is under B3 assessments, it discussed the types of diversity in 6303, the NUREG, saying there's six diversity types, et cetera, et cetera. But there's no

information on them. Section 3.8 in Rev. 7 actually provided examples and discussion relative to the types of diversity and related them to actual real-world applications, if you want to call it that, which is valuable. In other words, it's substituted words like "command" and "safe states," and stuff like that, which they're kind of jargon and slang. If you hadn't figured it out, I like the old 3.8.

And again, when you look at the section that's referred to with the 6303 words, it really needs a preamble, and the old 3.8 would be a nice preamble leading into it. The other stuff is okay. It's just context is lost relative to application.

Anyway, that's a few. I'm just amplifying Dennis' a little bit. I paid a lot of attention to that section since it seems to be kind of a meat-and-potatoes section. So, that's just a little heads-up. There's miscellaneous other questions I may get to at the end. I'm not going to try to interrupt you all the way through the presentation. I think it might be more useful to let you finish, and then, we'll bring up some questions. At least that's what I'm going to do. Whatever the Committee members want to do, they can do.

MR. MORTON: Yes, we'll try to touch on

those points as we get to the presentation to the best of our ability.

CHAIRMAN BROWN: Okay. Thank you very much.

Would any other members like to make any other opening comments?

(No response.)

Okay. Proceed. Who's going to open up? Eric?

MR. BENNER: Yes. Thank you, Members Brown and Bley.

CHAIRMAN BROWN: We finally got to Eric.

MR. BENNER: I think it was helpful to get some of your initial comments before because I think we all agree the whole purpose of this interaction is to allow the staff the opportunity to talk about what we've done and allow you to react. So, having some of your initial reactions in the front end I think will help. I mean, we're not going to like completely revise the presentation on the fly, but it ties us to the areas we should focus on. So, this is likely going to be a long day. So, anything we can do to focus on areas of lack of clarity or areas of disagreement I think serves both of us well.

So, I'm Eric Benner. I'm the permanent

Division Director of the Division of Engineering and External Hazards in NRR. Right now, I'm acting as Deputy Office Director for NRR, but this is an area near and dear to my heart. So, I've never strayed too far away from it.

I think the real reason why I didn't have a tabletop here is not that I need no introduction. It's because my role here is much less important than the roles of the people to my left. I have Deanna Zhang and Wendell Morton, who are both technical reviewers in my Division. Deanna and Wendell have both done actual licensing reviews for new reactors and operating reactors licensing actions as well as Topical Reports, supporting platform reviews that support licensing action. So, they've been instrumental in incorporating the lessons learned from their and the rest of the technical staff's reviews into revisions to this document. They're competent and capable enough that I believe they've had very effective dialogs with the stakeholders as to what's necessary to meet our regulatory findings.

My understanding is, hopefully, some of what we did was repackaging to make it simpler for a reviewer to go through. So, some of this, hopefully, will be an explanation of that.

I'll say regarding maybe some detail that's been lost, we may need to have a followup action just because, separate from this activity, there's a broader activity to look at the NRC's Standard Review Plan overall and try to focus it more on what truly are the acceptance criteria. And there's an acknowledgment that there's some level of detail in the Standard Review Plan that is valuable, but it's more of a knowledge management-type nature, and it may be better to move that information to a supplemental product.

So, that may be some of what happened here. And I think, in the absence of where that information would reside, I don't think we're going to make a decision here as to whether that information needs to be back in the BTP or kept somewhere else for posterity's sake. But it's good feedback to talk through that because I think we'll learn lessons here for the BTP and we can take that back to make sure that, as we do the broader Standard Review Plan modernization, we're not losing things that do have value to the technical reviewers.

With that, I'll turn it over to Deanna and Wendell to conduct the presentation.

CHAIRMAN BROWN: I'll make one other

observation that I forgot to bring up before. Again, I agree with you, we're not going to sit here and decide what we're going to put in and what we're going to put out. The purpose of us providing this initial input is to lay on the table some of the thoughts that, as you go forward, how do we not lose some of that valuable information.

The spurious operational is another example where we have made some comments in a letter back in 2011 on the Rev. 6, which you all incorporated very well and your all's responses twice. And it was also carried over into Rev. 7. But it did not get necessarily carried over into Rev. 8. And I'll point a couple of those out.

The other point I guess I would like to make is an overall point. Over the last few years, 10 or 12, all of the Committee's reviews have been focusing on what is the architecture look like. What's the framework and the architecture of the reactor trip or the reactor protection system, consisting of reactor trip systems and safeguards? And when you really get down -- again, this is my opinion, not the Subcommittee's or the Committee's -- when you really get down to evaluating diversity, it really needs to be done, and defense-in-depth, in

terms of the framework, the five fundamental principles.

Some architectures will demand a lot of stuff that you won't know you need if you've got a good architecture that truly meets all of the fundamentals. And the word "architecture" I don't think is mentioned once -- it might be once. I think I word-searched it last night. There might have been one word of "architecture" in there. I can't even remember where it was. But nothing relative to the fundamental principles and how diversity in-depth is needed to compensate for or as part of an assessment relative to the overall architectures.

I happen to think, as a lead-in to the overall Branch Technical Position, some discussion of the principles and the importance of diversity in DID relative to that architecture is important. Again, that's my opinion only. So, that was one thing I forgot to bring up.

Have at it, Wendell, Deanna.

MR. MORTON: Good morning, and thank you for the initial input and comments. We'll try to get to them as we go through the presentation and we'll try to follow up at a later time, since we do have a couple more meetings scheduled with the ACRS and to

follow up on. So, if we don't get to them all today, we will get to them, rest assured.

Once again, thank you, Eric, for the introduction. My name is Wendell Morton. I am the lead for this particular project to update the BTP 7-19.

I want to also introduce the working group team. To my right is Deanna Zhang, Paul Rebstock in the audience, David Rahn, and Rossnyev Alvarado. I want to thank them for all their efforts and contributions to this work.

I also want to thank the Steering Committee for their support on this, as well as the rest of the agency staff, including OGC, other folks from Office of Research, and the rest I&C community, NRR as well. I just want to introductions out of the way.

You'll have to excuse my voice. It's kind of coming in and out today. I'm trying to keep my voice as clear as possible.

So, for today's agenda, besides trying to cover some of the input we got earlier on, we are going to talk about some of the background on why this particular update was coming forth and the objective of this particular update, as well as we'll go into

some of the key changes we've kind of actually gotten into in terms of the introduction of the graded approach -- this is not a graded approach for the document for the first time -- the overall defense-in-depth approach. And we can kind of touch on Charlie's point about focusing specifically on an architectural level, rather than maintaining an overall defense-in-depth approach in terms of the four echelons of defense-in-depth, which is where the Commission's direction --

CHAIRMAN BROWN: Which also are lost in the new writeup. The echelons virtually disappeared from the lead-in part of the BTP.

MR. MORTON: Okay, and we can kind of touch on that a little bit as well.

CHAIRMAN BROWN: If you word-check "echelons," I think it's mentioned once, maybe twice.

MR. MORTON: Okay.

CHAIRMAN BROWN: Not a whole lot in the whole description of what the echelons are. It's almost like you have to go off and get 6303 and, then, go read that, which doesn't make a whole lot of sense.

MR. MORTON: Okay, and thank you for that comment, too.

We'll also talk about the means to

eliminate CCF from further consideration. This is the enhancement to the testing criteria. Other means we want to provide industry flexibility for to address CCF outside of the specific D3 process itself.

We'll talk about the qualitative assessment and its usage within the context of the BTP. We will talk about the origins of that particular technical criteria. We'll talk about the enhancements and refinements to the spurious operation assessment, which is significantly refined from the previous revision document. And we'll also touch on the restructuring of the BTP, which a lot of the comments so far have come on the restructuring aspects. And we'll kind of give you more details on why we did what we did and some of the streamlining and refinements that took place.

And a number of these changes that we made, updates, I just want to reiterate, a lot of this was either identified internally by the staff as potential improvement areas for the document, but a lot of it was also informed by the feedback we've gotten from industry. So, one of the big parts we want to emphasize is that we had a number of public meetings with industry stakeholders to solicit their feedback on areas for potential improvement in terms

of what are the challenges you're having with implementing this document; what are the challenges you're having just reading the document, extracting information out of it? So, that's one of the big reasons why a lot of these changes took place where we saw these potential areas of improvement, based upon our operating experience with our own licensing reviews in both operating plants and advanced reactors and industry feedback.

Okay, yes, next slide.

So, we want to present these modifications, kind of going through this point. We have actually gotten a lot of ACRS feedback already. So, I'll just go ahead and get straight to -- past this slide.

So, just as a background for it, the BTP 7-19 is the implementable guidance for the Commission's policy on CCF. And we've summarized the four main points on there in terms of performing the D3 assessment to demonstrate vulnerabilities to CCF have been adequately addressed. Really, it's to ensure you have adequate defense-in-depth for your plant and it is maintained when you're modifying a system of varying safety significance, whether it's the A1 or A2 systems or B1 or B2 systems, which we'll

get into in our later slide.

You're analyzing each postulated CCF for its effect on the plant's accident analysis using a relaxed methodology from the initial licensing basis calculations that were used to develop the safety analysis. That provides that flexibility there.

And the next two we'll be getting into a lot in terms of the refinements and improvements we've made in terms of, if the assessment could be shown to disable a safety function, provided diverse means to address that particular failure mode. So, we've had a number of different challenges when it comes to that particular piece in terms of some industry confusion in terms of do you mean all safety systems or do you simply mean safety systems we categorize as A1, which is RPS/ESF systems, or are you including all of the safety subcomponents like safety chillers, and things like that?

So, one of the big things we did with this update is we got some clarifications in terms of the scope of what specifically you need to do for your analysis to demonstrate a safety case, which is one of the reasons why we have the graded approach in the first place. And we also clarified a number of legal aspects within the document, so that it's clear where

this document begins and ends in terms of your requirements in terms of scope and the rule that you're operating under if you're trying to modify the plant, either between 50.59 or 50.90. We'll get into that in another slide.

And, of course, providing diverse displays and controls looking at the control room and the system level. That actually provides a specific design criterion that you need to address specifically. And we provided some refined guidance on that as well.

MEMBER MARCH-LEUBA: For my edification, are those four positions connected by "ands" or by "ors"? Do you have to have all four or one gets you?

MS. ZHANG: So, we believe it's "and," meaning that, if you satisfy each one of those, it doesn't mean that you've satisfied the overall position for D3. And that's why we actually had to clarify and separate some of the acceptance criteria. It was that we saw the acceptance criteria being different, depending on whether you're reading it from point 3, position 3 here or position 4. And so, some of that takes into account the actual language that was in the SRM and providing flexibility where it should be, but also maintaining the Commission's

direction was in the SRM.

MEMBER MARCH-LEUBA: I know it's the Commission direction, but if you describe No. 1, you have done a follow-on detail with the assessment and CCF has been adequately addressed. Why do you need to do the rest?

MR. MORTON: As Deanna was saying, that fourth bullet, that's essentially a "shall". You're providing that bullet, the diverse displays and controls in the main control, and I don't want to say "irregardless of what the previous three bullets are," because when we said "ands," we really mean they need to address, a licensee would need address all of them. It's not a situation where they can provide a D3 assessment; they're clean in terms of potential vulnerabilities to the plant, but that's part of the Commission's direction on addressing CCF, is providing that set of diverse displays and controls.

MEMBER MARCH-LEUBA: Okay.

MR. MORTON: Like I said, this is one of the things that we engaged OGC on a number of different items inside here to say, hey, what does that mean? Is it really an "and" or is it an "or"? Or you have to satisfy all three? So, a number of the changes we made within the update are interpretations

to ensure that it's correct and consistent across the board.

MEMBER MARCH-LEUBA: And your update does not require a rule change? I mean, this is just an interim.

MR. MORTON: I'll get to that. I'll preempt it. In a slide, I'm going to get to it, but we have another SECY, SECY 18-90, which actually the staff determined that there was sufficient flexibility within the Commission's direction and policy that we could make the revisions we're making within the BTP. Okay?

Next slide.

And so, the background, I just mentioned the SECY 18-90 clarifies the application of the Commission direction. Essentially, the most important thing to keep in mind, like I just said, is that we determined that there is adequate flexibility within the Commission direction that we can make the refinements and improvements that we are targeting within this revision, such as having the flexibility to have a graded approach on the safety significance; providing more methods to directly address CCF within the specific design itself outside of the actual NUREG-6303 D3 process. And also, the restructuring

that we've done to clarify and revise a few things within the readability of it. So, those things were all within our purview to do and still address the Commission direction.

Next slide.

So now, we'll get into the summary of changes. We kind of touched on this already. One of the things I do want to highlight on this slide is that third bullet, which is the incorporation of qualitative assessment criteria from Supplement 1 to RIS 2002-22.

There's two things about 50.59 sort of guidance we clarified with the BTP. The first thing we did, and this is one of the significant comments we got from industry, which is, do we or do we not have to implement the BTP Commission direction if we're doing a modification under 10 CFR 50.59? We clarified that, no, you do not. It is not applicable to mods under 50.59. It's one of the clarifications we made within the document.

CHAIRMAN BROWN: Would you say that again?

MR. MORTON: One of the larger industry concerns was whether, if you're performing a digital modification under 10 CFR 50.59, do you have to implement BTP 7-19, a D3 assessment, for those digital

mods? And we clarified you do not. It is not applicable. 50.59 is its own separate thing from the BTP. So, we clarified that within the document.

CHAIRMAN BROWN: If it's a whole new digital RPS replacement, why wouldn't you have to consider the aspects --

MR. MORTON: I'll get right to that.

CHAIRMAN BROWN: I thought you said you didn't have to consider it.

MR. MORTON: I'll get right to that with this bullet, too.

So, the second part we did was the qualitative assessment criteria from the RIS supplement. The RIS supplement, if you're not aware, the RIS supplement provides technical criteria to address software CCF.

CHAIRMAN BROWN: But only for A2-B1-type systems?

MR. MORTON: Correct.

CHAIRMAN BROWN: Not A1?

MR. MORTON: Correct. So, when you cross into LAR space, you're implementing the BTP for A1 systems.

CHAIRMAN BROWN: Change into what space?

MR. MORTON: Well, 50.90 space, for

license amendment space.

CHAIRMAN BROWN: License amendment?

MEMBER BLEY: Remember, Charlie, when we did the other one, they said it doesn't apply?

MR. MOORE: Could anybody on the public line please put your phones on mute?

MEMBER BLEY: You couldn't use 50.59 for a complete replacement.

MR. MORTON: Right.

MEMBER BLEY: That throws you back here.

CHAIRMAN BROWN: No, I understand that. We haven't had our subsequent meetings on 50.59, which is another observation, because of some other statements in the BTP relative to the inconsistency between safety analysis and the whole FSAR. I'll point that out at some point.

MR. MORTON: Okay.

CHAIRMAN BROWN: But it's not useful right now. So, I'm still kind of confused when you're saying -- Dennis didn't help me any. I walk away still being confused about 7-19 doesn't apply if I'm replacing the entire system because 50.59 --

MR. MORTON: It does. It does.

CHAIRMAN BROWN: I thought you said it didn't.

MR. MORTON: No, just not for A1. For B1, A2, and B2 systems.

CHAIRMAN BROWN: That's what --

MS. ZHANG: Let me try to clarify.

CHAIRMAN BROWN: He just said it doesn't apply to A1.

MS. ZHANG: Yes. Let me just try to clarify this a little bit.

So, the reason we incorporated the qualitative assessment here -- we could have just said, well, if you're performing a qualitative assessment, that means that it's not an A1 system. And that means that you're likely to do it under 50.59. So, why put any guidance on qualitative assessment here?

And the reason we decided to do that is, one, this is not just for a plant that's coming in for a digital modification. This also applies to new reactors. So, we want to have consistent criteria applied for new reactors as well as for operating reactors performing a digital mod. That's the first.

The second thing is, for any reason -- let's say there was a tech spec change or something related to an A2 or B1 system, and they had to come in for a LAR. We wanted to make sure that the

qualitative assessment, that there's consistent criteria, whether you're doing it under 50.59 or whether you're submitting a LAR for a number of other reasons that would have triggered the requirement of a LAR.

The thing about the D3 assessment is that we're very specific: this only applies to an A1 system. And our underlying whole premise here is that an A1 system needs a LAR.

MR. MOORE: Charlie, does that clarify it for you?

MEMBER BLEY: I think there was some miscommunication about A1. If you have A1, you've got to come here and you've got to do the 3.1, whatever. It's the detailed analysis.

CHAIRMAN BROWN: Well, you've got to have a license amendment as well.

MR. MORTON: Yes.

CHAIRMAN BROWN: So, that's how you get the 7-19 --

MR. MORTON: Yes.

CHAIRMAN BROWN: -- for the A1 systems.

MEMBER BLEY: I know I've asked this before --

MR. MORTON: Sure.

MEMBER BLEY: -- but I forget the answer. As far as guidance goes and people's use of it, there is no real difference between a Branch Technical Position and a Reg Guide, right?

(Laughter.)

I guess you do both. There is a real difference?

MS. ZHANG: Yes.

MR. MORTON: There is. There is a difference.

MS. ZHANG: And this is why, you know, you see a lot of repetition in there, and there's a reason for that. So, the original intention of a Branch Technical Position, a Branch Technical Position is a subset of the SRP. SRP, staff review guidance, is not intended to be licensing guidance for an applicant.

However, because of some of the previous work that's been done, that line has been blurred for a number of the Branch Technical Positions, Interim Staff Guidance. So, as a result, in this BTP we tried to separate acceptance criteria and review guidance. So that, once we do push forward with the overall SRP modernization, the acceptance criteria and the focus of the review can go into the actual SRP; whereas, the review guidances, we can change the language more

easily and port it over to a Regulatory Guide. So, that's why you see a lot of repetition there. It's intended for future implementations to make it easier to separate those.

MR. MORTON: Yes, because, functionally, the staff understands that the BTPs, especially this one, in particular, BTP 7-19, has been effectively used like a Reg Guide. It is technically staff guidance, but it is the principal guidance that exists in the regulatory infrastructure to address CCF. Industry has used it as such, and we understand that.

MEMBER BLEY: But what Deanna just said, although these have been around for long, long periods of time, the real intent is eventually this goes into Reg Guides and SRPs?

MR. BENNER: Absolutely.

MR. MORTON: Yes.

MR. BENNER: We actually just had a public meeting yesterday -- this is Eric Benner again -- where we talked about the longer-term activities for digital I&C. And the core of that is we've been doing a lot of stuff with our heads down for the last however many years, more focused in the last four years. And once we sort of get these pieces in place, there is an acknowledgment -- now we haven't blessed

this recommendation, but, basically, there is a bigger recommendation to say we need to step back, look at the right, for lack of a better word, architecture for the regulatory guidance and make sure we port all of the things we've done over the last couple of years to SRPs, the staff guidance, the right set of Reg Guides for applicants and licensees, have coherence and consistency between all those documents.

So, it's an acknowledgment that we've done a lot of these interim steps or patches, or however you want to call it, but the end state needs to be a much clearer, overall picture as to what an applicant or a licensee should submit and how the staff will review that information.

MS. ZHANG: So, one thing that I want to clarify on this slide is, we talk about, and we're going to go into more detail about, means to address CCF. We really took it from a hazard identification and control perspective when it comes to CCF. And that's why, when you look at the structure of the D3 assessment and the steps, it goes to, can you eliminate the hazard? If you can't eliminate it from consideration, can you mitigate it? And if you can't mitigate it, can you cope with it; can you accept the consequences? And that's why it's structured the way

it is.

We want to make that clear. And if you read the flow diagram, that's how it drives, yes, right? If you can eliminate it, you don't have to do anything else. If you can mitigate it, you don't have to do a full consequence analysis. Otherwise, you then do the consequence analysis.

But we do recognize that maybe there are portions of the system you can do the elimination from further consideration of the hazard. There are other portions that you can do mitigation. This is what we've seen in a number of the previous reviews, is that it's not a one or the other. So, because of that, if you see a lot of repetition comes with the acceptance criteria, it's because we recognize that, for different pieces of the system, you may choose to do one set of strategies for one and a different strategy for another portion of the system.

MEMBER BLEY: Since you mentioned the flow diagram, the impression I got, reading through the document, is you had done that at some point in the past and you didn't really update it to exactly match the new words that are in the text. Take a look at it and see if you agree.

MR. MORTON: Okay. Thank you for that

input.

CHAIRMAN BROWN: And before you go on, I just went back, and I presume you're referring to figure 2.1?

MEMBER BLEY: Yes, I was.

CHAIRMAN BROWN: Yes. And you've made a very cogent, clear, crisp set of statements. You said what were the three things you do, A, then B, and then C. I've just gone back and looked at this, and there is no lead-in for this assessment that says the approach to mitigate, you know, to dealing with the CCF is, first, to evaluate what was your first thing. There were three things you said once you determine it. Can you repeat that?

MS. ZHANG: Eliminate, mitigate --

CHAIRMAN BROWN: Mitigate.

MS. ZHANG: -- or cope with the consequences.

CHAIRMAN BROWN: I guess my point being, I started getting lost trying to figure out what was that flow that you were trying to -- it's not in the diagram. It does not say that. But in the beginning of Item B3, it should have, "We've structured this to do the following" -- bang, bang, bang. And then, your subsequent writeups should follow that flow, which

they don't.

MEMBER BLEY: Yes, that was my point.

CHAIRMAN BROWN: Okay?

MR. MORTON: Okay.

CHAIRMAN BROWN: And you can't find that relative -- I mean, first, the words and the diagram, and then, where is that flow in the acceptance criteria? It's not. That's where I got lost in terms of there was all these -- bang, bang. That's where I struggled, and it sounds like Dennis had some issues or concerns --

MS. ZHANG: I got it.

CHAIRMAN BROWN: -- about that also.

MS. ZHANG: Yes, we definitely understand that, and we'll try to explain the figure more and tie it --

CHAIRMAN BROWN: Stop. Please, not the figure; the lead-in.

MS. ZHANG: Yes, the lead-in to the figure that explains the figures, right?

CHAIRMAN BROWN: Don't take me wrong. I'm not beating on you, okay? Just the focus here was, right in the beginning of your paragraph, say this is structure to do the same, the following things. If you have CCF, here's what -- bang, bang, bang -- you

do.

MS. ZHANG: Yes, we tried to do that in terms of the actual guidance themselves. And if you look at, on page 7-9-15, it does try to -- so, the A, B, and C in there, there are kickout clauses at the very end of each of those sections. So, in A it says, "In this case" -- which "in this case" means you've eliminated the CCF from further consideration -- "then, Items B and C below" of this subsection would not apply to the A1 system. So, that is our way of trying to -- maybe it's not that clear and we'll try to enhance that.

CHAIRMAN BROWN: Okay. I'm 78 years old. Okay? And my brain fries at about line 3; whereas, you said it in about a dozen words as an A, B, and a C, which only had three or four words in each item. And then, you can translate that into here's --

MEMBER BLEY: It wouldn't have fried your brain if her words were at --

CHAIRMAN BROWN: Exactly. I mean, I was looking for where is that framework that you're trying to establish. And now that you say that, I understand what you're saying. But, even when I go back here and read it, it doesn't leap out at me that I'm in this stage or that stage or the following stage.

MR. BENNER: And that's the beauty of a fresh set of eyes looking at it, because the people who have been working on it are so immersed that that structure is inherently obvious to them. You're right that, both for members of the public and the reviewers who will pick this up later on, that needs to be obvious to them. So, we certainly accept the feedback that, if that is the plan and it's an acceptable plan, it needs to be obvious to the reader of the document that that is the pathway by which you get to --

CHAIRMAN BROWN: It's kind of the architecture for addressing the assessment.

MR. BENNER: Yes.

CHAIRMAN BROWN: Love that word.

MEMBER BLEY: But I would go back to my opening comments. I know for 12-13 years this process has been going on. We've followed it. And I know a lot of people from industry have participated with you. I don't know how far throughout the industry the participation has extended. I think everybody who has been involved for the last many years, the words work just fine. They know what they're doing. But if you go out to a new plant that hasn't really been closely involved and new engineers trying to use this, I think it would be worth doing that experiment and seeing

what you get back from them.

MR. MOORE: Mr. Chairman? Mr. Chairman, I apologize for this, but we were dropped off the public line. So, we need to call back in and it has to be done from here. So, Paula is going to call us back in. Just hold the presentation for just a second.

(Pause to reconnect to the public phone line.)

CHAIRMAN BROWN: Are we okay now?

MR. MOORE: Yes. Thank you, Chairman. Yes, you can go ahead.

CHAIRMAN BROWN: I just wanted to follow up. This is just another thought. I've just been mulling this over for quite a few days.

If you start with the overall architecture of the system, whatever it is, and you work through the eliminate, mitigate, cope with it, all three of those, then you start looking at how do you do those. And the last item on the list in many circumstances, manual operations, crediting manual operations. But when you get right down to a lot of these systems, the simplest coping, or even if you can't, regardless of whether you can do the other ones, is manual operation. It doesn't cost you anything. It's a

procedural item. A guy has to be trained to respond if he sees certain things. Yet, that is pushed downwards in terms of what you evaluate.

And to me, we ought to be looking at the easiest ways to do these and manually coping/crediting is really a function of what is the specific critical nature. What if you can't eliminate, mitigate, and you can't cope, how important is it?

In other words, I know in my old program -- I'll just use an example -- probably one of the most difficult problems to deal with was you can't pull rods very fast in these plants. Navy plants are different. They're operating all the time and they need to be -- and for various reasons, they have high rod speeds and they're continuous, not graduative. That accident scenario of all rods going out rapidly is a critical one and has to be responded to very fast. You can't manually respond in the 100 milliseconds or so that you see that occur generally, depending on the plant.

But there are a ton of other scenarios or events -- for instance, those which are tripped by temperature. Temperature cannot change very fast. So, you've got minutes to respond to critical events which result in overtemperatures, temperatures going

where you don't want them to go. Pressure drops fast, but the consequence of pressure dropping fast is also a deferred -- it's not real fast; it just sets up conditions, but you can still manually respond to those if it's set up properly.

It just seems to me that the whole idea of incorporating complexity into the designs -- one of the designs we reviewed years ago had a complete set of analog backup systems which -- I didn't say anything at the time -- seemed to be overkill in terms of what was going on, but that was the perception of what they thought they needed.

That has not necessarily been the case in some of the later -- you correct me if I'm wrong. I don't think it's been quite as extensive as that. You probably know what I'm talking about.

And I don't see any of that thought process of what do you do about the potential common-cause thing, if you're going to believe in them, that drive you towards simpler solutions. It's very open.

MR. BENNER: That's excellent feedback, Member Brown, because I think in the discussions with the staff there really has been no preference for which path an applicant to chose to address CCF. But I can see in how the sequencing and the construct of

the flowchart could lead one to believe that they have to go through it in the order in which you indicated, and I don't think that was our intention. So, we can also look back to make sure we're not driving licensees or applicants to sort of a perception that there is a preferential solution, because there isn't. I think that's an important thing for us to consider in how we structure the document moving forward.

MS. ZHANG: Member Brown, just to add to what Eric said, I think one of the things that we wanted to recognize is that this analysis, this D3 assessment, needs to be done on an event-by-event basis, right? So, if you look at the SRM, it says, for each event analyzed in the safety analysis section of the Safety Analysis Report, you should do the assessment.

In this case, if an event is a quick-acting event that you can't expect an operator to mitigate with reasonable margins, then that should probably be done by an automatic system. In other cases, if this event is a slow-acting event, then, of course, manual operator actions would make more sense.

And this is where we've seen in previous reviews why there are portions of the system that took credit for different diverse means. It's because, for

a particular function that is performed by one portion of the system, they didn't need the automatic diverse actuation; whereas, other parts, they might because of the nature of the event and the response time requirements.

MR. MORTON: Let me clean up on this one point, Member Brown, before you respond.

CHAIRMAN BROWN: You're going to let me forget? Go ahead. Please, no, no, go ahead.

(Laughter.)

MR. MORTON: Sorry. So, just to kind of touch on also what Deanna is saying and what Eric was saying, part of the process when updating the provision, we didn't want to presume with a specific design solution a licensee may use.

CHAIRMAN BROWN: Oh, I understand that. I understand.

MR. MORTON: We want to provide flexibility in the various options that a licensee can use to address these issues. In some reviews, we've seen licensees credit preexisting manual controls that are already in the plant. In other ones, they install a new one. It depends on the plant, the plant's individual design and design basis for how they can address software CCF. So, I just wanted to kind of

reiterate that point.

CHAIRMAN BROWN: I understand that. You don't want to tell them; you want to give them the flexibility to do stuff.

MR. MORTON: Yes, right.

CHAIRMAN BROWN: But you also don't want your writeup to drive them where they don't need to go because you haven't said that. Like you made the comment that the SRM says event-by-event. Does it say that in here?

MS. ZHANG: I think we tried.

CHAIRMAN BROWN: Until you just said that, I didn't realize that. And I read this, believe me, I read this in detail.

MS. ZHANG: So, that's definitely a great comment, Member Brown. We'll take that and we'll make sure that we are clear in terms of that, you know, that it is event-by-event and that the solutions may be different for each event.

CHAIRMAN BROWN: Okay. The point of my comments is to not drive these systems so they're so complex and costly that we don't get them done. Because this whole commercial world has been, it's just a disaster that they have not converted, in fact, some of these systems, the protection systems, to the

digital-style system. They're so much more reliable and easy to maintain.

So, okay, go ahead.

MR. MORTON: So, before we get off this slide, I want to kind of reiterate something we touched on, which is restructuring the document, because we got a lot of feedback in terms of how the document has been reformatted to address some of the feedback we've gotten.

And touching on that, along with the figure 2-1, I think 2-2, one of the reasons we tried to put together a process flow is because one didn't exist previously. It's really that simple. So, when we've seen various licensees, either in advanced reactors or operating reactors, try to use the document, the flow and structure of these evaluations are always different. Some people catch some things. Some people don't do other things. There wasn't a lot of consistency in there.

And even within the staff reviews, because this is a Branch Technical Position, we saw that there needed to be some improvement in terms of following a specific structure. So, we do take that comment strongly that maybe the wording that we have in there didn't match the process that we actually envisioned

with the figure that we put together. The figure really does sort of encapsulate how we envisioned a licensee going through the process of addressing D3.

And part of that is, with the testing aspect providing other means to eliminate CCF outside the D3, that was an effort to simplify the overall analysis. Can you eliminate certain portions from the system from the D3 to constrain the analysis to only be where it's actually needed, and not include every ancillary portion of the system, if it's possible to do that?

MEMBER BLEY: For me, it helped a lot. It would be even more helpful if it matched the language better.

MR. MORTON: Yes.

MEMBER BLEY: And I think it would allow you to simplify the language.

MR. MORTON: Yes. So, thank you for that comment.

So, I think we can go on to the next slide, and I will turn it over to Deanna.

MS. ZHANG: Thank you, Wendell.

So, in the next few slides, we're going to go over the details of the categorization scheme and the graded approach that we're proposing in this

revision to BTP 7-19. And this is something new to this revision. So, it wasn't in previous revisions.

And the reason that it wasn't included, one, it was to really incorporate the guiding principles that were outlined in SECY 18-0090 by providing a graded approach based on safety significance. But, also, it's to recognize that, yes, you don't want to put a lot of effort for a system that doesn't contribute significantly to safety. You want to get the best bang for your buck, right? So, for those systems that definitely contribute to safety, like your protection systems, we do want you to perform the D3 assessment, the full scope of it.

CHAIRMAN BROWN: Keep talking. I'll let you finish for once.

MS. ZHANG: Okay. So, if you see on this slide, we've broken it up into four categories:

A1, which is the safety-related system with high safety significance, a significant contributor to plant safety. So, for example, this would be your reactor trip systems, your ESF systems, generally your protection systems.

You also have your A2 systems, which are those that are safety-related, but may not be a significant contributor to plant safety. So, this

could be your safety chiller systems; yes, HVAC support systems.

And then, you also have your systems that are not safety-related, but may contribute to safety, like rod control systems. Or you could have a system that's not safety-related and doesn't contribute to plant safety.

So, in this case, I do believe this aligns very well with what we've seen in the NuScale reviews with the categorization, but different from that is that we actually provide criteria for how you should address it based on that categorization, which didn't necessarily exist for the NuScale DSRS.

MR. MORTON: If I may jump in, I want to address Member Bley's comment; I think Member Brown's comment, too. So, there was an early comment on the categories that we have, A1, B1, A2, B2, and the appearance of mixing together A2 and B1 systems in terms of the technical criteria. So, I want to step back and give you some of the thinking the staff had in terms of the graded approach.

Originally, when we were looking at the scope of the Commission's direction, what it applied to, we clarified that really the Commission's direction applied to A1 systems, those protection

systems; RPS, ESF, ESFAS systems specifically. And we keep those apart specifically to perform the D3 assessment.

We also consider for completeness, well, there may be other systems that may come in for a license amendment to be modified for some reason. It could be an A2 system which would generally be a subsystem, like safety chillers, to a larger protection system potentially. Or a B1 system, for some reason, you've got to bring a feedwater mod in the license amendment, a rod control mod for the license amendment, et cetera, et cetera. And even a B2 system, like service water, or something to that extent.

So, we thought, there's nothing in the current Rev. that addresses those particular systems that may come in for a license amendment. What do we do? What sort of technical criteria would we apply to make a safety case for those type of systems? So, it's clearly the Commission's direction does not apply to anything outside of the A1 category. What would we apply?

And as Deanna stated earlier, we determined the qualitative assessment criteria will be useful means to address potential issues and hazards

with those systems if they happen to come in for a license amendment.

So, the reason why we're not necessarily mixing B1 and A2 systems, they just have a similar technical criteria to address the hazards with those systems.

MEMBER BLEY: You're treating them the same though?

MR. MORTON: Yes.

MS. ZHANG: And, Member Bley, I would like to say that, while the qualitative assessment may be -- we say it applies to A2 and B1. The way you apply it and the necessary measures you would have to implement to show that the CCF has or hasn't been properly addressed may be different, depending on the particular system.

MR. MORTON: Correct.

MS. ZHANG: So, we don't want to say, oh, qualitative assessments, it's equal for an A2 or B1 system. I would say that it is highly dependent on the particular system and the actual design.

MR. BENNER: And I'll just add -- this is Benner -- that I think part of the rationales which we could make clear is, for an A2 system, right, we still expect the qualitative assessment to be adequate in

any case. So, for an A2 system, we see that as okay because it's still adequate, it's required by regulations, and it's lower safety significance. For B2, it's higher safety-significance, but, remember, pretty much for anything that happens -- or B1 space -- anything that happens in B1 space, somewhere there's an A1 system that's backing you up to mitigate it.

MEMBER MARCH-LEUBA: And that was the point I wanted to make. What confuses me when I look at this is the fact that you categorized it as safety-related and non-safety-related and safety-significant. Maybe in the text, maybe you can modify the table. You should describe B1 the way you did it, which means --

MR. MOORE: Member March-Leuba, the microphone, please.

MEMBER MARCH-LEUBA: You're going to hear me -- boom. Let me stand up. I mean, that boombox doesn't work with this thing.

B1 equipment is a piece of equipment whose failure will initiate an event, but it's not relied upon to terminate it. Right? I mean, if you could just put it in there somehow, then nobody would complain about it anymore.

MR. MORTON: Right.

MEMBER MARCH-LEUBA: Well, we would complain about it, but not rightfully.

MR. MORTON: Right. To your point, the B1 system would likely have a malfunction that is analyzed in the Safety Analysis, your rod control --

MEMBER MARCH-LEUBA: But it's not relied --

MR. MORTON: But it's not relied upon to --

MEMBER MARCH-LEUBA: It's not relied upon to fix it.

MR. MORTON: Correct.

CHAIRMAN BROWN: Thank you very much. I didn't realize that.

MEMBER BLEY: Well, that's true. But my argument was on the logic.

CHAIRMAN BROWN: Yes.

MEMBER BLEY: Now you can't find a system described by those words that will be as high safety significance as those in A1, as described by their words. So, I think the words are useful. If, in fact, you found a system like that, that somehow through interactions in the plant, if it was really safety-significant and was contributing to the risk,

you ought to treat it very thoroughly. But the way the words are added, it's probably not going to get in that condition.

CHAIRMAN BROWN: And just to echo Jose's comment about it, I just never realized that B1 really was more of an initiator, probably primarily, but not necessarily always, but at least primarily. But what constitutes an A1, a B1, an A2, or a B2 does not come out of the discussion.

I have no problem with the graded approach. I mean, it's a fine approach for doing business. It tries to get you out of the weeds where you don't need to be in the weeds. But what does it mean to be in any one of those particular boxes, I totally had no clue.

MS. ZHANG: So, Member Brown, thank you for that feedback.

CHAIRMAN BROWN: Yes, thank Jose.

MS. ZHANG: And Jose, Member Jose.

We will try to go through a little bit about the definitions and how we approached defining what an A1 system, B1-A2 systems are, in the next couple of slides. Okay?

CHAIRMAN BROWN: Okay. They ought to be in here, too.

MS. ZHANG: We'll try to make sure they are.

CHAIRMAN BROWN: It ought to be clear.

Can I ask, before you do that --

MS. ZHANG: Yes.

CHAIRMAN BROWN: This is a technical question. It has nothing to do with the BTP. I should have asked it in the beginning.

You read all the SECYs and the SRMs. It's common-cause failure. Software brings this whole new mystique of problems with it that you have to deal with that is not dealt with in the analog world. I have a little bit of problem with that definition, but that's beside the point. In the analog world, you have common-cause failures also. I have not reviewed or seen any of the analog-style systems in current plants.

What did I do wrong? Oh, for those folks that are on the phones, would you please mute your phone? We're getting feedback into our meeting. Thank you.

Where was I? Oh, yes. In today's world, if I go out and look at a commercial plant, do they have diverse systems to compensate for analog-style common-cause failures in the mode that we have them in

the computer-based? Is that a yes or a no?

MS. ZHANG: I would say that for some aspects of it, there are. For example, your ATWS, right, that wasn't created to address a digital common-cause failure. It was treated because, there wasn't --

CHAIRMAN BROWN: Everything fails.

MS. ZHANG: Yes, everything fails. You need something, right?

So, I would say that common-cause failures have been addressed in different ways.

CHAIRMAN BROWN: Take ATWS out of this. I understand what you're talking about with ATWS.

MS. ZHANG: Yes.

CHAIRMAN BROWN: I was at NR when ATWS first was born, and there was tons of discussions on that because they didn't exist initially. It was an add-in.

I'm just looking at today's analog reactor protection systems, trips and ESFAS. Do they have the same scrutiny and do they have diverse systems to somehow compensate for common-cause failures in any particular set of channeled divisions of the two primary protection systems?

MR. MORTON: Let me see if I can --

CHAIRMAN BROWN: It's not a yes or a no?

MR. MORTON: I was going to say, yes, insofar as most plants are either actually 279 plants or 603 plants; would have separate, independent manual controls to punch out the plant if you have a failure in those protection channels.

CHAIRMAN BROWN: I got the -- manual is manual, okay?

MR. MORTON: But they would be diverse from each other from that standpoint.

CHAIRMAN BROWN: But you've got that in the computer-based world also. Okay?

MR. MORTON: Uh-hum.

CHAIRMAN BROWN: So, the real answer is no, other than manual operation. I was just curious because I'm totally unfamiliar with the commercial plant protection systems. And are we applying a higher standard now because of a perceived issue of, quote, "software failures," which software doesn't fail? It's a design failure, fundamentally, in your program. You programmed a function incorrectly, and it could be in all the divisions. That you have to know how to deal with somehow. Okay? So, that's why I asked the question relative to the analog.

You can go ahead and finish your going

through -- I diverted the discussion there for a minute, and I didn't want you to lose your cogent thoughts, unless you wanted to hammer me a little bit.

MS. ZHANG: Member Brown, I just wanted to add onto what you said. So, yes, we do not provide the same level of scrutiny to analog systems having CCFs. But part of the reason -- and if you look at it, right? -- requirements-wise, you have the GDCs. You still have GDC 22, which does say you should have functional diversity.

However, to the level for a digital system, why we wanted to go a little bit further is because of the capabilities of digital systems in terms of system integration and the functionality and the complexity of it, or the potential complexity of it, where it makes it harder to analyze and to determine whether there are any latent systematic faults within that system.

CHAIRMAN BROWN: Yes, but within that concept, I fully understand that because I can say, in 1978-79, when we first tried to apply this to the naval nuclear plants -- and the only processor available was a Z80, 2.3 megahertz, high-powered, node memory -- we went out with a set of specs. And the vendors that we went to bid said, oh -- and we were

going to put a microprocessor in every one of 29 instruments, because we didn't even know how to make stuff work, period. And they said, no problem, we only need four processors; we will have an executive that oversees everything which distributes all the data. And that was all four divisions.

MEMBER BLEY: And right there you hit the difference.

CHAIRMAN BROWN: That's right.

MEMBER BLEY: We started trying to integrate, integrate and tie things together that weren't tied together in the analogs.

CHAIRMAN BROWN: Exactly. And we said no.

MEMBER BLEY: So, we can still have common-cause failures in an analog world, but it takes out a much smaller subset.

CHAIRMAN BROWN: Exactly. However, if you meet the design of the five principles -- independence, deterministic, straight through, redundancy, control of access -- you put yourself back into where you have -- that's what we did. We ended up with four separate divisions, all independent. You could put a steel plate between them and nothing communicated between them. And that's what we've been trying to drive to, and all the applicants, in the new

designs that have come forward. So, we've kind of gotten ourselves -- and by the way, the combining RTS and ESFAS, that was also deleted from R7 and to R8.

MEMBER BLEY: But you kind of tripped into something here that I had in my head until I just spoke with Jose. When it comes back, I'll tell you.

(Laughter.)

CHAIRMAN BROWN: I thought I was the only one did that.

MS. ZHANG: So, let me finish with the definitions, Member Brown and all ACRS Members.

CHAIRMAN BROWN: Yes, thank you.

MS. ZHANG: And then, we can go into a lot, some parts of how we've accounted for integration in this BTP.

Okay. So, in terms of the definitions, I'm not going to read every part of this definition, but I want to give you some of the background as far as how did we derive these definitions. Where did they come from?

So, actually, originally, we had looked at a lot of our 10 CFR Part 50.2 definitions for a safety-related SSC. And then, we went through trying to find a definition for, you know, those systems that are not safety-related, but may be important to

safety. Of course, many of you guys know there's not a specific definition for those types of systems.

So, we, then, tried to expand and look internationally at the various --

MEMBER BLEY: You kind of blushed past 50.69, which uses the same language.

MS. ZHANG: Yes, I will get to 50.69 in two slides after that.

So, in terms of looking at the international standards, so we looked at IEC 61226, which is the IEC for nuclear power systems. How would you categorize the various functions performed by systems? And you would perform the categorization based on the definition, and then, you would allocate those functions to the corresponding systems.

So, taking that, and then, taking our definition for a safety-related SSC, is how we derived these definitions. Now they may not be perfect. This is a start. We definitely welcome additional feedback on these definitions, as well as we haven't gone to public comments. And we feel that, if there are improvements to be made by members of the public, we feel that we would definitely welcome that.

MR. HECHT: Deanna, have you considered adding examples to these definitions, because it's not

totally clear? For example, what does an auxiliary or indirect function mean? Just as an example, is aux feedwater an auxiliary function and what makes it different from primary feedwater?

MS. ZHANG: So, one of the things you have to consider is, in reading this, we were trying to look at actuation functions versus maintaining plant at a safe shutdown state. So, if you look at A1, those are really your actuation functions, your initiation logics and everything. So, aux feed initiation would be considered an A1 function, right? And if a system is performing that particular function, we would consider that an A1 safety-related system.

Now, for aux feed control of the level and amount, that we would consider an A2 system. That would be one example, because it's after you've had your initiation, how do you maintain the level was in the prescribed limits?

MR. MORTON: Also, if I could lead off in terms of Deanna's point, a lot of this depends on how the individual licensee defines their systems. So, one of the challenges we had when we were looking at the definitions, especially when you're getting into the controls for A1 systems, like IPSI, filler

controls, or load sequencing logic, what would that constitute? Would it be an A1 system or an A2 system, and how would you treat that? A lot of this depends on the individual licensees' description within their licensing basis of these particular systems or subsystems. So, that's one of the considerations.

MR. HECHT: So, you're not putting in -- I'm sorry -- so, you're not putting in examples because you feel that they would be misinterpreted?

MS. ZHANG: That is part of it. Also, we want to recognize that it is different for various licensees and designs. And because of that, we didn't want to -- we gave a few examples in the beginning when we introduced the categories. So, like HVAC systems, safety chillers, we did identify those as an A2 system, and your protection system, your ESF logic, that as an A1 system. But when you got down to every possible system and how you would categorize each of those particular systems, I think the variations in the licensing basis, I think that prevents us from making that, providing that entire list.

MR. MORTON: To get to that level of refined and in terms of considering each and every way a licensee may have categorized their system is challenging. So, leaving it a little more open-ended

provided more flexibility. If a licensee determined that, for example, their safety chillers were A2 or an A1 -- so, it depends on what they would choose to consider it as.

MS. ZHANG: And part of it is how they've selected the -- what's the basis for categorizing particular systems? So, it has to be documented and provided as part of the license amendment request or as part of any new applications. So, that part we tried to emphasize was in the actual BTP. It's a basis for it, for categorization.

MR. HECHT: Yes, well, I guess that's a problem here. That basis, when you use the words like "auxiliary" or "indirect," there's some ambiguity there. And it should be, I think, in light of your comments were very -- your oral comments were very informative, and this is the second time it happened. It happened earlier, too, when you were trying to go through the three decision points, basically, about mitigate, eliminate, or cope. And I'm just wondering if that wouldn't be helpful here perhaps in the supplement as opposed to the primary text, where you say this is informative rather than normative. But you might want to consider that.

MEMBER MARCH-LEUBA: In that light,

following up, let me give you an example. ECCS, I grant you that ECCS is used to maintain the plant in a safe state after you scram. Therefore, it would be an A2. And clearly, it's not. It's an A1.

So, I think on the definition of A1 you need to include those systems that are used to put the plant into a safe state. Because with the language you are showing me there, ECCS falls into A2, you know, and then, it's a 50.59, and you never say it. So, we need to be more -- I mean, you need to have some lawyers that would write this for you, how to think about their lawyers, how their lawyers will interpret it.

MS. ZHANG: Yes, like I said before, these definitions definitely could use additional refinement, and we definitely welcome the feedback we have received today. And providing more examples may be helpful maybe as part of an annex to this BTP.

In addition, I just want to state that --

(Noise on phone line.)

MEMBER MARCH-LEUBA: That is your feedback.

MS. ZHANG: No, there's no feedback here.

MR. MOORE: Again, could members of the public please mute your phones?

MS. ZHANG: So, one of the things that I wanted to recognize is, because we derived some of this language from the IEC 61226, and if you look at it, architecturally, the difference between a European plant versus a U.S. plant, right, they are more about maintaining levels of defense-in-depth a lot more than we are in terms of the categorization and, then, the independence between various categories, not only from a safety-related to a system that's not safety-related, but different gradations of safety, such as when you have a system that's performing a category A function versus a system performing a category B function, versus a system performing a category C function.

That level of defense-in-depth I think we were trying to capture was in this BTP. Maybe we didn't articulate it as well, but that was some of the thinking when we put these words in.

MEMBER BLEY: I would offer one suggestion to the kind of things Jose brings up. If we had quantitative assessment of everything, you could just go with what's in the language in 50.69. We don't, but we do on many things. So, if you had a first bullet that says, it's a system whose "degradation or loss could result in significant adverse effects on

defense-in-depth, safety margin, or risk" -- and that's right out of 50.69. That's what a safety-significant function is. That kind of covers it.

ECCS pops up, even if we don't do a detailed analysis, because we can't, of the software digital control system, the equipment that's driven by ECCS pops to the top in every analysis that's done. So, you've got to have your safety equipment start. So, if you had words like that, that kind of covers it.

And I know you've gone with qualitative descriptions for most of them because that's all we can really do with the digital I&C system right now.

MS. ZHANG: So, going forward, I won't go into this much because we've already talked about a lot of this.

But the next slide goes directly into, Member Bley, your comment about use of risk insights to support the categorization. And we definitely included language within this BTP to recognize that risk insights can be used for that integrated determination process. But we want it to be focused on what the risk insights mean in terms of safety consequences for a plant-specific PRA rather than the probability of a failure of a system, which for a

digital I&C system would be very difficult to model. So, that's why we were very cautious in our chosen words for use of risk information.

CHAIRMAN BROWN: But, to your point, I want to amplify one thing Dennis said before I do this back on the A1-A2, when he suggested the 50.69, but I don't remember what those are, but okay, and he stated them.

The words you have about initiate and complete, you don't want to lose those, but you want to get the thought of the words you use into that as another bullet, or whatever. But you still need to have a little bit of that plain English along with the higher-level thought process.

Now, for here, when you talk about your eliminate, mitigate, cope with, as soon as you make a differentiation between first, second, or third of those, in a way you are applying risk insights in terms of what approach you're going to have. Whether you do it qualitatively or whether you have some quantitative approach, there's a built-in risk insight that's already in this entire defense-in-depth and diversity approach to doing business.

I didn't really think about it in that way until we got into this discussion. So, I mean, in

fact, if somebody says, well, you ought to incorporate it, I think you have. It's not explicitly stated, although you do talk about risk within the BTP.

Dennis?

MEMBER BLEY: Well, they did. After the definition, they have a little short paragraph --

CHAIRMAN BROWN: Yes.

MEMBER BLEY: -- that says, oh, yeah, you can think about risk, too.

But A1 is the things the digital systems drive put them up in the A1 category. And so, I think including that as a bullet in A1 would get you out of the woods of things people are worrying about.

Since we're right at that point in your report, right after that, and when you jump to the application should address the following criteria, and then, you're sending people to Section B3 and B4, and all over the place, I think right at that point if you called out your figures 2-1 and 2-2, gave a brief explanation of them, I think then they should read on. Because I'm marking this up as I go, "What the hell is D3? What's that about?"

(Laughter.)

And you would see how it all hangs together, and then, the rest of it might flow better.

Just a thought.

OPERATOR: Excuse me. This is the operator. I've pulled your line out of conference here. Some of your participants are having a hard time hearing you.

MEMBER BLEY: The operator interrupted; people on the line are having trouble hearing us. Our audio system is not in good shape.

OPERATOR: Oh, okay, I'll just let them know that then. Or you may want to just let them know because they're wondering what's going on. So, all right. Thank you.

CHAIRMAN BROWN: For those folks on the line, we'll just let you know that we've had a snafu, a problem with our audio system the last couple of days, and we apologize for the difficulty that you may have in hearing. We're trying to do our best in making ourselves clear, so that you can hear and understand what we're talking about. We're trying to get that corrected as fast as we can, but it's not going to happen today. So, thank you very much.

MEMBER BLEY: For the members around the table, the big box and the thing with the two little blue lights on there are the microphones for the telephone system. So, if you can project that way --

the speakers are trying to do that, but they can't quite do it well enough.

MEMBER MARCH-LEUBA: Let's just ignore it and keep going.

(Laughter.)

CHAIRMAN BROWN: All right, go ahead, Deanna. Thank you.

MS. ZHANG: Okay. So, let's go on to the next slide.

CHAIRMAN BROWN: We'll get here. Go ahead.

MEMBER KIRCHNER: One minor point. Could you go back to the slide for B1? I think you could simplify the second bullet definition. Just end at "safety". It's already a DI&C and that kind of puts a constraint on the system. You would worry about it if it were two systems.

CHAIRMAN BROWN: Or one system.

MEMBER KIRCHNER: Or one system. Either example could be prone to CCF. So, I think that's just overdefined. Thank you.

MS. ZHANG: Thank you.

So, in terms of the D3 assessment, we tried to clarify the guidance for D3 assessment. Obviously, based on member feedback, we recognized it

could be done a little bit better. So, in terms of the applicability of the D3 assessment, we stated that it should be performed for A1 systems. However, we wanted to make sure that, if we have integrated systems such as if you have the level of integration that we've seen in large light water reactors and the new reactors, that you wouldn't be looking at the A1 system from just a protection system perspective when you have that systems integration and the extensiveness of that system integration not only from a logic perspective, but also from plant operators and the controls and displays perspective. We wanted to make sure that system integration and interconnectivity is taken into account when you categorize a system and when you address the applicability of the D3 assessment to those systems.

So, if you have significant integration and interconnectivity, and you can show the level of independence required to show that the A1 portion of the system will not affect the A1 system, then you should consider all of it an A1 system and perform the D3 assessment accordingly.

So, then, the next part of it is going to what we had talked about, which is how do we address the CCF hazard. So, you could address the CCF

vulnerability by eliminating it from further consideration through the use of the design attributes, testing, or defensive measures. And I'll go into those in more detail in later slides.

And if you can't eliminate it from further consideration, then do you have acceptable diverse means to mitigate the consequences of the CCF and the design basis event that you're evaluating to?

And then, lastly, if that can't be done, if you can't mitigate it, then can you live with the consequences? Again, this is where we've seen, for different functions, licensees and new reactor applicants have taken different solutions. So, for maybe a large break LOCA, they would have had a diverse function performed by a diverse system versus like a feedwater trip they would have maybe taken credit for manual operator actions.

So, we were trying to take that into account when we structured the D3 assessment and the acceptance criteria for the assessment.

MR. MORTON: And just to emphasize what Deanna was saying, this is where staff was challenged in terms of striking a good balance between the technical considerations that we've seen in advanced reactor designs, where you have fully integrated

protection systems. So, you're talking A1 systems integrated with A2 systems, and even a little bit of B1 integration, too.

CHAIRMAN BROWN: What do you mean by "integrated"?

MR. MORTON: There's direct interconnectivity, digital interconnectivity, bidirectional communications.

CHAIRMAN BROWN: But we have that anyway, I mean, even under the designs we've -- are you talking about ones we've even reviewed now?

MR. MORTON: Yes, yes.

CHAIRMAN BROWN: Well, but you look at the RPS, it's one way. There's nothing feeding back. I mean, you go back and look at any of the ones we've looked at, the reactor trip system and the safeguards, the ESFAS systems, all the communications out to these other data networks have been via hardware-based, one-way communications. So, I don't call that integrated. You've isolated it.

MS. ZHANG: Well, it depends, right?

CHAIRMAN BROWN: So, I'm a little bit confused because we don't allow any interdivisional communication at all, except to go to the voting unit. And there, we've compensated to ensure that the voting

unit, you can't have one thing threaten. You look them all up via watchdog timers. You've mitigated the consequences.

MEMBER BLEY: You've done the first step in their analysis, right?

CHAIRMAN BROWN: Exactly.

MEMBER BLEY: See if I'm saying what you're saying. I think you're saying the same things. They're saying you've got to look if it's all mixed together. If you can show that they are separated, then you're not vulnerable and you pass at the top step in their diagram.

CHAIRMAN BROWN: Unfortunately, we had to work hard on that 10 years ago.

MS. ZHANG: Yes.

MR. MORTON: And we took that input.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Not just 10 years ago. But now Deanna is a believer.

MS. ZHANG: But, in addition to that, we also want to recognize, for an A2 system, like for new reactors, safety chiller controls may be integrated as part of a protection system, a function within the overall larger protection system. It might be a separate processor was in the protection system. The

same thing with safety control functions, like your aux feed control, that might be integrated within -- you know, it might be downstream of your initiation logic, but it still was in the same system. And that's not isolated.

So, if you look at the APR1400, you have the initiation logic, but, then, once you get down to the actual actuation logic, there are a lot of safety control functions that are being performed in those systems. So, it's not separated. We would consider that. You would have that integrated A1 system and you would have to analyze it accordingly.

CHAIRMAN BROWN: Thank you very much. Can you hear me now? Okay.

The level of integration relative to isolation, I mean the one that struck -- I'll just throw this one out -- the one we have reviewed, where there was, for a number of the -- once you got out of the RTS, the reactor trip, and the ESFAS system, all the data flowed out. It went into a network, and that network had a -- I've forgotten the exact words -- segregated, distributed. They bracketed the software, so that part of the software controlled these functions; another part was partitioned into another part and did something, but it was all packaged within

the same set of processing systems. It just where it got it and how it was allocated was just a little bit theoretically partitioned and isolated, when it really is not. Okay. I've never liked that, but you guys bought off on it and we didn't say anything.

Because the critical systems -- I'm not criticizing; it's just that was a construct because you could live with that; whereas, you wouldn't have done that same thing, you would not have taken the reactor trip and ESFAS systems and put them into an executive-oriented where you partitioned the software to deal with each, but it was the same set of processors.

I understand what you're saying --

MS. ZHANG: Yes.

CHAIRMAN BROWN: -- but the chiller is not part of the reactor trip system. It's downstream, and if you look at the overall setup, it's completely isolated. It's a box setting over there with its own processors that's integrated doing something.

MS. ZHANG: I think that's very design-dependent.

MR. MORTON: Right.

MS. ZHANG: If you look at the APR1400, not for the reactor trip, but for the ESFAS portion,

the actuation logic actually flows downward and, then, integrates into the same boxes as the safety control functions.

CHAIRMAN BROWN: You mean in order to start an ECCS function?

MS. ZHANG: Start an ECCS, and then --

CHAIRMAN BROWN: And the chiller is in the same processing unit?

MS. ZHANG: Not necessarily, maybe not the chiller system, but a lot of the safety-related balance-in-plant functions.

CHAIRMAN BROWN: They were distributed in the architecture of the processing?

MS. ZHANG: Yes.

CHAIRMAN BROWN: That didn't come out in the discussions. I think we're going to have to write another letter on the --

MS. ZHANG: Maybe I should go on.

(Laughter.)

MR. MORTON: But, to Deanna's point -- and we've emphasized this before -- it depends on how a particular licensee has classified their systems. And we talked about in operating plants, if you have a HPCI initiation, you have the initiation's command features and, then, you have the actual flow control

feature. It would be a separate function away, physically separate from the initiation aspect. But, in advanced reactors, oftentimes, those are integrated within the same set of processors. That's why we're saying the whole integration thing is --

MEMBER MARCH-LEUBA: The explanation that it is application-dependent and we have to look into it --

MR. MORTON: Yes, correct.

MEMBER MARCH-LEUBA: -- to me, it explains what you are trying to say.

MR. MORTON: Yes, yes.

MEMBER KIRCHNER: Doesn't this beg you to start at a higher level? Because what I take away from the words, just the words, not the intent, is it's driving you down to component level and that's the basis for really trying to demonstrate susceptible or not susceptible to C3. When you really want to do it, and if these systems in the advanced plants are very integrated, whatever that means, then one needs to be looking at much higher level first at the architecture and, then, drilling down to a system and, then, to components. Does that make sense?

MS. ZHANG: Yes, that does. And if you look at some of the latest guidance we've put out,

such as ISG-06, Revision 2, as well as the DSRS -- and our current work was the Advanced Reactor Design Review Guide -- we are trying to drive down, starting from the architectural level, then going down to analyze for the various principles how the architecture supports meeting those principles.

It's just for this particular BTP, since we are revising a BTP and it's not integrated with the rest of the SRP, we've had to kind of put it in its isolation, exactly.

CHAIRMAN BROWN: An administrative logistics issue, we are -- I'm giving you all a heads-up -- we are going to break at 12:00. And this will allow some folks to try to work on this interference that we're getting (referring to the phone system). So, just look for a point in this progression that you think would be a place to break at about 12 o'clock.

I went through the next four or five slides. We are not going to get through four or five slides in the next 15 minutes, or I'd be very surprised if we did.

MS. ZHANG: So, let me just propose this: since this is at the beginning of the D3 assessment, and the rest of it is about the three bullet points to address the D3 assessment, I think it's a good

breaking point right now.

CHAIRMAN BROWN: Okay. All right. Do the members have any problem with that?

MEMBER MARCH-LEUBA: We don't need to start at 1:00. We could start at 12:45.

CHAIRMAN BROWN: Scott, what did you say?

MR. MOORE: Mr. Chairman --

CHAIRMAN BROWN: I can hear you, Scott.

MR. MOORE: So, Mr. Chairman, here's what we're doing. We've got an A/V expert in. We cannot get the other room up and running fast enough to change over just within the lunchtime, and that's why we can't just move over that quickly.

We are going to try moving the speaker, so that you won't get feedback on this side. And so, we will do what we can during the hour, and we'll try to figure out what's going on with the caller line. I mean, you all know that it's a temporary fix, but --

CHAIRMAN BROWN: No, I understand that, but it's just right now it's kind of interrupting --

MR. MOORE: Right.

CHAIRMAN BROWN: -- the thought process. You're trying to listen, but, yet, you've got the babble.

MR. MOORE: Absolutely.

CHAIRMAN BROWN: We have a little bit of a babble in the background.

MR. MOORE: We'll work with the A/V expert to try to get it fixed.

CHAIRMAN BROWN: Okay. Now we should restart at 1:00? That's the schedule.

MR. MOORE: We should start at 1:00 because that's the time we advertised.

CHAIRMAN BROWN: That's fine. Okay.

MR. MOORE: Thank you, sir.

CHAIRMAN BROWN: So, we'll break right now. We'll recess right now, and we'll come back at one o'clock. Thank you for the suggestion, Deanna. And we'll go from there. Okay?

Recess.

(Whereupon, the foregoing matter went off the record for lunch at 11:44 a.m. and went back on the record at 1:05 p.m.)

A-F-T-E-R-N-O-O-N S-E-S-S-I-O-N

1:05 p.m.

CHAIRMAN BROWN: The meeting will come back to order.

And one announcement before we restart with the briefers. For those on the phone line, a couple more people have come on the line since we asked this question a few minutes ago. Would you please place your phones in mute, so that interference is minimized? We will try to minimize the interference from our side as well. We will hope it works, as we have taken action over the lunch break. Okay. Thank you very much.

And, Deanna and Wendell, if you all want to get started?

MS. ZHANG: I guess I'll get started with saying, "Next slide."

So, the next few sections we're going to talk about what are the ways to address CCF within the D3 assessment. So, this includes means that you can use to eliminate CCF from further consideration or diverse means that can be credited to perform the same or a different function, as well as other means that can be used.

So, for the first one, means to eliminate

CCF from further consideration, this has been in the BTP since Revision 6, which is diversity within the digital I&C system or component. So, in this case, we just clarified the guidance a little bit and made sure that the acceptance criteria matched the review guidance.

And in this case, there wasn't a lot of change with respect to this particular means, which was the use of design attributes. So, really, we're looking at, if you have two divisions within a system being diverse from another two divisions and they're performing the same or different functions, then that would be one acceptable way of eliminating CCF from further consideration.

This particular attribute has been used in the NuScale, in the protection system there, as well as in the Wolf Creek MSFIS application. And one thing I think Member -- I'm not going to pronounce your last name -- Member Jose has mentioned during our break was consideration of maintenance of one division and the other two divisions having a common-cause failure. So, of two sets of redundant portions with two divisions performing one function and the other two divisions being diverse, if you take one of the divisions out of service for maintenance or testing,

what happens if you suffer a common-cause failure within the other two credited diverse divisions?

So, one thing we did add within the BTP -- and I'll read it -- is that, "It should be noted that since each redundant safety-related division is credited for compliance with a single failure criterion and is, additionally, credited to prevent CCF, the allowable time that a division can be bypassed, as specified in the technical specifications, may be more restrictive than if the redundancy is solely credited for meeting the single failure criterion. This is specific for each application."

So, we did try to address that aspect.

MEMBER MARCH-LEUBA: So, in that light, how does the CCF, common-cause failure, propagate to the Safety Analysis Report? Clearly, there is not anything in Chapter 15, design basis event, correct?

MS. ZHANG: Yes. So, a CCF is considered a beyond design basis event, and this has been the direction of the Commission, as specified in the SRM-SECY-93-087.

MEMBER MARCH-LEUBA: But it would affect Chapter 19, "Probabilistic Risk Assessment". So, the frequency of the system being unavailable increases if

you have one in bypass mode and you are susceptible to CCF on two of the remaining three. And that will, I guess, translate to how much time you can have the system in bypass. Depending on your tech specs, how much you are allowed to have your system in bypass, it will give you the frequency that you have to input. So, these will have to be evaluated in Chapter 19.

MR. MORTON: Yes, as Deanna was saying, that's another aspect that's a plant-specific item to make that determination, based on the licensing basis.

MEMBER MARCH-LEUBA: Is there any guidance to how to guesstimate what the CCF frequency is? I mean, we're happy in the I&C in the Chapter 7 domain to say it's possible. Now these guys have the difficult job of saying it's 10 to the minus 4, 10 to the minus 8, 10 to the minus 25.

MR. MORTON: Generally, with this guidance, because it's following the direction of the Commission on this, we don't get into estimates of frequency in time when it comes to the CCF. It's really to ensure you have adequate defense-in-depth in the presence of a postulated CCF.

MS. ZHANG: So, we will phone a friend.

(Laughter.)

MR. REBSTOCK: Paul Rebstock, the Office

of Research.

And we're in the early stages now of initiating a research project to do just that, to looking at ways to quantify software for digital-system-related failure rates and, also, a separate project that's looking at common-cause failures and the question of how to risk inform when you don't have numbers. Both of those are present, you know, current issues.

MR. HECHT: Are you aware of past efforts to have done this from many different sources, both within Research and from ORNL and others? And how is the current research going to be different?

MR. REBSTOCK: I know that there have been a lot of efforts to do this in the past, and some people are skeptical as to whether it could actually even be done. Exactly how this particular project is doing it, I'm not involved in the project, so I'm not sure exactly how they're going about that.

MR. HECHT: It's not a matter of skepticism so much as it is a matter of whether the data that's being used and the operational experience that's being collected is truly representative. And there have been problems in past NRC studies to do that.

MR. REBSTOCK: Yes, I think that's true, and I think there are also issues about definitions, and how things are quantified, how things are categorized is also a legitimate concern.

MS. ZHANG: Okay. Thank you, Paul.

MR. REBSTOCK: Okay.

MS. ZHANG: Next slide. No?

CHAIRMAN BROWN: Stay there. When you talk about being tested, how does this thought process affect operation with a particular division out of service for a while? Does that mean you have to shut down?

MS. ZHANG: So, we envisioned that the tech spec time limitations for a division out of service may be more restrictive in this particular case. But, again, that is a design-specific issue, and I don't think we can provide specific numbers on how much the time will be reduced by right now.

CHAIRMAN BROWN: I mean, the normal thought process -- and this is in my own mind because I can't even envision the projects I used to have if one of our divisions, redundant divisions, were out of service; you operate because you still had two out of three in operation. Is that not a concern in the commercial world? When you say "the tech spec," does

the tech spec drive -- I don't remember a tech spec that says -- always kind of assumed that, if you had four divisions, you could operate indefinitely with one division out of service. But I'm just not familiar with a tech spec that restricted that. So, you're telling me there are?

MR. MORTON: So, for an operating plant -- and this would be comparable to advanced reactors, too -- you would still be expected to meet the criterion for single failure with one channel in bypass or one division in bypass for some particular reason. If you end up having another division fail and you can't meet your single failure criterion, you're going to end getting into a tech spec LCO. It may get into a shutdown, but that depends on the plant and its configuration.

CHAIRMAN BROWN: Well, that wasn't the point.

MR. MORTON: Okay.

CHAIRMAN BROWN: One is out of service for some reason.

MR. MORTON: Uh-hum.

CHAIRMAN BROWN: I'm operating with three. I'm now two out of three for generating my scram, or whatever it is. You can handle a single failure and

you can still get your protective actions.

MS. ZHANG: Yes. So, in this case, it's a little bit different because you're not doing -- in the design, it's not a two-out-of-four strictly, just like in NuScale it's not a two-out-of-four. Because your crediting diversity was in the design, so two divisions would be performing one function.

CHAIRMAN BROWN: I understand that.

MS. ZHANG: And the other two divisions would be performing a diverse function for that particular event or the same function. But what we're saying is that, if you do have to bypass one of the divisions with the one-out-of-two, then if you were to have a common-cause failure with the other two, you're left with one division having to --

CHAIRMAN BROWN: I know that.

MS. ZHANG: In that case, we're saying that the tech specs may be more limiting because you're creating diversity within the design.

CHAIRMAN BROWN: I understand that. It just still --

MEMBER BLEY: There's another side to this and it's not an electronic side. In fact, a long time ago, if you didn't have tech specs on like three pumps and you only needed two, there were conditions where

one of them was essentially used as a parts inventory and it just wasn't there. So, there's always been a drive to make sure you have some restoration.

CHAIRMAN BROWN: No, I understand that point. I understand the drive to a fix is a point that's a valid -- I'm aware of that. It's just that I'm trying to sit here thinking that you talk about using risk concepts for something. It just seems to me that you're not going to turn off the electricity for a half a million people because it's kind of a hard choice to make because one of your systems is out, and it might take you two or three days to get it serviced and put back in operation.

MS. ZHANG: So, in this case, this is where the architecture would help. So, instead of having just -- you're bypassing an entire division, right? You can have redundancy within a division, so you are only bypassing a processor. That way, the tech spec's limitations aren't as restrictive as if you were bypassing an entire division.

So, this is where I think digital technology does offer a lot of benefit and flexibility for this particular use of this particular --

CHAIRMAN BROWN: Yes, but if you look at a particular -- back into one of the particular

designs that has processors in it, each division effectively had one processor processing all the data and, then, feeding, generating a trip, and that would then get sent out to the voters. There weren't multiple -- I mean, it couldn't just bypass a processor. You may be able to bypass a function or negate the response of a function via a test switch of some kind, but that would still take that function out of service for a period of time.

So, there's a lot of conundrum; there's a lot of different variations within -- it's just the whole concept just seems to be driving this in the wrong direction in some way, without having some other assessment that allows some flexibility.

MS. ZHANG: I think by merit of saying that this is design-specific and that this is part of a LAR, as opposed to -- you know, so this will be evaluated by the staff as far as how much the tech specs contributed, how much the PRA contributed. So, I think it's more of a holistic look at the overall system and the different aspects of it.

MR. MORTON: And to touch on what Deanna just said, the goal, overall goal, of the BTP is to ensure you have a diverse way to accomplish the safety function in the presence of the loss of that

particular safety function, if it's to stabilize CCF.

In terms of all the other considerations, in terms of outage time for the particular system through the tech specs, that's a consideration each plant has to deal with within their own assessment in terms of how their tech specs are written.

CHAIRMAN BROWN: This is a downside to the whole idea of having diversity from that standpoint then. It restricts your ability to maintain the plant operation in a rational way.

MS. ZHANG: I think it depends on how they implement it. We've certainly seen designs where they have multiple processors within a division to perform the safety functions. So, again, I think this is very design-specific, and the level of redundancy within divisions and within the overall I&C architecture I think needs to be considered when using this particular means to eliminate CCF.

CHAIRMAN BROWN: Okay. I've mouse-milked that enough, unless somebody else has a comment.

Dennis, did you want to say something or --

MEMBER BLEY: No.

CHAIRMAN BROWN: Myron?

MR. HECHT: Yes. I'm sorry.

CHAIRMAN BROWN: No, go ahead.

MR. HECHT: I was looking at the language of the actual BTP, Revision 8, and I'm having trouble understanding what constitutes sufficient diversity. Let's just deal with -- I don't know -- a spectrum ranging from two software-driven processors driving the same function to one processor having a different operating system, to processors having different languages, to one being an FPGA, and so on. How is the staff going to know what sufficient diversity is?

MS. ZHANG: So, thank you, Myron, for that question.

One thing is we do reference the six diversity attributes within NUREG-6303. We did reference that. In addition, one of the new things for this revision of the BTP is that we incorporated, we referenced NUREG-7007, which was developed in 2008 to provide a qualitative way of evaluating sufficient diversity. So, it gave additional criteria to evaluate what is sufficient diversity.

MR. HECHT: Okay. So, in my case of all those functions controlling a relief valve for pressure, where would you say it's not acceptable among the four that I gave? Clearly, having two identical, software identical processors is not

acceptable, even though there's physical diversity, you might argue, and then, the redundancy. But where does it work that way?

MS. ZHANG: So, we do look at equipment diversity. So, in that case, you wouldn't have equipment diversity. We also look at signal diversity. So, are the same sensors feeding both different processors? We would also look at whether there's any human diversity. Did different design teams program the different parts of the processor? So, those are all things that we would look at to see if there is sufficient diversity.

And right now, without a full analysis, I don't think I can give you a "just do this" type of design without considering the overall system design.

MR. MORTON: And also to that point, fundamentally -- maybe we don't make it clear in this section -- overall, you're trying to ensure that the two different widgets aren't subject to the same type of CCF based upon, for example, some common port or common trigger within the design. Signal diversity is one aspect you're trying to remove a commonality between two different divisions. Equipment diversity, software diversity, these are all common aspects that could fail two or more different devices concurrently

or within the same timeframe. Fundamentally trying to ensure that they're not subject to that is the point of that. We might not have made that necessarily that clear here, but that's generally the idea, what you're trying to do to demonstrate sufficient diversity.

MS. ZHANG: Yes, and in NUREG-7007, it tries to provide a little bit more weight on the different types of diversity. So that you can say, well, is equipment diversity the most important or is it signal diversity? And so, I think by incorporating NUREG-7007, referencing that in this revision, I think we are actually providing more criteria for measuring what is sufficient diversity.

MR. HECHT: Okay. Thank you.

MS. ZHANG: Slide.

So, I think this one of the ones that was on everyone's mind when we first started this, which is the testing criteria as a means to eliminate CCF from further consideration. When we went through this, at first we thought maybe we should just get rid of this testing. There's so much confusion as far as what constitutes sufficient testing. Originally, we had the term 100 percent testing. Well, what is 100 percent testing? And that added to a lot of uncertainty from the licensees and, actually, from the

staff, because there was a lot of contention as far as is this sufficient testing.

Ultimately, we decided to leave it in because, one, we wanted to provide flexibility, because it may be applicable to a very simple portion of the design, right? So, it might not be applicable to an entire system, but maybe a component within the system where you can at least eliminate that part of it from the rest of the D3 assessment. So, that's the reason we decided to leave it in. We got rid of the 100 percent testing terminology and just provided the criteria associated with that testing.

Now one thing we did note in this is what does testing buy you. For one thing, it is that if you have system requirements that resulted in CCF, testing is not going to necessarily tell you what those system requirements are or not, right. These are really meant for the design implementation aspect. So, what testing will tell you is it will reveal any latent design and implementation errors, theoretically. And then, with that, you will be able to say, well, either you fix that or you say this is a methodology we can use.

But this could only be, this testing methodology is really only intended for very, very

simple devices and components, not a system. Because we recognize the number of test cases, once you add in more than a few inputs or having memories/internal states, the number of test cases will get virtually impossible in testing in a reasonable amount of time. So, we did add that as a caution.

MEMBER BLEY: You've had a lot of public meetings on this and interactions with people. Are there stakeholders who are really strong on the testing and are there specific things they think that will help?

MR. MORTON: So, part of the process for developing this refinement in the guidance, we actually solicited a lot of feedback from industry in terms of their ideas for how we wanted to have testing to eliminate CCF as being a tool that we didn't want to leave out of the toolbox. But, clearly, the current version in Rev. 7 it is not feasible for most applicants or most licensees, or applicants, too. So, trying to provide a more flexible approach to eliminate CCF reasonably was what we were looking to do. It wasn't a situation where we kind of came up with this entire criteria internally. It's something we got a lot of feedback from industry to say what specifically input would be beneficial to use this as

a tool to help simplify the D3 assessment by eliminating certain portions of the system from having to be part of the D3 assessment.

MEMBER BLEY: I think you wrote in enough caveats to protect us from a cavalier approach to testing, but you may get into some difficult arguments along the way on the testing side, I expect.

MS. ZHANG: Yes, I think this is an area where really it will be a lot of attention will have to be paid on if this particular attribute or means is used, and in terms of what methodology was used for the testing; for the cases, the test cases, the actual system, the actual device and component-level design, and what are the inputs; what are memory states, et cetera. So, this isn't intended to be applicable to a lot of systems or components, but very, very simple ones.

CHAIRMAN BROWN: That's pretty clear. You eliminated the words "100 percent" usually. But if you look at the lead-in sentences for A, B, C, and D, like the combination of every possible input or all possible timing sequences, or any kind of memory, et cetera, et cetera, et cetera, fundamentally you've couched the 100 percent in the words without saying it.

MS. ZHANG: Well, there are --

CHAIRMAN BROWN: I'm not criticizing that because that's -- I don't interruptions. Don't worry about that. Okay?

MR. MORTON: So, Member Brown, you're right. So, one of the things we wanted to keep in mind with this testing aspect is that the original design attribute was titled simplistically or sufficiently simple, such that it could meet all those particular testing attributes. So, we wanted to maintain that theme, but not necessarily watering it down, so to speak, but it has to be a high level of assurance that you've covered enough test cases, et cetera, et cetera, without necessarily being 100 percent. Because we've had certain cases where the staff has accepted a high assurance level of testing without it being 100 percent.

MS. ZHANG: This is where D comes in. So, we've seen cases where there are unused parts of an overall component, right. So, if there are unused part of a circuit, and they can show that that unused part does not affect the actual functional part, then those particular aspects won't have to be included in the testing. So, this is where we see that relaxation.

MR. MORTON: So, there's potential benefit if a licensee or applicant can demonstrate that, if there's code or unused portions of a particular device, and if the device fails or restarts, that unused portions will not somehow affect the operating portions. We're trying to put that flexibility in there, so that it doesn't necessarily have to be 100 percent all logic-tested, because we do recognize there are cases where not all logic is being used or implemented within a particular device.

MR. HECHT: Does that mean that, moving forward, you might consider a memory partitioning, so that, for example, if you're only using 1000K for location of your critical process variables in a IC that might have 256 MEGs, you won't have to worry about the other 256 MEGs?

MS. ZHANG: I think it really has to do with, one, do you have discrete cases you can test, right? And also, whether the other parts of the processor can influence the part that you're using. So, if there's no way to isolate them, you know, so the partition -- because if you're just partitioned, there still may be some interdependencies among the partitions.

MR. HECHT: What if I include a hardware

memory management unit?

MS. ZHANG: Again, this is where we'll have to get into the details and exactly how it's implemented. I don't think we can give you an answer right now.

MR. MORTON: Yes, in that particular case, what we were trying to do is give high-level criteria without giving specific design solutions or appearing to give something a little deeper than what we're trying to get to because of all the variations in what a licensee applicant can provide.

MS. ZHANG: But this wasn't envisioned for a microprocessor-based system.

MR. HECHT: It was not?

MS. ZHANG: It was not.

MR. HECHT: Okay.

CHAIRMAN BROWN: For testing?

MS. ZHANG: For testing.

CHAIRMAN BROWN: Oh, yes, I got it.

(Laughter.)

MS. ZHANG: Okay. Next slide.

So, this is, I think, one that Member Bley had identified, as well as Member Brown, as far as the defensive measures. Because although we say this could be used as a means to eliminate CCF from

consideration, and we did provide some criteria as far as what those defensive measures have to demonstrate, the acceptance criteria referenced a NRC-approved methodology. And the reason that you won't find that NRC-endorsed methodology within this document is because that doesn't exist.

CHAIRMAN BROWN: It doesn't exist.

MS. ZHANG: Yes.

So, this was intended to give flexibility because we do anticipate that industry, particularly with NEI and their EPRI research, that they will be coming in with a methodology that can be endorsed by the NRC. This was supposed to be NEI-16-16. I think because of other constraints, that wasn't completed in time for this BTP. However, we didn't want to issue this BTP and not recognize that that may still be a possibility.

But we did add in a sentence in there in terms of, if a particular application wants to come in to credit their specific defensive measures, and they provide the methodology and the technical basis, then we will evaluate that on a case-by-case basis as part of the application.

So now, we've gone towards the mitigation portion of how the CCF hazard can be addressed. In

the next couple of slides, I'm going to talk about the diverse means that could be used to perform the same or different function as the safety function postulated to be disabled by the CCF.

And again, if you look at the original SRM, it does say --

MEMBER BLEY: Can I jump in with something?

MS. ZHANG: Uh-hum.

MEMBER BLEY: In your guidance, just before you get to this, at the higher level, at the 3. -- there's no 3.0 -- but at the 3 level, which is diversity and defense-in-depth assessment, which you'll do for A1, the details really start at 3.1 with diversity. At that higher level, you have a set of acceptance criteria, and it makes me a little nervous that we have acceptance criteria before we get into the details. It's almost like you don't have to go into the details. And if that's what you mean, and if this is the vulnerability assessment, it didn't jump out at me that that was the case.

MS. ZHANG: So, part of the discussions we had during break is the need to enhance the structure as well as the flowchart to make it more obvious where are we having guidance and acceptance criteria, and

whether you eliminate the CCF hazard, mitigate it, or cope with it, that those are all acceptable paths. They're not linear.

MEMBER BLEY: Okay, I agree, you need to clarify that.

MS. ZHANG: Yes.

MEMBER BLEY: Then, I'm happy.

MR. MORTON: Yes, we took that as part of the restructuring concern, that the impression may be given that it's a sequential, linear-type process, when really it's any particular path a licensee or applicant chooses to use would be acceptable.

MS. ZHANG: So, we identified three diverse means within this section of the BTP, including use of existing systems. So, this could be your ATWS system. It could be other existing systems. And if you can show that the existing system is of high reliability and of sufficient quality -- and in this case, what we mean by "sufficient quality" is something comparable to the quality guidance within GL 85-06 for an ATWS system -- and that it can perform the function within a reasonable amount of response time, and that it's not subject to the same CCF, then that would be an acceptable means.

For manual operator action, this is an

area where we did get a lot of industry feedback for use of manual operator actions, particularly with respect to -- yes?

CHAIRMAN BROWN: Before you get there, you open up 3.2 with the words that say, "A diverse means," per position 3. "A diverse means should be provided to accomplish the same or different function disabled by the postulated CCF." In other words, you must have a diverse means, which is pretty clear.

And then, you go through the crediting part, and that's where you get to the "equipment to be credited is highly reliable and of sufficient" -- and you're talking about associated equipments; in other words, an already existing system. And you say, "to credit an existing plant system as a diverse means". Those appear to be not consistent with the opening statement. We go from you must have a diverse means, but, then, an existing plant system. And if you look at all it's got to be is highly reliable, right away you're into a quality or a judgment, and it's like a risk assessment effectively. Am I reading this wrong?

MR. MORTON: So, Deanna correct me if I'm wrong, but I believe within the Commission direction that the diverse means does not have to be safety-related. It can be non-safety-related as well.

CHAIRMAN BROWN: I got that part.

MR. MORTON: So, therefore, when we say "highly reliable," we weren't trying to say Appendix B quality or anything to that extent, because it simply needs to be highly reliable because it can be non-safety-related.

CHAIRMAN BROWN: But how do you define "highly reliable" if it doesn't have a set of recognized quality control requirements from the design, the production testing, component selection, et cetera, et cetera? I mean, this is really fairly well undefined as to how you really define that. If I was a licensee trying to do it, I would be struggling with that.

I mean, that's all. I understand the words. I understand the concept. I don't have any problem with the concept. It's just the use of the words "highly reliable" and "of sufficient quality". "Sufficient quality" has a whole range of meanings.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Just the testing of those parts when they're manufactured is one realm. If they sample test, and 1 out of every 1 million can fail as opposed to 100 out of every 1 million can fail, that's a difference; that's a substantial difference.

MS. ZHANG: Thanks, Member Brown.

So, the reason those words were there was because those were the direct words within the SRM to SECY-93-087.

CHAIRMAN BROWN: You can tell it was written by people who don't know what they're talking about.

(Laughter.)

MS. ZHANG: And the reason what those words were placed in there was because -- this is from what we can gather -- is, originally, in the SECY paper the staff said you need to provide safety-related diverse means. That part was taken out by the Commission at the time.

CHAIRMAN BROWN: Yes, and I agree with that. I happen to agree with it.

MS. ZHANG: But if they said, but in that consideration, they needed to put some sort of boundary as far as what system that's not safety-related you can use, what diverse means that's not safety-related you can use. So, they used the words, with a lot of flexibility, "highly reliable" or "of sufficient quality that's not subject to the same CCF". So, this where we got into -- we did reference the six attributes within NUREG-6303 as far as subject

to the same CCF. We did add in a part about having comparable quality to an ATWS system, as provided in the guidance of GL 85-06. And as far as the reliability aspect, I think that's a lot of it; it would be engineering judgment.

CHAIRMAN BROWN: Let me just retrofit this thought process to the basic, original safety system design, that you've got your four divisions. They're highly reliable. They're of high quality, highly tested. Why do you need to consider that they're going to all fail from a common failure simultaneously? You've effectively said it's okay to have a system that may do that. It's non-safety, but it's highly reliable, of high quality.

MS. ZHANG: So, I think it is -- you have to look at it from independent events.

CHAIRMAN BROWN: You can see where I'm going, can't you?

MS. ZHANG: Yes. So, we're concerned from independent events. If you're looking at it from just a safety-related system, do we postulate that, with a high frequency, that it is going to experience a software common-cause failure, such that you will need an independent safety-related system? We're obviously saying no, because that system is Appendix B

qualified. You do have four division. You have independence. A lot of that goes into the design and architecture of the safety-related I&C system, your protection system.

But, given that, if you have a complex visual system, and you can't test out the latent software defects that is in it --

CHAIRMAN BROWN: What is a latent software defect?

MS. ZHANG: A latent software defect is --

CHAIRMAN BROWN: I was going to go ahead and ask you that question. It's in the title.

MS. ZHANG: Okay.

CHAIRMAN BROWN: I don't know what a latent software defect is.

MR. MORTON: Well, finish your thought first.

MS. ZHANG: Okay.

CHAIRMAN BROWN: I'm sorry.

MS. ZHANG: So, let me finish that before I come back to what a latent software defect is.

That you will still have a means of addressing that particular event. So, because the likelihood is sufficiently low, this is why the diverse means can be non-safety-related, but with some

caveats as far as its quality and reliability.

MR. MORTON: Let me say that a little bit differently.

CHAIRMAN BROWN: No, let me --

MR. MORTON: Because of the high-quality testing, V&V, all that good stuff, of the protection system, one of the reasons why the Commission's position moved from having a diverse safety-related to diverse highly reliable means is because of the quality of the protection system that was built and designed to.

CHAIRMAN BROWN: And I would argue that, if it's that high of quality -- you talk about a latent software defect. The most likely -- and here I'm into the risk thought process, I guess -- software defect is a programming error that doesn't allow you to accomplish an end-state when it's asked. However, how is that likely to happen? Do all of them get confused at the same time when all of them have different clocks that are not synchronized? Do they all get the same data stream and field of data that's coming through that could possibly confuse it?

MR. MORTON: Well, that's the reason you have the six diversity attributes --

CHAIRMAN BROWN: Yes, but --

MR. MORTON: -- that you have in 6303. They're designed to prevent you from having a common trigger that could trigger that particular latent defect.

CHAIRMAN BROWN: You've got to figure out, you've got to have some idea of what you think a latent defect is. I mean, you've covered just about every -- with the independence of the architecture, components are already highly reliable. You're not worried, if a processor fails, bang, it just quits; it doesn't matter in one division. All of those are fundamental.

They're similar to analog systems. A piece can fail, an output can fail, all those types of things; a single failure can occur. And the only real thing that could hurt you is somebody programming it wrong and having that same error all the way -- however, you test to see that the inputs run up through the stream of data and that you get a trip throughout the range of it's supposed to be tripped, and it lights up its lights and it triggers whatever the voting unit is supposed to be, you know, when it finally gets to the voting unit.

Somewhere along the line, you've got a very high-quality system and, yet, you're trying to

say something, even though I've got it totally independent, nothing is synchronized, I'm not crossing data streams, independent data going to each channel from separate detectors, okay, none of them are providing this, and if there was a field that had a corrupted thing that would trigger this, quote, "programming design error," the idea that it's going to strike exactly at the same time, in all of them at the same time, is somewhat aberrational. How's that for a big word?

MEMBER BLEY: So, you're hanging part of your argument on the idea that you have to have defective data coming in --

CHAIRMAN BROWN: No, it's just one way.

MEMBER BLEY: -- to drive --

CHAIRMAN BROWN: Just one way.

MEMBER BLEY: -- to get into a spot that's triggered in this hidden flaw in the software. And it might be that all the data are good, and it's just that the plant got into a condition you hadn't looked at before.

CHAIRMAN BROWN: You know the range of pressures and temperatures at which you operate and at which you exceed --

MEMBER BLEY: At which you're normally

operating.

CHAIRMAN BROWN: At which you exceed --

MEMBER BLEY: And what we protect against are the cases when we're operating outside of where we normally operate.

CHAIRMAN BROWN: Yes.

MEMBER BLEY: So, I don't think your argument hangs.

CHAIRMAN BROWN: I don't agree with that.

MEMBER BLEY: It's pretty good. It says it's a pretty darn good system, but it doesn't cover the case they're talking about and the one --

CHAIRMAN BROWN: But if you've got range covered, you've got range coverage, out-of-range coverage, so when you get outside, it's really the range of the instruments, not so much the range that the plant could be in. As long as you know where the plant is --

MEMBER BLEY: As long as the plant stays where you thought it was worth testing originally.

CHAIRMAN BROWN: Well, then, that's got to be within the range of what you're doing, if you've got all the data coming in over the range of temperatures, pressures, flows, levels, et cetera.

MEMBER MARCH-LEUBA: Yes, but there is

something else you need to consider, this missing data. When you start having one or two failed sensors, when you expect four temperature sensors, but you are getting only three, and that --

CHAIRMAN BROWN: Well, that's a single failure.

MEMBER MARCH-LEUBA: Yes, but a single failure that propagates into the software, and the software needs to have programming correctly. And it makes it very difficult to test every possible combination of three different failures.

MS. ZHANG: Yes. I'm going to -- thank you, Member Brown and Member Jose.

CHAIRMAN BROWN: Are you trying to tell me to shut up?

(Laughter.)

MS. ZHANG: I'm going to take from another industry, and this is the Boeing 737 MAX. I recently read the Joint Assessment Technical Report that came out. And one of the things that it went on about is, one, system integration and the complexities of the systems making it not easily analyzable. And because of that, a lot of the behaviors of the system and the software is not necessarily what you would have expected when you started doing your design.

This is even further an issue when you have changes as you are designing and implementing the system, where your original assumptions may not be what actually gets implemented into the software and the system.

So, this is why we emphasize that software common-cause failure is a hazard, that while we have these great testing programs and quality of the systems and design, we still have to assess for the potential of a CCF.

CHAIRMAN BROWN: I would argue that is apples and oranges. I absolutely agree with you on the 737 MAX stuff. I haven't read that report, the most recent one. I've only read excerpts occasionally for interest purposes. But that is a highly-integrated feedback-control system with degrees of freedom that are unrealized or not even associated with the systems we deal with. On top of that, it integrates operator actions which can theoretically override or not override, or have the operator overridden because he tried to override.

That is not the case with our systems, so that you don't have that complexity of logic detail that you have to deal with. And I would argue that it's a good point, but, as Dennis told me, okay, I

would argue that overkills relative to comparing that. Do we have to consider that for these systems which are once through, you know, take data once through, tell it to go this way or that way. There's no operator intervention, not a feedback control system.

I just would argue I'm just trying to provide a thought process for somewhere in this whole setup that we integrate some common sense maybe about the level of goodness or badness of these systems. I'm here to provide some thought processes which may or may not be agreed with. But, personally, I think we have overdone it relative to what we consider we have to take care of.

There are manual means that can be used in most of these as long as you've got displays that are, quote, "independent". You know, they may be getting the data from some of the same detectors, which they will be, but, again, a single failure of those with the multiple sensors you've got covers that particular circumstance.

Anyway, I'm just trying to provide some counter-thought to what I've been listening to for 10 or 12 years. I'm not disagreeing with the thought process; just how do we address it? That's all.

MEMBER BLEY: You seem to be saying we've

done such a good job, these things can't happen. And, in fact, we had presentations some years ago where we were shown some cases from the aerospace industry where a number of these events have happened, where the data came in, real data, and took us outside the range of where we were expecting things, and systems went wrong.

I'm trying to remember where you were on one of your arguments there. But we've seen cases in nuclear power plants in other systems, and some folks have drawn this kind of conclusion, where taking operators out of the realm of where their experience lies can lead them to do things you don't expect. And there are some folks that are maybe we can use that same approach on software. Nobody has figured out how to do that well yet.

But I think there are enough cases that we want to be really careful. When people can react easily to one system shutting down and all I have to do is start it up again, people don't react too well to cases where things are failing outside of their normal experience and training. And they do odd things. And we don't want to put them in that spot. So, spotting these things ahead of time, we're making as sure as we can that they don't live there. It

seems a really good idea to me. And I think they're on the right track here.

CHAIRMAN BROWN: That's why you have some of these systems automated, like we've done with the trip system. That's the really critical ones. That's why we do that. And the operators are not there to be the primary -- I agree with you.

MEMBER BLEY: And as long as those systems work the way we designed them, everything is hunky-dory.

CHAIRMAN BROWN: And we design them heavily and we look at them. I have a difficulty with the aerospace and airplane industry because our systems, our feedback control systems with human interactions that are integrated into that are extremely complex to make sure they get it right because there are so many undefined areas where you may end up.

Here, we have a very structured and a far more well-defined -- it doesn't mean we might not have a problem, but it's a pretty well-defined --

MEMBER BLEY: As long as things fail in the neat order we've planned, that holds up.

CHAIRMAN BROWN: You can see that we have a unanimous agreement on the Subcommittee.

(Laughter.)

MEMBER BLEY: Yes, we're not as far away as all this sounds, but --

MR. MORTON: And, Member Bley, you raise a great point. Before we go on, I want to make this point.

CHAIRMAN BROWN: You're not going to agree with me? You're going to agree with him?

MR. MORTON: I'm going to agree with you both.

(Laughter.)

But I want to bring more context now.

CHAIRMAN BROWN: Oh, oh, oh, you're trying to split this. You're play Solomon, right?

MR. MORTON: Maybe.

CHAIRMAN BROWN: You're going to split the baby.

MR. MORTON: Maybe. But, in terms of CCF for an I&C system, you've got different measures for different types of phenomenon hazards you're looking at. You've got fire zones. You've got physical isolation independence for electrical faults and fires. You've got seismic qualifications, just in case the ground moves and shakes things up, causing a potential CCF or a spurious actuation.

But in software it's a little different because with seismic qualification I can get to a certain point I can quantify what this plant is rated for based on its location. But software, potential bugs or latent defects, however you want to characterize it, it's a little different.

We all know that there are various design features and measures in place and state-of-the-art systems. You have self-testing features. You have things looking at data frames to make sure you haven't lost corrupted data. You've got things ensuring that, if you get bad signals, you switch that particular sensor feed off. You rely on those things. There's a lot of measures and design features we have in place, and that's what we tried to get to, to provide licensing flexibility to address them.

And that's really sort of the goal when we were getting into all the diverse means part. That's the overall, general context, but we take your feedback and we understand what you're saying.

CHAIRMAN BROWN: All right. Go ahead.

MR. MORTON: Okay.

MS. ZHANG: Okay. So, I think this is a good opportunity again to manual operator actions, which is another area where, as I had started this

conversation, that we got a lot of feedback from industry stakeholders.

In particular, they wanted us to clarify whether the manual operator actions, whether they had to be performed within the main control room, whether the equipment that is used for the manual operator actions, whether it has to be in the main control room or could it be somewhere else within the plant, and how does that all tie together? And because in previous revisions we had stated an acceptance criteria that any manual diverse means, it has to be at the system or division level, depending on the design, and that has to be from the main control room, there was a lot of question as far as, well, can this be at the component level; can this be outside the main control room?

And when we reviewed the SRM, between position 3 and position 4, we noticed that there are essentially two separate ways you can read that, whether 3 can be 4; can something that's credited for performing 3 also be credited for performing position 4, and the other way around? So, when we looked at that, we said, obviously, position 4 was very, very specific. It didn't give you any flexibility.

CHAIRMAN BROWN: The main control room?

MS. ZHANG: Yes, from the main control room. And that has to be system level, actuations of the critical safety functions.

CHAIRMAN BROWN: Actually, downstream, you left out the word "downstream" someplace in here also.

MS. ZHANG: I think in the SECY paper it talks --

CHAIRMAN BROWN: You've got to bypass --

MS. ZHANG: Yes, the SECY paper talked about downstream, but not at the --

CHAIRMAN BROWN: Bypassing the --

MS. ZHANG: The logic.

CHAIRMAN BROWN: -- logic area?

MS. ZHANG: Yes.

CHAIRMAN BROWN: Yes.

MS. ZHANG: Not subject to whatever.

CHAIRMAN BROWN: Bypass the computerized portion?

MS. ZHANG: Yes.

CHAIRMAN BROWN: You left that out.

MS. ZHANG: Yes. So, in that case, we still wanted to maintain that because we're not changing the position within the SRM for that aspect.

CHAIRMAN BROWN: I wouldn't disagree with you on that one. You're probably surprised.

Let me ask a question relative to that. Outside the main control room, I don't know what the staffing is like outside the main control room. It's not like the plants I was familiar with. We had the main control room and, then, we had seven guys out in the space. You could trip turbines. You could start pumps. You could do anything you wanted to, and it took you -- I won't say microseconds -- but it did not take long to get something taken outside.

And based on the plants I've walked through commercially, which is two or three of them in my tenure here, it didn't look like the staffing out in the plants was all that readily -- where you could send a guy running upstairs and downstairs and around the corner to --

MEMBER BLEY: Well, they can do that, but they don't have people on station the way the Navy --

CHAIRMAN BROWN: That's what I mean, the staffing right down in the plant. They may have them on the site, but they don't have them in the plant.

MR. MORTON: They've got floor operators walking the site routinely, as well as maintenance --

CHAIRMAN BROWN: Yes, but they're not at an operating location --

MR. MORTON: They're not at a particular

station.

CHAIRMAN BROWN: -- the way they are on a warship.

MR. MORTON: Right. Yes.

MS. ZHANG: But, in terms of position 3 was in the SRM, it doesn't specify whether the diverse manual means has to be, was in the main control room, and whether it has to be system level.

CHAIRMAN BROWN: But 4 covers that.

MS. ZHANG: So, where we see this is that, if you meet position 4, you can credit the controls in position 4 to meet position 3. However, if you were to choose to credit other manual operator controls and indications outside the main control room, then those controls cannot be used to meet 4. So, it's not an "if and only if".

CHAIRMAN BROWN: But you also have to demonstrate that the ones outside the main control room do what they were intended to do, if you're going to credit them.

MS. ZHANG: Exactly.

CHAIRMAN BROWN: Even though they may not substitute.

MS. ZHANG: Exactly.

CHAIRMAN BROWN: That's reasonable.

MS. ZHANG: In addition, I know one of the points that were identified earlier was, why is the 30-minute margin, why is that not in here anymore? And the reason it is that way is because we're trying to align with SRP Chapter 18, which recently underwent a revision, where they want to take it from a more holistic look, and not just at a timing aspect, but also the accessibility of the equipment, the reliability of the equipment, and the availability of the equipment during the associated event conditions.

MEMBER BLEY: We had actually encouraged that once upon a time because some things are very simple and easy to do.

CHAIRMAN BROWN: I agree. Yes.

MEMBER BLEY: And 30 minutes is much more time than you need.

CHAIRMAN BROWN: Exactly.

MEMBER BLEY: Other things involve lots of interactions and, for some of those, 30 minutes might not be enough time.

CHAIRMAN BROWN: Well, but 30 minutes can also be equated to -- can you figure out what you need to do in 30 minutes?

MEMBER BLEY: Well, that's what they're saying. Can you get to it? Can you do it? And

you've got to balance that against how long it all takes.

CHAIRMAN BROWN: Yes. I still like the 30 minutes.

MS. ZHANG: Yes, this is why we do reference SRP Chapter 18 for the acceptance criteria in terms of the human factors engineering suitability analysis.

CHAIRMAN BROWN: Did we review that revision? I don't remember seeing that.

MEMBER BLEY: Some version sometime in the past, but I don't know -- not the most recent one.

CHAIRMAN BROWN: Not since I've been here.

MEMBER BLEY: Remember what you said about your memory earlier?

(Laughter.)

CHAIRMAN BROWN: Yes, but my memory is fairly good on the human action stuff because you beat me up.

MEMBER BLEY: We've got a letter somewhere on the same topic. I don't know if it's in exactly --

CHAIRMAN BROWN: It just sounds like it's now been changed in Chapter 18, and therefore, now they want to take it out of 1.152 or 1.53, whichever Reg Guide that was. Well, you didn't reference those

anymore in this, either. They were deleted from the relevant guidance. So, they're no longer relevant guidance in the BTP.

MS. ZHANG: Well, if you look at Reg Guide 1.62 in terms of where the manual system feeds in --

CHAIRMAN BROWN: No, you've got that one. It's 1.53 and 1. -- maybe it's 1.153 and 1.52. I've got it written down in here somewhere.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Two Reg Guides that were deleted from the relevant guidance list.

MS. ZHANG: Yes.

CHAIRMAN BROWN: 1.62 is in there.

MS. ZHANG: So, we are trying to remove the portions that weren't relevant to common-cause failure. If those were specific to addressing single failure criterion, we tried to -- because people were getting confused about is this for single failure criterion or is this for common-cause failure criterion, that's why there's some that we did remove because we wanted to remove that confusion.

CHAIRMAN BROWN: 1.62 is manual; 1.53 is the single failure criteria, and then, 1.152 is the criteria for computer use. I guess 1.62 is still there. I haven't looked. You all retained that one?

You don't have to look. I think you did --

MS. ZHANG: Yes.

CHAIRMAN BROWN: -- because I have a checkmark by it.

MS. ZHANG: Yes. So, lastly, it's the diverse system. One thing we did clarify in this is, if you have a diverse system, we don't want to imply that it must be an analog system. So, this is where you could have a digital diverse actuation system. It could be a part of another system. It could be a separate, standalone system, and it could also be a system that's not safety-related, provided that it's highly reliable, also quality.

So, there were a lot of perceptions of what this diverse actuation system needed to be. We wanted to make sure that we were clear in the guidance for this particular diverse means that there is flexibility in terms of the implementation of that diverse system.

CHAIRMAN BROWN: Okay. That's Section 3 --

MEMBER BLEY: Mr. Brown --

CHAIRMAN BROWN: Oh, I'm sorry.

MEMBER BLEY: -- just for your entertainment, in April of 2009 -- and I do believe

you were here at that point in time --

CHAIRMAN BROWN: Yes, I had been here for seven months. I had no idea --

MEMBER BLEY: -- we wrote a letter on digital I&C Interim Staff Guidance 5, "Highly Integrated Control Room Human Factors Issues". And we talked about and made recommendations on improving the guidance, adding additional guidance on the estimation methods of the time required for operator actions, and more.

CHAIRMAN BROWN: Although John put that back in in one place when we did the --

MEMBER BLEY: In any case, we have addressed it at times --

CHAIRMAN BROWN: Yes.

MEMBER BLEY: -- more than once, but that time in particular.

CHAIRMAN BROWN: I've got that. Okay, you've now convinced me that I was here.

(Laughter.)

But you and John were so persuasive that you probably winged it past me. I'm just teasing you.

Let me divert off; 3.2 is where this is fundamentally addressed. And if you remember my comment back earlier relative to elimination,

mitigation, and coping, you have to kind of read everything to try to figure out that that's point you're trying to make. And here, you've captured it in seven words and it's not in the lead-in of 3.2: diverse means, here's what we mean by that. You can use existing systems, manual operator, and here's a discussion of what we mean by that. It would have made it so much easier, because I haven't really categorized -- I never did condense it down to these three means as what you meant by that. It's just a matter of clarity and making sure that the lead-ins, the preambles define your basic framework and, then, discuss each of the allowable options.

MR. MORTON: Yes, comment noted.

CHAIRMAN BROWN: I don't have any problem with most of the stuff in here.

MS. ZHANG: Thank you.

Next slide.

Since I talked about this to great detail on the previous slide, I think I'm going to skip this slide.

CHAIRMAN BROWN: If there's somebody on the phone line, would they please make sure their phone is muted? We're getting some feedback. I'm not sure where it's coming from. We would appreciate the

help. Thank you. Sorry about that, those listening in.

MS. ZHANG: Okay. So now, I will pass it to Wendell to complete the rest of the presentation.

MR. MORTON: Should I wait until they get the phones -- should I just go for it? Okay.

Thank you, Deanna.

So, we've touched on the qualitative assessment portion of it earlier this morning. And really, its specific purpose is to apply technical criteria the staff thought was suitable for non-A1 systems, your A2-B1 systems, and B2 systems.

The basic qualitative assessment is taking, basically, an engineering judgment on the actual design quality and operating experience a licensee or applicant may have of a particular system they're modifying and the software and/or components they're modifying it with to determine whether the potential likelihood of a CCF is sufficiently low, so that you can make the safety case within the license amendment space. And that's just leveraging pre-developed content from RIS 2002-22, Supplement 1.

Yes?

CHAIRMAN BROWN: I'm going to give you a kudo because you read very quickly. You can see the

three items listed to see what you're trying to talk about in Section 4 right upfront.

MR. MORTON: Yes.

CHAIRMAN BROWN: So, that was a good approach.

MR. MORTON: Unfortunately, we may not have been consistent with that approach through the rest of the document.

(Laughter.)

Which we will take that when we take a look at it, yes.

CHAIRMAN BROWN: No, no. It was just it stood out here. So, it was obvious what you were trying to do, so that you could understand what you were going to read in the following couple of pages.

MR. MORTON: Yes. That's really all there is to the qualitative assessment. It's part of the overall new graded approach we've instantiated within the BTP.

So, is there another question on it?

CHAIRMAN BROWN: Yes, go ahead.

MR. MORTON: So, another key change we had was with the spurious operation assessment. Now Rev. 7 did have some guidance on spurious actuation. We redefined it as spurious operation to be a little more

technically correct. So, that's why it doesn't say --

CHAIRMAN BROWN: As opposed to what?

MR. MORTON: Spurious actuation. That's what it currently says.

CHAIRMAN BROWN: I didn't quibble with that word.

MR. MORTON: Yes.

MS. ZHANG: We wanted it, yes. That was actually a huge discussion --

MR. MORTON: Yes.

MS. ZHANG: -- because we want to be consistent with how it's used in fire protection.

MR. MORTON: Right. It became more of a quibble discussion. So, we just decided to go with a different paradigm for the phrase, and it's spurious operation going forward. So, we may slip back and say "spurious actuation". It's actually "spurious operation," in case one of us does that.

One of the challenges in this particular aspect is that the guidance previously was not very well-refined and not particularly clear. And in terms of if you're a licensee in operating plant space versus an applicant in advanced reactor plant space, how are you looking at that? And this is where, when Deanna was talking about the level of integration

aspect, you know, the level of digital you're actually installing in your particular modification kind of leads you to a greater consideration of potential spurious operation assessment.

So, one of the things that we did with the guidance in order to take into account the differences in licensing basis, as in you have an operating plant with an established licensing basis; you have an advanced reactor design that oftentimes will not have an established licensing basis. So, we did decide in this particular area of the BTP -- and it's the only area as far as I understand -- that it is actually treated differently between operating plants and advanced reactors.

The basic gist of the bifurcation that we call it -- and you can call it a different word if you want to -- is that, really, for operating plants, we just want to ensure that the licensees ensure that whatever design and whatever modification they're making to their RPS/ESF systems, that they're not invalidating the already-established spurious operation assumptions that are in their licensing basis. That's the real directive we gave in terms of that particular area.

The other area for advanced reactors we

gave a bit more detail because there's a greater level of integration in software instantiation within advanced reactor designs that we've seen.

CHAIRMAN BROWN: My difficulty with that was I understood that you did some separation of powers here relative to prelicensees and other licensees, et cetera, et cetera, which I thought were, who cares? But you did it. I mean, I'm not saying that pejoratively. It just seemed to be irrelevant to the actual whole point of spurious operation.

The thing that was interesting, we made a significant comment relative to the definition of this stuff when we from Rev. 5 to Rev. 6. And one of your all's responses was very good, and that was the last two paragraphs of what's now Rev. 7, Section 1.8, where it talks, just lead in, where it said, "Failures of automated protection systems stemming from software can cause spurious actuations." You use "operations". That's fine.

Then, it goes and talks, in the second paragraph, it says, "The overall defense-in-depth strategy" -- and it's a paragraph about that big. It kind of gave a categorization of "What does it mean?" that's absent from this now. My suggestion would be to reconsider that, I think I said as a preamble to

the whole Section 5.2 before you get into separation of church and state, of licensees and when they were licensed, and whether it's '91 or whether it's "O Dark Thirty," or what have you. You all did a very good job of providing that overall discussion/thought process back in 2011. And so, that's a suggestion, to think about that. I'm not saying change any of the rest of it. It's just something to characterize what's the point.

The other one was in Section 3.7 of the Rev. 7 there was a set of words, if I can find them. That's Rev. 8. I need to find Rev. 7 here. You notice I've still got paper. It was, yes, Section 3.7, your all's response in cases in which a credible postulated spurious operation caused -- I've changed the word -- caused by a software CCF -- they talk about coping strategy. And that was another good generalized thought process that I thought part of the preamble to go along with the other two. Again, that's a suggestion. Obviously, our comments are comments personally. They are not Subcommittee comments. They're not even Committee comments until we write a letter, and we won't be until after your public comments, the public comment period, and we see how all this plays out.

MS. ZHANG: Thank you, Member Brown. I think this is one of the areas that goes back to what actually started all this, which is the CCF hazard. In this case, for a CCF hazard that can cause a spurious operation, we also want to follow the same strategies that would be disabling the safety function. And in that case, it would be eliminate, mitigate, or cope.

CHAIRMAN BROWN: That doesn't come out of this, either.

MR. MORTON: That's part of the greater comment we have about kind of tying the loose ends in terms of leading into the technical content, yes.

MS. ZHANG: Yes.

CHAIRMAN BROWN: Yes, it was just a bunch of stuff.

MR. MORTON: Yes.

CHAIRMAN BROWN: And I'm saying here's the definition of what we're talking about that we used to have in there, and then, go into your eliminate, mitigate, cope.

MR. MORTON: Cope, yes.

CHAIRMAN BROWN: And then, you go with the rest of the stuff in here. I think you have a prescription. Again, that's the suggestion. It's up

to you all, and we may disagree in another five months or six months, whatever it is.

MR. MORTON: Actually, I don't think we disagree at all. I think we agree with that comment. That's a general comment. We take that across the entirety of the document --

CHAIRMAN BROWN: Okay.

MR. MORTON: -- that that needs to be cleaned up in terms of how we're leading into the section described to the person who hasn't spent 10 months writing it --

CHAIRMAN BROWN: Right.

MR. MORTON: -- what we're trying to get you to do.

CHAIRMAN BROWN: Preambles are nice --

MR. MORTON: Yes.

CHAIRMAN BROWN: -- when you have a concise description of what you're trying to accomplish --

MR. MORTON: Yes.

CHAIRMAN BROWN: -- and the outline part of it.

MR. MORTON: Okay.

CHAIRMAN BROWN: Okay? All right, go ahead. You can go ahead. How many slides do we have

here, anyway, 24?

MR. MORTON: Just a few more. Just a couple more I think we have left.

CHAIRMAN BROWN: Twenty? Twenty-nine? Oh, we're way behind. We've only got 10 minutes.

MR. MORTON: Oh, just we have a few more, and the rest are background slides.

CHAIRMAN BROWN: Oh, okay.

MR. MORTON: Yes. So, lastly, in terms of key changes we've been --

CHAIRMAN BROWN: Famous last words.

MR. MORTON: I know.

(Laughter.)

We have kind of been talking the entire time in terms of restructuring the BTP 7-19. Like we said earlier, some of it was internal staff identification of deficiencies and how to document it was composed. And then, we did get a lot of feedback from industry in terms of, hey, the document can use some improvement in terms of its flow and structure.

So, what you've seen in Draft Rev. 8 is our attempt to sort of improve it. But, like Deanna said a little earlier, it's still a work-in-progress. It's not set in stone, the particular structure of the document. So, we welcome any feedback you have on

improvement. We've gotten some and we appreciate that.

CHAIRMAN BROWN: Yes, on this particular one, to me, the three points I took away from you all's revision was not so much SECY-18-0090, which just says the Commission gave us latitude to do stuff we think is smart. I don't necessarily call that guidance. I call that wisdom.

The incorporation of the graded approach and the RIS 2002-22, Supplement 1, because that was not in Rev. 7. And, God, there was another one. What was it? Well, that's the two I can remember right off the top of my head right now. Let's see, the graded approach, the RIS. Well, those were two of the big drivers, it seemed to me, to get this thing out, and then, trying to integrate the graded approach with the rest of the language that you had in the old, in the previous revision. And after that, it seems to me those were the big points.

Oh, the echelons, you missed those. They're still not in there. That got totally lost. If you don't go off and read 6303, nobody will ever know what you're talking about.

MR. MORTON: Yes.

CHAIRMAN BROWN: I went off and read 6303,

1994, which I think is the latest revision.

MR. MORTON: Yes.

CHAIRMAN BROWN: And it only had about three or four pages which listed about that much for each of the echelons. So, it wasn't particularly illuminating; whereas, the old versions of some of the information you had in the Rev. before was more illuminating on what in the world were the echelons in the first place and what did they mean. And that was another suggestion, would be to try to somehow provide some information as to what that means, so that somebody doesn't waste their time looking at the other thing and not getting any information out of it.

MR. MORTON: Yes, we would agree that we referenced defense-in-depth for the entire plan, that this whole process is to ensure you have adequate defense-in-depth.

CHAIRMAN BROWN: Yes.

MR. MORTON: But what we did not do is necessarily say what are the composite parts of defense-in-depth in the four lines of defense. So, we recognize that as --

CHAIRMAN BROWN: Again, that was another.

MR. MORTON: Yes.

CHAIRMAN BROWN: You took that out of the

beginning. To me, that was a valuable part of the old revision. At least I understood what you were talking about. So, anyway, that was the suggestion.

MR. MORTON: Okay.

CHAIRMAN BROWN: Is that all the slides? Or did you have anything more to say? I interrupted you.

MR. MORTON: No, this is pretty much -- I think we talked about restructuring a lot.

CHAIRMAN BROWN: Yes, we needed to know where you're going here, next steps.

MR. MORTON: Next steps. So, we're looking to target public comment periods starting very soon. We're still working with our friends in OGC to ensure we have MLO complete by December, so that we can initiate the public comment period in January. So that we can get through and complete that in February of next year.

CHAIRMAN BROWN: Thirty days?

MR. MORTON: Sixty days.

CHAIRMAN BROWN: Sixty days?

MR. MORTON: Yes. I should have put that on my slide. It is a 60-day public comment period.

One of the potential things that we offered to industry is that, if there was desire, that

we could have another public meeting with industry during the 60-day public comment period to sort of address -- they could provide direct concerns they may have with what they're seeing as the publicly-available draft version and have further conversation, get further feedback on what they see as potential areas for refinement, based upon the publicly-available version. So, that hasn't been necessarily specifically scheduled, but we did provide that to industry, if they thought that they wanted to support that or not.

CHAIRMAN BROWN: Because it ends on February 28th? It's the end of February or when is it going to be issued, actually issued?

MR. MORTON: Final issuance is, we're talking the third quarter or early third quarter of next year. So, maybe around July or so.

CHAIRMAN BROWN: No, no, no, no, issuing for public comment, when will you do --

MR. MORTON: Oh, we're looking to issue public comment sometime in December of this year.

CHAIRMAN BROWN: Oh, okay.

MR. MORTON: Yes.

CHAIRMAN BROWN: Okay.

MR. MORTON: Yes, hopefully, initiating a

public comment period ending in February of next year.

And since I jumped to it, we're looking for the final issuance date essentially early third quarter of next year. So, we're talking July.

CHAIRMAN BROWN: Okay.

MR. MORTON: The July timeframe is what we're looking at.

And then, we do anticipate two more ACRS meetings. One, another Subcommittee meeting, I believe we're targeting for April of next year, April 8th of next year. Thank you. That meeting will take place after the public comment period is completed. We will resolve public comments. So, we should be in plenty of time for that. And the full Subcommittee meeting will be, I believe, the following month in May of next year.

So, that's generally the next steps in the process.

MS. ZHANG: One thing we would like to add is part of our brainstorming during break is a lot of the restructuring that we think would be a good idea, based on the feedback we received here, we probably will not be able to get that done before we issue it for public comments. So, that is one thing we will probably have to note in the FRN, that this is

something we intend to do, that we would welcome public feedback as far as how we should proceed with that. And then, once we get into a good place where we are, if we do have that public comment period, a public meeting during that public comment period, then we will present it.

So, we would like to improve upon what we have right now in terms of the structure, the clarity, and some of the preamble language/introductions, but, most likely, that won't be the case until sometime as part of the public comment period resolution.

MR. MORTON: So, effectively, it will be editing the document to take into account your input in terms of the structural concerns during the public comment period, as long as we notify the public in the FRN that this is one of our goals, is to provide some additional restructuring to improve the document.

CHAIRMAN BROWN: How will industry, then, have an idea of what they're looking at? Restructuring doesn't really change the content per se --

MR. MORTON: Correct.

CHAIRMAN BROWN: -- or the focus, other than maybe a couple of them, based on some of the discussions, if you decide to change your mind on

something, I don't think.

MR. MORTON: Yes, but the intent would not be to change the technical content, with the potential of maybe refining the figure so that it doesn't appear -- because I think we heard some comments on the figure made up here to be a little more sequential than it was intended to be. So, other than that, we would not be changing any technical content. This would strictly be reshuffling --

CHAIRMAN BROWN: So, you think industry will be able to give you the input that you need to try to, then, resolve their comments or meet with them, subject to getting --

MR. MORTON: Yes.

CHAIRMAN BROWN: Would you have any meeting with industry after you get the public comments in the process of resolution, or do you all just resolve those in absentia without talking to the --

MR. MORTON: Well, the point of --

CHAIRMAN BROWN: I have no idea what your process is. I forgot.

MR. MORTON: Oh, structurally, we're having a public comment period meeting, public meeting, to address some of those concerns. But we

will be resolving the public comments internally.

CHAIRMAN BROWN: But industry is part of the public comment?

MS. ZHANG: Yes.

MR. MORTON: Yes. Oh, yes. Oh, yes.

MS. ZHANG: So, part of the concern to have it as part of the public comment period is, one, facilitate our resolution of the public comments, as well as give the public a chance to interact with the staff as far as any clarifications that we needed, kind of like what we're doing right now.

MR. MORTON: Yes, but, essentially, it's consistent with what we've been doing all year, which is, when we've made a major structural change like the ones you're seeing today, that was actually presented to industry, I believe, in September.

MS. ZHANG: August.

MR. MORTON: August.

MS. ZHANG: The 29th.

MR. MORTON: August 29th of this year. So, industry had seen this new structure. It's just the ACRS hadn't seen it yet. So, we've been doing this the entire year so far. In terms of major structural changes or updates, we present them in the public forum to industry to see what their feedback

will be on it. And it will be the same case with this potential public meeting during the public comment period.

CHAIRMAN BROWN: Would it be useful to get a copy of the transcript, so you can look at our -- I mean, between Dennis, myself, and Jose, and Myron in a couple of cases, we have identified a couple of concerns. I did not write all of those down as we went because I was too busy trying to listen, an unknown thing for me to do usually, but I tried.

(Laughter.)

You're chuckling, Dennis.

So, how long does it take us to get a transcript? Three or four weeks? Two or three weeks? Okay, we ought to give them a copy.

MR. MORTON: Yes, that would be very helpful. That would be great, yes.

CHAIRMAN BROWN: Try to get them that unofficial version, and then, get the official version out after that. And then, send a copy of the transcript subsequent, you know, along with all the other feedback we get today.

MR. MORTON: Yes, that's great.

CHAIRMAN BROWN: Because I did not write down everybody's. I couldn't follow all of it and

integrate it, and then, think at the same time.

MR. MORTON: Okay.

CHAIRMAN BROWN: And I wasn't trying to chew gum at the same time, either.

(Laughter.)

I guess you all are done with this slide, is that correct?

MR. MORTON: That's correct, and that generally concludes the presentation.

CHAIRMAN BROWN: It's amazing, we actually finished right on the schedule. Actually, we're a minute early --

MR. MORTON: A minute early.

CHAIRMAN BROWN: -- 2:29. You are to be congratulated.

We are going to take a 15-minute break now, according to the agenda. And we will reconvene at 2:45. I think that's what it says. Yes.

So, we are recessed until 2:45.

(Whereupon, the foregoing matter went off the record at 2:29 p.m. and went back on the record at 2:51 p.m.)

CHAIRMAN BROWN: All right, the meeting will come back to order.

And we have NEI who is now going to make

their presentations. Who's in charge? Is that Stephen?

MR. VAUGHN: I'll lead us off, yes.

CHAIRMAN BROWN: Okay. All right. I just want to make sure I ask the right guy who wants to lead off, and we're ready to go. Okay?

MR. VAUGHN: All right. I'm Steve Vaughn with the Nuclear Energy Institute. And real quick, I'd like to introduce the gentlemen up here to my right. You've got Warren Odess-Gillett from Westinghouse, Neil Archambo from Duke Energy, and Ray Herb from Southern Nuclear.

On behalf of NEI and its members, I would like to appreciate the opportunity to discuss our perspectives on common-cause failure in digital systems with the ACRS.

And even before I get started, I would like to commend the staff over the last 10 months. The effort we've put forward in the four public meetings discussing this technical topic, I think it's fair to say that the dialog has been great, great technical exchange, and we're not done yet, but I think we're on a pretty good track. And we look forward to wrapping this up here in early 2020, maybe towards the end of 2020.

So, this presentation, before I get started, we're not going to go through and sort of rehash the comments we had on Branch Technical Position 7-19. We've been providing comments for the past 10 months. So, we figured we'd take a step back and provide more of a high-level look. So, the next slide I'll get into is sort of the background and context to lay the framework or reframe the problem, so to speak. And then, the next two slides we'll provide the solution at a high level of where we see the path forward will be.

Before I get started, any questions?

MEMBER BLEY: Yes. In the past, we had had a number of presentations from the folks out at EPRI. Are they still involved? Are you coordinating with them at all?

MR. VAUGHN: We do work a lot with EPRI, and EPRI will be speaking after NEI.

MEMBER BLEY: Okay.

MR. VAUGHN: Matt Gibson from EPRI is here to talk about some of the technical research they've been doing over the past, gosh, three-plus years.

MEMBER BLEY: Yes, actually more than that.

MR. VAUGHN: Yes, many years. But we do

work with EPRI.

All right. So, the concept of the common-cause failure -- and this was discussed earlier -- isn't unique to digital systems. I think it was Chairman Brown who mentioned that analog systems have been susceptible to common-cause failure for forever, right? So, it's not a new thing. But what has posed a challenge is that software does introduce a new perspective that we definitely need to deal with.

In that vein, we did some early benchmarking at current fleets that do have an analog RPS/ESFAS and have modeled that in their PRA. And there are some PRAs out there that are pretty detailed.

Just to get a sense of what CCF was, a ballpark picture, and it was what we would expect. You know, 1E minus 4 would be the dominant basic event for a common-cause failure. And they went all the way down to 1E minus 6, 1E minus 7.

MEMBER MARCH-LEUBA: That's for analogs?

MR. VAUGHN: Yes, for analog. And the reason we did that is because we agreed that what we're shooting for here isn't a zero defect. It is the current analog fleet, is what we need to meet, right? And that really ties back to the first bullet

here. It is the termination of reasonable assurance shouldn't be -- analog and digital should be on the same playing field. So, in a sense, we're sort of reframing the problem to an extent, and that ties into the next bullet here and some of the challenges.

MEMBER MARCH-LEUBA: Sorry to interrupt, but it's our job to interrupt you.

(Laughter.)

MR. VAUGHN: Yes.

MEMBER MARCH-LEUBA: But isn't it absolutely a problem that software failures tend to be more catastrophic or difficult to predict? You don't know in what stage you're going to end up; whereas, in an analog system, when it fails, everything goes to the ground.

MR. VAUGHN: Yes, good point. Software does present that unique challenge. And you'll see in our solution we'll provide at a high level; EPRI will get into more details. But the solution will be a robust software quality development process, both at the platform and integration and application level, as opposed to trying to prove that you will have zero defects in software, which in discussion with the NRC I kind of went down that path. I forget exactly where, but just it's you can't prove that you're going

to have zero defects or latent defects. What you can do is go through a robust process to ensure that you meet that reasonable assurance. And we'll get into it later, but it's appropriately addressing CCF as opposed to eliminating it.

CHAIRMAN BROWN: What were the numbers you quoted? You said 1E to the -- the susceptibility to CCF, whatever you all's analysis did, it was like 1 times 10 to the minus 4th to 1 times 10 to the minus 6th? I've heard two different numbers.

MR. VAUGHN: In some of the models we looked at, there were maybe 70 to 80 basic events, CCF basic events. And some of the dominant ones, you know, the 1E minus 4, once you have one of those, that pretty much dominates the overall outcome. But they went all the way down to 1E minus 8. But this model was fairly sophisticated, in that just the CCF events alone, there were about 80 of them.

CHAIRMAN BROWN: So, these were PRA --

MR. VAUGHN: Yes.

CHAIRMAN BROWN: -- models?

MR. VAUGHN: Yes. Current PRA.

MR. HECHT: Can I ask, is that per year or is that per plant life?

MR. VAUGHN: It's a basic event like any

other basic event in a PRA, whether it's a valve or a pump. A CCF basic event for, you know, two or three pumps --

MR. HECHT: Okay, but my question is, is that 10 to the minus 4th per year or 10 to the minus 4th --

MR. VAUGHN: Per year. Oh, per year.

MR. HECHT: Per year? So, that means that, roughly, you know, with 100 plants operating, we would expect one of those failures about once a century or so, the expected volume?

MR. VAUGHN: Well, in PRAs, CCF failure events for pumps and valves are similar magnitude, and there aren't a lot of common-cause failure events. The data pool is fairly small.

MR. HECHT: Yes, but I'm surprised that the numbers are that high.

MEMBER MARCH-LEUBA: Since we're confessing about that, I have had --

CHAIRMAN BROWN: This is analog systems.

MEMBER MARCH-LEUBA: -- an analog system common-cause failure myself, and it was we were destroying nuclear weapons and monitoring the destruction of nuclear weapons, and my whole system went down. And it was electrolytic capacitors on

every single component which were independent had dried out. And when we turned the power off and on, all of them died at the same time. So, it happens. It happened to me.

CHAIRMAN BROWN: I would counter that, in 35 years of running of the I&C division for the Naval -- well, 22 for running it and 35 in it -- I had one common-cause failure which was a relay that they processed the laminations, cooled them, quenched them in oil, didn't bother to clean them. And when they put them in service, the oil oozed out on the top of the laminate; the armature came down. It took a while, but they would stick. And we had one occur.

We went off and said, why the heck did that occur? It took us a year and a half to find that. They had subcontracted their manufacturing of these relays. GE had an operation that they had down in Puerto Rico. their QC got lost somewhere along the line. But it took us a while to track it down to that. And we actually fixed it by cleaning the surfaces every six months or a year until the oozing quit. And we know what the population of the relays and where they had fundamentally gone into by the way we track stuff.

But, I mean, I can't count -- I've had

individual failures, but that's the only one I could literally track to say, hey, I had it happen. Once we saw it once, it happened again on another system. So, that was in an analog system.

I'm not saying no to anything else. I'm just saying we had a higher level of quality on the parts, tons of inspections. The samples were greater, much more control over the population of what we had. It's far different than what you have in this particular world.

MEMBER REMPE: Let's get a little more precise. What you had was a failure probability. The frequency was determined because you turned the power on, right?

MEMBER MARCH-LEUBA: It was a common cause which was cycle power.

MEMBER REMPE: But it was a probability. And so, when you ask what's the frequency per year, isn't it a probability? You don't have an initiating event as much --

MEMBER DIMITRIJEVIC: This could be on demand. It's dependent on what signal they noted. It could be on demand. It's a monitoring signal that could be time-dependent. And even demand could be standby time failure which can fail between tests.

So, I don't know what -- I mean, because they obviously broke it on all kinds of different components which contribute to the signal. That's why you have so many common cause. It could down to relays. It could be down to the electrolytic capacitors, or whatever. And it's dependent on what signal they monitor. Most likely, it's further back.

MEMBER REMPE: That's what I'm catching.

MEMBER DIMITRIJEVIC: Yes.

MEMBER REMPE: So, when you said it was 10 to the minus 4, was that really per year or was that a probability based on something else going on?

MR. ODESS-GILLETT: This is Warren Odess-Gillett from Westinghouse/NEI.

Often, it's referred to as probability of failure on demand as well. Sometimes they use the two interchangeably.

MEMBER DIMITRIJEVIC: But that failure on demand may happen because --

MEMBER MARCH-LEUBA: Microphone.

MEMBER DIMITRIJEVIC: Yes, I don't want to.

(Laughter.)

MEMBER REMPE: It has to be on the record.

(Laughter.)

MEMBER DIMITRIJEVIC: So, that failure on demand could be time-dependent because it either failed because he introduced shock, like with this electricity that's different or it could fail because something happened like that oil leak during the standby, which is time-dependent. And then, it's depending on the test interval, how often you have a chance to discover that standby failure. So, it could be both. Demand failure could be time-dependent and could be further back.

CHAIRMAN BROWN: I didn't want to interrupt you, Vesna. Are you okay now?

We have to hold for a minute. We have to dial back in. Apparently, we lost our phone connection. Is this our public phone connection? Okay.

(Pause to reconnect to the public phone line.)

Let's go ahead and, then, I'll check in five minutes or so to see if people dialed back in.

MR. HECHT: Can I ask a question about the common-cause failure concept? There are actually, within software, there are what I would consider to be two kinds of failure. Actually, there are many kinds. But there's one kind of failure where they are random,

and that is that an operating system might hang or it might crash just because of a unique set of events that happens on a particular channel. And they're timing-related, and there are enough variances, variations between channels, as Charlie had mentioned, that they're really not correlated, all running the same code, but just because of the particular sequence of how the dispatcher chose to activate or deactivate certain tasks or allocate memory, something happened.

And then, there's another kind at the application level. There just might be requirements or a design or a coding error that caused a particular application to crash across or to do something you didn't expect across multiple channels because of that common design or requirements or coding defect.

Do you distinguish between those, and how would you do that?

MR. ARCHAMBO: I think we're going to hit on that as we go through this presentation. If you're talking about platform software versus application software, and the different things we do about that, we're going to discuss that a little bit in a slide or two. Is that okay for now?

MR. VAUGHN: And I think the last two questions have been a good segue into this second

bullet here. One of the challenges we have seen is just taking the word "common-cause failure," which has a well-defined structure in PRAs and PRA development, and bringing it into a digital I&C with a more deterministic perspective, if there's a communication challenge there, exactly what do we mean? Because when you mean common-cause failure from a PRA analyst, they have a certain set of rules they follow. And in a digital I&C context, there's a great question about how do you partition it, whether it's application or the platform level. That's a great question. Maybe we need to rethink about, do we need to clarify what we mean in this context?

And then, the third bullet here about -- this is really trying to change the problem a little bit or the framework, where the focus has been on eliminating the consideration of CCF. And just the concept of eliminating CCF and taking something to zero is just a minimal model that is difficult to prove, where I can say what we should be focusing on is how do we appropriately address common-cause failure, right? It's not eliminating it. It's appropriately addressing it with the tieback to the first bullet; the reasonable assurance determination, analog and digital should be on the same playing

field. So, we're trying to move the focus from eliminating to appropriately addressing common-cause failure.

MEMBER MARCH-LEUBA: By that, you mean mitigate or convince yourself that it's not a problem?

MR. VAUGHN: Yes, so appropriately address could be, obviously, through design, manual operator actions like diversity as being one case, and then, coping. So, it's all different levels. In our presentation, we didn't get into all those. I know the NRC's presentation did. But it involves all those and taken collectively in the aggregate, as opposed to one or the other.

MEMBER BLEY: It sounds like you're agreeing with the staff and the approach they're taking, is that correct?

MR. VAUGHN: So, what we do agree with is that, going back to 100 percent testing and diversity being the only two ways to eliminate CCF, we didn't agree with because it was unattainable. All right. We don't need to rehash the discussion, but the whole 100 percent testing, that was designed for simple things that you could 100 percent test; whereas, if someone comes in with an RPS/ESFAS, a complex system where you have software, you can't test it. Well,

that ability in the BTP, you just couldn't do it. So, what's the next step? It was just diversity.

But now there's this third option. They mentioned defensive measures and they said NRC-endorsed guidance, and that's what you see on our next two slides, at a high level, what our path forward is going to be. That's going to tie that link.

And again, there was also discussion about is it one or the other. We like to think that you can do all three, not 100 percent testing, but sufficient testing, or we had extensive testing. But you do all three and you take those collectively. And if you do that, and you do that right, our argument is that you will appropriately address CCF and meet their reasonable assurance determination.

CHAIRMAN BROWN: Just to make sure I understand, NEI's focus -- I want to understand your line here -- is you're moving from the consideration of eliminating CCF, as opposed to appropriately addressing? You're going to eliminate by defensive measures? Is that the point you were trying to make?

MR. VAUGHN: Actually, the point I'm trying to make is a little bit philosophical. So, there's a subject to interpretation here. But the idea of -- you mentioned earlier about what is a

latent software defect.

CHAIRMAN BROWN: Uh-hum.

MR. VAUGHN: You can't design complex software with -- it can't be error-free. And so, the argument to eliminate, design a software system where you have zero latent defects is unattainable. So, if you can't do that, what can you do? Well, obviously, you can test quality, the software design. There are a lot of things you can do. And in the aggregate, our argument is we'll appropriately address CCF and meet that reasonable assurance determination. So, it's more of a mental framework. We're not trying to prove the negative--you can never have software defects.

CHAIRMAN BROWN: Well, a latent defect is kind of -- how do you eliminate something, an unknown that you don't know about? And that was in the BTP --

MEMBER BLEY: Nobody here today has been arguing that. So, are you disagreeing with the approach laid out by the staff in their Branch Technical Position or are you supporting that, or are you suggesting a completely different alternative? Or are you going to even comment on the staff's approach?

MR. VAUGHN: We have commented on the staff's approach. And part of that, the feedback they did incorporate was that third path, the use of

defensive measures. So, again, I mentioned this is more philosophical. Before, it was "eliminate". Now, it's "eliminate the further consideration of". Before, it was "eliminate the consideration of". The concept of just eliminating to us was the wrong mental model.

MEMBER BLEY: Yes, I would agree with you.

MR. VAUGHN: You never say you want to eliminate it. You say, hey, we need to appropriately address this. It's not zero, right? Our threshold here is reasonable assurance, and it's what the current analog CCF is. We're trying to change what the target is, the target for success.

MEMBER BLEY: Go ahead.

MR. VAUGHN: Okay.

MEMBER BLEY: I haven't heard anybody argue with that position all day.

MR. VAUGHN: And one other thing I'd like to mention, that the whole software and hardware reliability, the focus has been mostly on software, and we understand why. But the hardware piece, the system needs to be looked at as a system, from a system engineering approach. So, hardware obviously is part of it. And we'll get into later with ours at a high level; EPRI with probably more detail. But you

need to take that system engineering holistic approach to the system, and software is one of the more challenging pieces. I just wanted to make that distinction.

And I'm hearing the phone --

MEMBER BLEY: Yes, try to keep going. Ignore it if you can.

MR. VAUGHN: Okay. We lost connection? Continue or?

CHAIRMAN BROWN: Sorry, gentlemen, our high-quality, microprocessor-driven, electronic system is getting confused from a common-cause failure.

(Laughter.)

(Pause to reconnect to the public phone line.)

Is there someone on the line?

MEMBER MARCH-LEUBA: They need to call in.

CHAIRMAN BROWN: It said there's two people including us.

If there's somebody on the line, can they hear me?

MEMBER BLEY: They're probably silenced.

(Someone on the phone line speaks.)

CHAIRMAN BROWN: Thank you. Please mute now. We appreciate that.

MR. VAUGHN: All right. So, that's the background and context, sort of framed the challenge that we been dealing with for several years and are continuing to deal with.

And now, I would like to turn it over at a high level to provide what our path forward is from a solution perspective. And I'm going to turn it over to Neil Archambo from Duke Energy to lead that discussion.

MR. ARCHAMBO: Okay. In the industry, of course, up to this point, we've been dealing with common-cause failure in kind of a hybrid, confusing approach. We know we have to deal with common-cause failure. We know that the probability of common-cause failure is not zero.

So, what we're doing here, what we're talking about here on these first principles, we want to take a step back and see what constitutes a CCF -- where does it come from? -- and understand that. Instead of throwing everything and the kitchen sink at a design, step back and see where do we need to focus our efforts to eliminate/mitigate common-cause failures in these digital systems, primarily software.

So, the first principle you see up there -- and software quality depends on complete correct

requirements, design, and implementation -- and what we found when we implemented digital systems, and we've had errors in those digital systems or events that were caused by those digital systems, is it could be usually traced back to an incomplete or incorrect requirement. There was an incorrect requirement. It was either missing or it was incorrect.

Now it doesn't matter how good your software is, if the requirements that you used to design that software are incorrect or missing, you're probably going to experience some problem. So, we realized that that's probably one of the first things we have to do, is work on our requirements development. And we'll talk a little bit about that in the next slide, the path forward on that, how we're addressing requirements development.

The second one is we realize that we need concurrent triggering to trigger a defect. If you have software and it has a defect, it has to be triggered somehow in order to cause you a problem, to cause you a failure. If you have a single-loop controller out there with a design defect in the software, and then, that defect gets triggered, you'll have a signal failure, but you won't have a common-cause failure. Now, if you have a couple of single-

loop controllers in the system and they experience the same concurrent trigger, then you'll have a common-cause failure. So, that's one of the guiding principles that we're talking about.

MEMBER REMPE: Would the people on the line please mute themselves? Thank you.

MR. ARCHAMBO: Okay. No problem.

And we've also recognized that the effects or likelihood of a software defect can be minimized by design, design attributes. It might be actually software design. It might be external system design attributes. So, we can apply design attributes to further reduce the likelihood of a common-cause failure or mitigate the effects of a common-cause failure.

And then, we recognize that operating history can also support software quality. By that, we mean a lot of these platforms that are out in the industry and have millions of hours of operation. And EPRI -- and I suspect Matt will talk about this in a little bit -- has some research on platforms that have been out there and have a tremendous amount of operating experience with a lack of any type of software common-cause failures. So, we can capitalize on that operating history. The operating history may

also show you a system that you want to avoid. So, it works both ways.

The first principle, we first wanted to align, put our arms around the issue, and figure out what we need in design space to tackle that issue.

MR. HECHT: Can I ask a question with respect to the operating history? Earlier this morning, we heard about yet another RES attempt to do some quantitative estimation of software failure probabilities. And I know that the past studies have been hindered primarily by the lack of relevant operating experience, particularly from the nuclear industry. And I think that's been a problem within the NRC for a long time in attempting to address it. In another life, I was also part of those efforts.

What do you think is the probability that NEI or EPRI, or both, would be willing to share data that was pretty much at this point safeguarded and kept from the NRC in terms of helping to get that relevant operating history and those failure modes that would really enable a better attempt to address that?

MR. ARCHAMBO: Yes, if you're talking about platform software -- and I'll phone a friend, Matt, perhaps -- EPRI just completed a report recently

on SIL certification of platforms. And I believe the NRC has that report.

MR. HECHT: That's the report. That's not the underlying data.

MR. ARCHAMBO: Yes. No, I'd have to ask EPRI if they would be willing to share that underlying data. I'm sure there might be some proprietary information there. So, I'll leave that up to Matt. Maybe when he gets up here --

CHAIRMAN BROWN: We'll ask him.

MR. ARCHAMBO: -- he can address that question. I can't answer that one. I don't know if anybody up here on the panel can.

MR. HECHT: Just with respect to that last point, I mean, data can go a long way to addressing what are largely hypothetical concerns because we don't have enough --

MR. ARCHAMBO: Sure.

MR. HECHT: -- real experience.

MR. ARCHAMBO: Understood.

Any more questions on the first principles that we talked about?

CHAIRMAN BROWN: Yes, I had one question. Because I haven't seen this in probably 10 or 15 years now. When the program I was in first started doing

our computer-based systems in 1979, one of the problems we ran into was a complete lack of software standards. Programming standards just did not exist; quality standards did not exist. And you ended up with a large amount of what I call "spaghetti code". Stuff was carefully intertwined. Programmers love to be fancy, and they all thought they were smarter than everybody else.

So, we initially had to develop our own set of software programming standards that we utilized. But, over the years, there's been a great deal of emphasis, at least from what I've read in the IEEE magazines and stuff like that, on developing commercial software standards. I mean, I guess Carnegie-Mellon had some or somebody. I've forgotten the names of all the participants.

Is there a good track of really high-quality software standards, like you comment your code extensively, so you can track line by line what you're putting in and what it's supposed to be doing, as opposed to what you thought it was doing, but you forgot because you didn't tell yourself? I have no connection with that now. It's just been so long.

MR. ARCHAMBO: Yes, there is actually. And we've been looking at the IEC standards, primarily

the 61508 and the 61511, I believe. IEC 61508, Part 3, has a pretty significant guidance on coding standards, exactly what you're talking about. It goes down to the detail of commenting, how much white space, how many lines per module of software code. For instance, they want to keep the lines per module of software below 100 lines of code; one single input, one exit to a routine, things like that. So, today there is good standards out there to develop software.

We're looking at those standards in our industry to apply those to, more or less, the application software that we mostly deal with. But those standards do exist now. Other industries are using those standards.

CHAIRMAN BROWN: I guess the operating system coding is pretty tough to get your hands on from --

MR. ARCHAMBO: It is.

CHAIRMAN BROWN: -- the various guys that build the platforms.

MR. ARCHAMBO: Right. Now what we have to rely on the platforms, for instance, the platform software, is, one, it's either been pre-approved by the NRC -- that means the NRC looked at it and pre-approved it. And what we're trying to go for, also,

we'll work with the NRC on, and I think we're getting there, is the SIL certification, the Safety Integrity Level certification. If you're not familiar with that, there's four levels of SIL certification.

And the SIL certification is usually based on the IEC standards. So, for instance, a protection system may be a SIL 3-certified system, would demonstrate the quality needed for a system of that safety significance. So, those are the kind of things we're looking at right now bringing into the industry, so we can demonstrate software quality at the platform level.

Because at the plants, clearly, we don't have access to the code. We don't have that. We probably wouldn't know what we were looking at. What we need to focus more on at the plants is if we have good application software. We have to develop -- I mean platform software -- we have to develop application software, and that's where we want to really focus our efforts on, because that's where we find in the research, in EPRI's research and operational experience, that's where our failures come in. It's development of the application software. The platform software works fine. It's the application software.

And again, a lot of that goes back to the requirements, an incomplete or missing requirement that led to that application software defect. The software usually does exactly what you tell it to. Sometimes you didn't intend to tell it to do something, and it will do it perfectly in most cases.

MR. HECHT: In response to your question, Charlie, there is a standard called MISRA, which was developed by the Motor Industry Reliability Association of the United Kingdom. It's called MISRA C, and there's one MISRA C++, which are widely accepted now in multiple industries.

With respect to operating systems, the FAA has accepted for use giving licenses for an integrated system of real-time operating systems from several vendors, including Green Hills, Wind River, and several others. And they've made that source code available, and they've provided what are called certification packages, so that an avionics manufacturer can include that software data with their own application and submit it to the FAA for approval, including --

CHAIRMAN BROWN: The source code was open?

MR. HECHT: To the FAA.

CHAIRMAN BROWN: To the FAA?

MR. HECHT: Yes. Including the MCAS system and the 737 MAX, but, as was pointed out earlier, I think that was a requirements and an integration problem, as Joy pointed out.

CHAIRMAN BROWN: Okay. Thank you.

MR. ARCHAMBO: If there's no other questions on that slide, I'll go to the next slide.

All right. So, how do we apply these first principles? That's what this slide is all about. Again, our research and our experience tells us it goes back to requirements development. You have to do your homework upfront to get those requirements correct.

Now, up to this point, when we developed requirements, it was a lot of times a lot of people sitting in a room coming up with things they thought would be good for the system. And there was other sources where we got requirements from. We never had a real systematic process for developing your requirements. Well, that's changed. That's changed. The nuclear industry has implemented the Digital Engineering Guide from EPRI, and the Digital Engineering Guide is really heavy on requirements development.

And what we're using is a process that was

developed by MIT. It's called the Systems Theoretical Process Approach, or STPA. And it's a system that walks us through how to develop requirements. It's not a haphazard approach.

We've had some industry workshops and it is very effective. In fact, some of the issues that we had where we missed requirements in designs, we worked through those with a blind class of people that had no idea what the problem was with that design. And we were able to flesh out that requirement that was missing prior to the design. So, it looks like it will prove very effective in developing our requirements.

So, we're applying that into our designs now to get our requirements. Because, again, even if you have the best software, the best software on the market, if you have a missing or incomplete requirement, you're going to have problems, and we recognize that.

MEMBER BLEY: Can you give us a quick tutorial, a couple of bullet items, on what kind of application software the plants are developing separate from the big system software that they're installing?

MR. ARCHAMBO: Sure. If you take a

turbine control system, for instance, you'll choose a platform for your turbine control systems, but, then, you have to apply it, of course, to your particular system.

One that's kind of near and dear to my heart is recent. We developed the requirements for that application software, and a lot of times that's logic that we're building for that particular, you know, to integrate that platform into our system. But we like to put in a lot of redundancy, as you would expect, into these systems, minimize the single points of vulnerability. A lot of times we do that by having three sensors feed a median select device that, then, feeds that signal into our system, right? And that way, if one of those sensors fails, you still have two others. And instead of median select, it usually goes on to an average of those two signals.

A lot of times people put a requirement that says, if those all of those three signals go out of range for whatever reason, trip the system; sometimes wrong. We don't trust our sensors, so trip the system. And a lot of times that's a good requirement, but not always.

MEMBER BLEY: It's not.

MR. ARCHAMBO: Not always. And in a case

I can give you an example of, there was cooling flow to a turbine, and we don't care if there's high flow, right? High flow is removing the heat. That's good. We're concerned about low flow. But the requirement said, if these sensors go out of range, trip the turbine.

Now we have two pumps that feed the system, the cooling to the system, and only one pump usually runs. And then, you like to cycle the pumps. But you start off the other, the second, the redundant pump, before you close down the first pump, of course, when you're changing the pumps. Well, as soon as you kick down the first pump, what happened? The flow over-ranged on all three sensors.

MEMBER BLEY: So, you have a trip.

MR. ARCHAMBO: You have a trip. The system did exactly what it was told to do, but the requirement was the problem.

MEMBER BLEY: So, I understand you write those requirements for this new control system you're getting. But, then, does the vendor of the control system do the coding or do you do that?

MR. ARCHAMBO: Generally speaking, yes.

MEMBER BLEY: Okay. But you feed them the --

MR. ARCHAMBO: We feed them the information.

MEMBER BLEY: -- plant requirements?

MR. ARCHAMBO: That's right.

MEMBER BLEY: Yes.

MR. ARCHAMBO: Now, generally, the design engineer at the plant is not going to be developing if it's complex application software. We will have a vendor do that. We'll work with them, of course, so we'll understand and --

MEMBER BLEY: So, when you submit the LAR, that's for the system with your requirements already met?

MR. ARCHAMBO: Yes, but, you know, it's not always with the LAR. With the turbine controls, that's not an LAR.

MEMBER BLEY: Understand that, yes.

MR. ARCHAMBO: But that's just the design process.

So, design requirements for development, of course, is a big-ticket item. We recognize that. We haven't done a good job of it in the past. And now, we have tools that should put us on the right path with requirements development.

We also recognize there's design

attributes. We know that, even with the best requirements development, with the best coders out there, with the best application software, we can never say that it's defect-free, 100 percent defect-free. We know that. We recognize that.

But we can apply some design attributes to either further minimize the likelihood of a common-cause failure or mitigate the effects of a common-cause failure. For example, if we have diagnostics to look at the system alarming, perhaps we can fix an issue before it becomes a common-cause failure. A lot of the digital systems, when they fail, we can determine what state it goes to. We can put it in a failsafe state. So, there's a host of design attributes that we can apply to the system on top of the quality of the software to help minimize and mitigate the effects of a software CCF. So, we do apply those now, but we'll continue to refine those and apply those in our systems.

Now the quality of the software design process, again, that goes back to your question. When it comes to the platforms, we have to rely on a couple of things. We have to rely on, hey, was this platform either pre-approved by the NRC or was it certified by another body perhaps? Was it developed by an Appendix

B supplier for use in a safety-related application? Those are things we have to look at to meet the quality requirements for software at the platform level.

Now, if you get down to the application software level, that's where you're not going to have those things. You're not going to have, chances are, pre-approved application software. You're not going to have a SIL certification on application software. So, that's where we feel we need to spend most of our time, on the application software development. That's our intent.

And then, as the slide says, division of responsibilities. Another thing that we recognize, that if you have complex systems, it's easy to drop things without a clear division of responsibilities. And that goes back to your requirements and your requirements traceability, who's responsible for seeing those things all the way through. And these are the areas that we found that, through root-cause analysis and analysis of issues, we've discovered were the primary cause of issues -- lack of requirements, lack of division of responsibilities, things of that nature.

So, that's at a high level of how we want

to attack the software common-cause failure issue. We know we can never get to 100 percent assurance that we're not going to have it. That's not the idea. It's to get to reasonable assurance that we've protected against software common-cause failure.

MR. HECHT: Can I ask a question about your definition of platform software?

MR. ARCHAMBO: Sure.

MR. HECHT: Is that simply the operating system or would that be, for example, a ladder logic interpreter or an IEC -- what is it? -- 1163-type language processor that would be on top of that? That would be used, for example, in PLC programming or something like that.

MR. ARCHAMBO: Yes, that would be included in the platform software. Take a PLC, for instance, an Allen-Bradley PLC. When I'm talking about application, it's simply the ladder logic. That's what we would develop, the ladder logic. Whatever comes in that box beforehand, the operating system, any other systems, that would be included in the platform software.

Does that answer your question? It doesn't look like it.

MR. HECHT: Yes, well, I know that in the

aerospace industry, of course, ladder logic is not used. I would imagine that in the IEC 61508 world it might be. But have there been SIL 3 ladder logic interpreters accepted or is that only the operating systems?

MR. ARCHAMBO: My guess is there has. And Matt's shaking his head, that that is the case, that they have.

Now, when you go to 61508, when you talk about platform software and things like that, you talk about full variability languages. And when we talk about application software, we're talking limited variability language, as I see it. That's the definitions you'll find in those standards.

So, yes, if that answers your question.

MEMBER MARCH-LEUBA: When I'm here thinking about what you're saying, I tend to oversimplify things. People get upset about it. What I hear you say is we're going to get real diversity and we're going to continue to do the same thing we've been doing for design, only this time we promise to do it right. That's what I hear.

MR. ARCHAMBO: Yes, well, you know, I like it. You brought it down to my eighth grade level. I appreciate that.

And the answer is yes. You know, diversity is a double-edged sword. There's evidence to suggest that having a diverse actuation system may -- may -- actually be detrimental to your core design or core damage frequency.

The solution to putting a DAS every time you have a digital system we don't feel is the correct way to go. There's applications for that. But what we don't want to say is anytime you have a digital system and a safety system, you have to have a backup, either digital or analog system. It creates complexity, and there's no real evidence that it adds actually any security.

MEMBER MARCH-LEUBA: It all depends on what that CCF frequency is. If it's 10 to the minus 8, of course, I think the system is high on complexity and it's not good. If it's 10 to the minus 2, that system helps you.

MR. ARCHAMBO: Sure.

MEMBER MARCH-LEUBA: When I'm driving a car, I like to have brakes in the front and brakes in the back just in case.

MR. ARCHAMBO: But, you know, in the newer cars all the brakes are electronic.

MEMBER MARCH-LEUBA: Oh, yes. Don't get

me going with --

MR. ARCHAMBO: And your shifter is electronic. There's no linkage anymore on that shifter. It's electronic.

MEMBER MARCH-LEUBA: When you're pushing the brake, you're just informing the computer that you would like to slow down.

MR. ARCHAMBO: Exactly. Exactly. There's no backup mechanical brake system unless your emergency brake is part of that system.

MR. HECHT: I don't think that's totally true. I think that there are hydraulic lines that work in addition to the automatic braking systems.

MEMBER BALLINGER: Not in my car.

(Laughter.)

CHAIRMAN BROWN: I can guarantee you there are hydraulic braking systems in my cars because they're so old.

(Laughter.)

MEMBER BALLINGER: If it's 1945, of course.

CHAIRMAN BROWN: No, it's hydraulic. It's 15 years old.

MEMBER BLEY: We're diverting wildly.

MEMBER MARCH-LEUBA: So, in your

experience, this diversity of the application software, having to have two independently-developed applications running, two channels one and two channels the other, is that expensive; is that difficult; is that prohibited?

MR. ARCHAMBO: You mean to have different, say, manufacturers, different vendors?

MEMBER MARCH-LEUBA: Yes. You say that application software is where all the problems happen.

MR. ARCHAMBO: Right.

MEMBER MARCH-LEUBA: Because the others you can really test better. Is it that difficult to have two different lines of code that -- I mean, it doesn't need to be one is Russian and the other one is Japanese. I mean, it doesn't have to be that bad.

MR. ARCHAMBO: Yes, the short answer is yes. But, to get back to the point of the requirements development, you're going to develop a set of requirements. And if you have two separate systems, let's say two separate design teams developing the application software for two separate trains, they're going to use the same requirements. If the requirements are incorrect --

MEMBER MARCH-LEUBA: Oh, no, you will have to develop requirements independently. Because the

biggest problem is going to be you're going to forget a requirement. That's the likeliest --

CHAIRMAN BROWN: That's why you write them down.

(Laughter.)

MR. ARCHAMBO: But what happens with that, you know, there's a lot of issues associated with that, not just the expense of building it, but the expense of maintaining it also. That's where the pain comes in. And then, you have to ask yourself, is it really necessary?

Now our evidence would suggest it's not. We have not seen a significant amount of common-cause failures. We've had digital systems in our plants for many years, operating out there as we speak. We have never experienced a common-cause failure. I'm not going to say it could never happen, but, so far, it's been significantly unlikely.

MEMBER MARCH-LEUBA: I find that hard to believe because I told you already I had that one analog common-cause failure. This piece of equipment crashes; the system you're running crashes two or three times a day.

MR. ARCHAMBO: Yes, you look at that system, though, and that's a system where they're

beaming down updates to you periodically and things like that.

MEMBER MARCH-LEUBA: Yes.

MR. ARCHAMBO: That's not what we're talking about.

MEMBER MARCH-LEUBA: What I was going to say is that, even though it crashes two or three times a day, I can still use it and it still works and it's useful, I guess. So, it's not always the end of the world.

CHAIRMAN BROWN: Well, I hate to tell you, but my common cause -- I have no failures of this.

(Laughter.)

It works all the time. I make phone calls and I can text. It's only 18 years old and I can get new batteries for it. So, I continue to do that. And it never crashes. And I don't have to download software, and it makes phone calls. And I can hear the people on the other end. They're not going sporadically in and out, except if I'm talking to somebody that's got one of those pieces of garbage. I'm just having fun.

All right, go ahead.

MR. ARCHAMBO: Anything else?

CHAIRMAN BROWN: You've got another slide.

Did you want to talk to that, or is somebody else going to do that?

MR. VAUGHN: It's a wrap-up slide.

MR. ARCHAMBO: I think somebody else.

MR. HERB: I'd like to make a point.

CHAIRMAN BROWN: Go ahead.

MR. HERB: Okay. I think that the member, Mr. Bley -- "Bley," is that how you say your name?

MEMBER BLEY: Bley.

MR. HERB: Bley. Mr. Bley asked what was our problem with BTP 7-19, and I don't think anybody really addressed that.

MEMBER BLEY: I think you're right.

MR. HERB: First of all, we do like BTP 7-19, but what we like about it was the additional freedom we got to address a common-cause failure. Because I think, as you can see, we always get bogged down into software, the digitalness, and how that's such an unknown. Nobody can eliminate all the issues with software. But what we bypass is that, with the new digital systems, they're highly capable systems. We would like to install them. Those design attributes can be programmed into them.

And so, the thought that you have to restart your phone periodically during the day, but

that's a value proposition; that's a risk proposition. The chances of you having to restart your phone right before you have to call somebody, a 9-1-1, that's probably pretty low.

And so, it's the same thing here. We're not eliminating CCFs. We're just suggesting that sometimes you can live with them and you can cope with them. The system can make you aware that a failure is happening in enough time that you can take correct, proper manual actions without having to rely on a diverse actuation system in time to either put the plant in a safe condition before your design basis event that's been designed, that that system's been designed to address long before that happens.

And so, the probabilities start to get minuscule that that common-cause failure is going to happen at exactly the time that the demand is required. Because these systems are not like the old systems; they get tested on a quarterly basis or a semi-annual basis. And you have to like live with that possibility that they have failed. Between that last time you tested and the next time you tested, there may be a design basis event that happens in between.

These systems will let you know

immediately when they fail. You can address that immediately. And we just like to have credit for that, rather than to say, you know what, the default is a diverse backup system.

And so, in some cases we may have to have a diverse backup system, but we want the option to be able to take the full spectrum of response. And I think that we've always felt that BTP comes with a presumption that you will have a diverse backup system. And it doesn't really give full credit to those other aspects.

MEMBER BLEY: Do you feel that way now? The way I read the current version, you have --

MR. HERB: No, I think it's much better.

MEMBER BLEY: -- a way out.

MR. HERB: But we haven't seen it since August.

CHAIRMAN BROWN: Well, since they put in the defensive.

MEMBER BLEY: Oh, you haven't seen it? Okay.

MR. HERB: We've seen in general, yes.

MEMBER BLEY: Okay.

MR. HERB: We have seen it.

MEMBER BLEY: But you haven't actually got

a copy of the document we have?

MR. HERB: And again, we still can't look into the minds of the inspector to see what weight that they provide each of those.

MEMBER BLEY: You aren't ever going to get rid of that problem.

(Laughter.)

MR. HERB: We're never going to do that.

CHAIRMAN BROWN: You must have been listening to the conversation we had earlier in the meeting about why do we worry about CCF. You were echoing my comments.

MR. HERB: And I agree with you instead of --

CHAIRMAN BROWN: I figured as much.

MR. HERB: I think that the NRC agrees with --

CHAIRMAN BROWN: I didn't bring up the point the other time that all of the systems we've gotten in the design systems and even -- are you the Common Q guy? That's what I thought. I thought I remembered that discussion.

All of the systems that have been put in have been built with significant self-diagnostics, where they're continuously running. Every few minutes

they're probably running through some almost complete testing of all the responses, with inputs coming in and seeing that they generate the proper output each time. And if they don't, then they bring something in.

Personally, I believe that is a significant benefit that we have not had in any of the instrumentation control protection systems or anywhere else. We used to have weekly setpoint and calibration checks because we knew the analog stuff would drift, and it did.

MEMBER BLEY: And we'd trip things accidentally doing these tasks.

CHAIRMAN BROWN: Accidentally because of that. But, once we implemented -- I had terrible problems with intermediate-range and source-range nuclear instrumentation always going off the reservation. When we developed the microprocessor-based instrumentation for the intermediate-range and source-range, which we applied in probably two dozen submarines before I retired, you could count the number of incident reports on those systems on no hands. It just tested itself continuously. If we did have a problem, it was a detector problem, not a processing problem.

I'm not trying to counteract. I'm just saying the self-diagnostics are a huge, huge benefit relative to monitoring the safety, the health of the system. And I personally think that has been inadequately utilized in terms of getting through this thing.

I believe in some diversity. It's a matter of how and where it's applied, where you have to have it because your other defensive measures don't cover you in that area, and determining where those are.

So, I just love these two systems, in spite of the fact that I hate software and I hate microprocessors, but they work awfully well and help us out.

And these plants are really very simple compared to the stuff I had to deal with when you're talking about submarines and aircraft carriers. You all, your brains would explode if you had seen what we did with the capability of those systems. It is truly phenomenal in terms of operational capability, and safe because it tests every one of those features all the time.

Sometimes it might take 5 or 10 minutes to test every part because you're doing it at the end of

every sample period, which might be 50 to 100 milliseconds, but every sample time has an allocated time for self-test. And you run through and you just pick up where you left off and keep testing until you finish the whole package, and then, start over again.

And from what I gathered, at least the two that I've seen -- I think Common Q kind of does that also for the most part, and there's one other one that does that also. I can't remember which one it was that I looked at.

MEMBER BLEY: For systems that aren't working, that's great. For having things running operationally, it's great. For these things we worry about that are extremely rare, it helps, but it's not enough.

I'd like to direct a question to staff, if I can.

CHAIRMAN BROWN: They're gone, except for Eric. Oh, no, is Deanna here?

MEMBER BLEY: The discussion about requirements is interesting and meshes with things I've seen in the past. And the BTP doesn't really draw any separation between applicant-developed requirements and any of the other software involved. Do you do anything special to look at those

requirements? And can you even see them from the submittals? Do you see those requirements? Is there anything in the process that shines a light there more than on anything else? If you can comment on that, I'd appreciate it.

CHAIRMAN BROWN: You're talking to Deanna?

MS. ZHANG: So, in general, when we do a platform-level review of an I&C platform, we don't typically review to address CCF because a lot of times that's not addressed at the platform level, but addressed at the system architecture level, which would be application-specific.

So, when you look at the BTP, what we envision is mostly this is talking about the application, not the individual platforms we may see, such as the Common Q or TXS or Tricon type of platforms.

MEMBER BLEY: I'm sorry, don't leave.

MS. ZHANG: Unless Ross wants to talk a little bit more about some of the other platforms we've reviewed --

MEMBER BLEY: Okay. My question was really aimed at the requirements.

MS. ZHANG: Right.

MEMBER BLEY: But I appreciate the

separation between the generic platform acceptance and the specific applications coming in for a particular plant.

MS. ZHANG: Right.

MS. ALVARADO: This is Rossnyev Alvarado, I&C Branch.

BTP 7-14 includes guidance for the staff to review how the licensees or the applicants provide the requirements specification. And it's one of the IEEE standards that we have endorsed. So, it is required.

We don't look at like details like requirement by requirement, but we do spot-check and track requirements to figure out how they have been implemented. And we do that for both platform -- like when you were asking about whether it's the software that comes with the component, that's right. Well, operating system is no longer used, the term. Okay. And we do, too, for the application.

The difference is that, when it comes in the platform, it's usually the vendors -- in this case, Westinghouse, GE, you name it, Rolls Royce. When it comes with a license amendment, it is coming through the applicant or the licensee. So, a lot of the responsibility shifts to the licensee to do that

review, but we still do check.

And one of the requirements is that they need to meet the functional requirements specification. We do require that. So, we do look at it. It's just not that we're going to do line-by-line code check. We just need to look at it.

CHAIRMAN BROWN: There's no way you can do a line-by-line code check.

MS. ALVARADO: No.

MEMBER BLEY: No, there isn't, but you can do something with the requirements.

CHAIRMAN BROWN: Well, we used to do that.

MEMBER BLEY: We've got your statement on the record. That's good. If one of you can show me where in this document you refer to the requirements, I would appreciate it, because you said it's in there.

MS. ALVARADO: This is not the document to address requirements. This is a document on how --

MEMBER BLEY: You told me -- I'm sorry --

MS. ALVARADO: BTP 7-19 is a document to address --

MEMBER BLEY: I thought earlier -- and I'll check the record -- I thought you said BTP 7-19 included --

MS. ALVARADO: 7-14.

MEMBER BLEY: 7-14?

MS. ALVARADO: 7-14.

MEMBER BLEY: Thank you.

MS. ALVARADO: BTP 7-14 is the process to review, that we follow to review all of the software-related development process.

CHAIRMAN BROWN: Thank you.

MS. ALVARADO: Sure.

MEMBER MARCH-LEUBA: No, don't leave. Don't leave. Don't leave.

CHAIRMAN BROWN: Come back.

MEMBER MARCH-LEUBA: Well, it's not a question. It's more a statement.

I have a problem with the PRA all the time about completeness, and it's a great methodology. The problem is, how do you know you accounted for everything? And when you review the functional requirements, how do you account, how do you review that they accounted for everything that they needed to account for?

MS. ALVARADO: We don't.

MEMBER MARCH-LEUBA: Because it's very easy to have requirements, implement software, and test the requirements are satisfied. Almost everybody knows how to do that. The problem is, oh, I forgot

that when this thing always happened, that one goes down, you're supposed to do B.

MS. ALVARADO: We don't, and that's not part of what we are doing. We're trying to do like a spot-check, like I'm saying, like peek at certain requirements to see that they follow their process. And if we determine that they didn't follow the process, then in that case we will ask them to address that, both the vendor and the licensee.

MEMBER MARCH-LEUBA: You're doing the easy job. I mean, it's tedious and long, but it's the difficult one is thinking about what is missing. And that's the problem with what you are proposing. It is, how do we know?

MS. ALVARADO: Well, but I mean it's --

MR. HERB: If I could answer that question for the industry, because we provide that requirements to the NRC for their review and acceptance for a part of a LAR.

Those requirements are informed by hazards analyses. And so, we do a hazards analysis and we look at the baseline function requirements of our current licensing basis and our current systems, and we look at the hazards associated with a digital system, applying those. Did we get the negative

requirements and the missing requirements from that by addressing -- there's several methods that we can use, STPA methodology, HAZCADS, fault tree analysis. And we look for the missing requirements.

And so, when we submit a license amendment to install a digital protection system, it includes a full set of requirements along with that that's available for the NRC to review.

MEMBER MARCH-LEUBA: Let me give you an example we just heard before. Whenever the signals for that turbine control system go out of the scale, you scram. Okay. The requirements you have, if it goes up, it's good. So, you should have two different requirements instead of only one. There was one missing.

MR. HERB: That's right. That's absolutely right. But you have to remember, turbine control systems are not protection systems. Protection systems are much simpler. And so, they're, generally, if a signal goes high, then you trip. If the signal goes low, you trip. There are some more complex ones that maybe have a curve that is developed based on your operating -- but they're much simpler than turbine control systems.

MEMBER MARCH-LEUBA: That is the easy

part.

MR. HERB: Yes.

MEMBER MARCH-LEUBA: Again, that's the easy part. That you're going to do. I'll stipulate that that you do right. The problem is handling exceptions. What happens if you have a division by seal? What happens if your variable gets stuck at 2.7 volts and doesn't move anymore?

MS. ALVARADO: I just want to add something, that maybe we're focusing a lot into requirements specification. It is important, your software requirements specification, but you also need to keep in mind that these processes go through a whole life cycle. And it's not just like I'm writing the requirements, I program, and I'm done. They do go through a whole set of tests at different levels, at different stages of development.

And one example, coming back to what you're saying, it actually happened with Diablo Canyon. When we got the application for the Diablo Canyon safety system, the reactor protection system, one of the vendors -- they were using two vendors, two different platforms for diversity -- did not fully understand, because he was the first time working with the nuclear industry, how to implement the

requirements for the alarms that were launched. Okay? And they didn't find that out until we started doing design testing. That required a whole lot of like rework and redesign and retests for the system.

But that's not something that is now my responsibility as the staff to say, oh, this requirement is good or not because, like Ray said, they are the ones who know what they want the system to do, right? So, that's why BTP 7-14 -- BTP 7-14, not 19 -- has all these different steps or plans and procedures and things that you have to do that are endorsed by the NRC following industry standards, in which they have to, you know, not just create the requirements, but they have all these different steps that they need to follow before they can go and plug it in the plan.

CHAIRMAN BROWN: We've overrun, but that's okay. We'll make it here.

Do you all have anything else to address?

(No response.)

I want to go ahead and move on to get EPRI up here.

Okay. Thank you all very much. Thank you, Ray, by the way.

MR. HERB: You agree with me.

CHAIRMAN BROWN: We will continue to receive the slings and arrows of outrageous fortune.

(Laughter.)

You're on.

MR. GIBSON: Well, thanks for having me.

So, today I'm going to give you EPRI's perspective on digital I&C --

CHAIRMAN BROWN: You've got to stay right up there. You can't lean back.

MR. GIBSON: Okay. I'm going to give you some EPRI perspective on digital I&C reliability and software CCFs, and some of the research that we've been doing really over the past 10 years. Now some of this you have seen already. So, it will be a refresher for you, but I'll give it maybe a little different context.

Let's see here. There we go.

So, our prior research has really looked pretty hard at some OE and some other reliability measures over the years. Now this is a list. In the interest of time, I won't read this to you.

CHAIRMAN BROWN: Tell people what "OE" is.

MR. GIBSON: Operational Experience.

CHAIRMAN BROWN: I know what it is. It's just I would just ask you to minimize the acronyms in

the discussion, if you can. Okay?

MR. GIBSON: That will be fine.

MEMBER BLEY: I'll remind you when we do the letter.

(Laughter.)

CHAIRMAN BROWN: I hate to remind you, but I like to spell things out, and then, I got beat on to put the acronyms in everywhere.

So, this is an internal disagreement here totally unrelated to your subject.

MEMBER BLEY: Go ahead.

CHAIRMAN BROWN: So, I'll turn off my mic.

MR. GIBSON: So, let's look back just for the folks on the phone, because I don't think I actually got introduced. But I'm Matt Gibson with EPRI, Technical Executive in the I&C Program. So, my responsibilities are doing research on digital I&C, cybersecurity, and human factors.

On the slide here you see a list of the products that we've produced over the past 10 years that are relevant to this discussion related to I&C reliability. We'll just give you a history of these.

The one you probably have seen before, because I know it's been presented here, is some OE work we did on U.S. and Korean data. We were able to

get that data through the utilities primarily and some from INPO. And we looked at those events, looking for your software versus hardware, versus safety-related versus non-safety related. And I'll just summarize these, but you can see the software common-cause failures that we detected in that data was just one out of the 49 events; zero in the 19 Korean events.

If you look down for the non-safety, because this is a good juxtaposition that we need to think about, you'll see that your common-cause failures rose a little bit. Of course, we had a lot more events to work with; Korea less events of 3 percent.

What's probably useful to see here is the non-software common-cause failures were significantly higher than the software common-cause failures in both the Korean data and U.S. data, and both for safety and non-safety. And that really lines up with what you guys have been talking about all day: why are we talking about software CCFs and what's the context?

So, the conclusions that we made from this was that your software CCF is something you have to think about, that's true; something you have to deal with; that's true. But is it any more problematic than other CCFS?

The methods used by the folks during this time period, which really goes back a pretty long ways, were -- especially for 1E -- were effective in limiting those CCFs. And when we looked at these, we didn't see platform-level CCFs, either, software CCFs. The one mentioned here, of course, people can argue what the definition of a platform is, and we can do that in a few minutes when we get onto questions, but more at the application level.

MEMBER REMPE: I was waiting for you to ask your question again. Are you going to?

MR. HECHT: It might be better if you ask it, Joy.

(Laughter.)

MEMBER REMPE: Oh, okay.

So, you heard earlier he was asking, is EPRI willing to share the underlying data with the NRC, with this new research project, the two new research projects that are started?

And then, I have a question for the staff that I'm curious about.

MR. GIBSON: That's a pretty long question. The short answer is no. All right. The long answer is that getting meaningful reliability data for stuff is a closely-guarded IP secret of these

folks, especially accurate information, because they share that information with the folks they have business relationships with or they have other relationships with. But we were able to get this data through a series of NDAs, and that sort of thing, that preclude us from actually giving raw data out.

MEMBER REMPE: That's a good enough answer.

Then, I would like to ask the staff person, weren't you the person who said you would come up and talk a little bit more about the two new projects that you're starting? Because I was looking up the -- we had a discussion with the staff in the beginning of November, and they didn't really discuss any new projects that are coming up on CCF. In fact, the user need was like 2015. So, could you talk a little bit about what it is you're doing with those two new projects more? And could you let us know, are they feasibility studies, or what are they?

MR. JENKINS: This is Ronaldo Jenkins. I'm the Chief of the Instrumentation, Controls, and Electrical Engineering Branch.

Paul Rebstock, who spoke earlier, he's not directly involved with the projects you're referring to.

The two risk-informed projects that we just started in the Office of Research, one is on how to enable the staff to use risk-informed methodologies. So, that's one. One of the projects is focused on that.

The other project, which is much more longer term, is to look at software reliability. And, of course, there's been a lot of questions about software reliability and what exactly does it mean. One of the problems is it's a moving target. As you know, the life cycle for software in terms of it being a product changes fairly quickly over time. So, if you're studying the reliability of a given product in the sixties, you're dealing with a different product than you are currently now.

So, our focus is on the nuclear power plant technology that, presumably, would be put into service with the digital upgrades. So, we're trying to estimate with that second project a reliability number. And it is going to be difficult; there's no question about it.

We also took action to look at the EPRI data, the operating experience data. We had a group of folks to look at that, and Matt Gibson was kind enough to help us to look at that data.

One of the problems you have is, when you're looking at a given report, it's summary-level information, and it doesn't get to the root cause associated with that failure. And that's really what you need. In order to compare apples to apples, you need to know you're dealing with the same apple or a version of it, not a totally different root cause associated with it.

Does that help?

MEMBER REMPE: That helps a bit.

MR. JENKINS: Okay.

MEMBER REMPE: We may have some follow-on questions.

MR. JENKINS: Okay.

MEMBER REMPE: But I'm glad this topic came up today. So, thank you.

MR. HECHT: I just would urge that, before precious resources be spent in investigating that issue, that you look at past related studies. I mentioned ORNL. There's been others done by Brookhaven.

MR. JENKINS: Right.

MR. HECHT: I'm sure that there are probably others in the archives. If you don't have data, if you don't have enough data, and if you don't

have sufficient quality data --

MR. JENKINS: Right.

MR. HECHT: -- you probably will end up in the same place as those other forgotten reports, and that would be a shame.

MR. JENKINS: Right. You're exactly right. The problem is getting data that will allow you to draw some statistical inferences associated with how is the reliability that you are trying to estimate, whether or not that data is sufficient or not. And so, that is always a problem in any type of research that you're going to do.

MEMBER REMPE: Is this a user need that's going forward or is this a feasibility study? What is this now?

MR. JENKINS: This is a user need. The technical lead for this project is in the Division of Risk Analysis. So, it's the same folks who are doing PRA. They're taking the lead on the project, but we're working with them from a digital I&C perspective.

MEMBER REMPE: Okay. So, it's an existing one with a new twist, is what it is? It's not a new one?

MR. JENKINS: No, it's a new project.

MEMBER REMPE: It is a new one? Okay.

MR. JENKINS: Yes.

MEMBER REMPE: Thank you.

MR. WATERS: This is Mike Waters.

I just want to clarify for Ronaldo that the goal is to look at existing methods, because we recognize industry are making reliability claims. They're going to continue to do so. We recognize one day they may want to start assigning numbers in their PRAs when we now modify to digital.

So, this research is to look at the state-of-the-art methodologies, what are limitations, what makes sense for us to independently evaluate reliability claims that are being made to us. So, I just want to clarify we're not developing a new reliability method or a new way to assess or quantify reliability.

MR. JENKINS: Yes, that's correct. It's not to develop a new methodology.

MEMBER REMPE: Thank you.

MR. HECHT: The methodology is not the issue. The parameters are.

MEMBER BLEY: Hey, Matt, just a little favor?

MR. GIBSON: Yes.

MEMBER BLEY: We got you to pull the mic up real close, but it's so close that it makes noise when you breathe. So, if you could push it off just a little bit? There you go.

(Laughter.)

MR. GIBSON: Well, we'll calibrate. How about that?

MEMBER BLEY: Thank you.

MR. GIBSON: Okay. So, I can use my outside voice, too, if I need to.

MEMBER BLEY: No, it's got to go on the record, so we need it through the system.

Christina, Matt's second slide had a list of EPRI reports. I know we've seen some of them. Can you see which ones we can actually get and take a look at? I don't want to do this now. Don't address it now. Just talk with them and see what we can get.

MS. ANTONESCU: Okay. Sure.

MEMBER BLEY: I just took a look. They're not publicly available, or at least the first couple I looked at were not.

MR. GIBSON: You have all of these.

MEMBER BLEY: The staff does?

MR. GIBSON: Yes.

MEMBER BLEY: You've given them all to the

staff?

MR. GIBSON: Yes.

MEMBER BLEY: So, we can get them from the staff. Okay. Thank you.

MR. GIBSON: You're welcome.

So, let's pick up with some research we did on the actual sensitivity of I&C reliability. So, in this particular research, we did really plug in digitalizing into the PRAs, looked at 18 initiating events, and experimented with sensitivity analysis. You know, having the system fail, always failing, and also never failing.

And what you see from that is the actual sensitivity that even protection systems have to overall plant safety. Because there's enough functional reliability in a plant that, when you do the probabilities and such like that, that I&C becomes less of an actual risk.

So, if an initiating event has a high frequency, if you just do the math, it will end up, you know, the reliability of the digital system will have more of an impact on the total risk frequencies or the consequence frequencies. If the initiating events have very long periods or low frequencies, then the reliability the digital system will have much less

of an impact.

Now, when Warren and such were up here, you guys were talking about failure of 10 to the minus 4 for reliability and such, and somebody used the probability failure on demand. Well, actually, in 61508 and ISA 84, probability of failure on demand takes the reliability of the system and mixes it with normal reliability math with the frequency of the event. Because, remember, it's probability of failure on demand, not probability of failure. The system may, in fact, fail once in a while, but if it doesn't fail on demand, which is when the initiating event is occurring -- so, those numbers are actually pretty high. I noticed you had an event initiation 10 to the minus 4 that 10 to the minus 8 would be the probability on demand. So, you would actually result in a consequence because that has to have coincident failure of the system along with the initiating event.

Anyway, these sensitivity studies also tell us a little bit about the impact of adding diverse systems, because there's probably been a little bit of too much of a focus on a specific failure mode. And I think some of the industry folks earlier talked about that.

If you truly are risk-informed and you use

risk tools to figure out what this is, you can insert an actual brand-new system that can itself trip the plant. Potentially, depending on how it's done, your total core damage frequency can go up. And you might have been attempting to address a specific failure mode, but if you don't evaluate that change you made to the system against the total risk, you don't really know if you're making the risk more or less. And I think that really brings the question of, you know, exactly how much are we going to use risk-informed and other tools to inform this process. I think that's a question on the table from measuring total system reliability.

CHAIRMAN BROWN: Go back to your previous slide. You said a lot of other things, but you didn't -- I was looking at your chart, and it says, "Event and sensitivity analysis concluded that a diverse platform was not more effective in mitigating postulated SCCF than functional diversity or manual operator action." And yet, I had no way to conclude that from looking at your little chart. I presume --

MR. GIBSON: No, this is an all-day discussion actually because we have to go at it through the data. But here's --

CHAIRMAN BROWN: No, no. No, no, no. I'm

not going to track through the data. Does this table somehow communicate -- I mean, I see all these accidents, events with CDFs, but how do they --

MR. GIBSON: If you look, it's --

CHAIRMAN BROWN: Let me finish.

MR. GIBSON: Okay.

CHAIRMAN BROWN: How do these relate to conclude that a diverse platform was not more effective in mitigating a postulated SCCF?

MR. GIBSON: So, if you look in the -- I printed these rather small -- but if you look at the righthand column, there's going to be a discussion about doing these probabilities by the insertion of diversity, which were just added onto the fault trees, right? You added a diverse system which would --

CHAIRMAN BROWN: Is that the little box at the lower righthand corner?

MR. GIBSON: Yes, the little box at the right that takes all of the -- you see how the lines go vertically?

CHAIRMAN BROWN: Yes.

MR. GIBSON: Those are the top and the bottom, and you'll see some of them are the six sensitivities that were done with and without diversity.

CHAIRMAN BROWN: So, what does that say?

MR. GIBSON: It says that your diversity, when you add it, controls for a specific failure mode, but doesn't necessarily reduce the risk because it itself adds risk. You can't add a diverse system without adding risk. So, the risk you add has to be less than the risk you mitigate.

MEMBER MARCH-LEUBA: What risk are you adding?

MR. GIBSON: The risk you're trying to mitigate is a software common-cause failure.

MEMBER MARCH-LEUBA: And now, I have a second system, a diverse system, and what risk am I adding?

MR. GIBSON: Your risk is you're adding a whole other system which in itself has reliability --

MEMBER DIMITRIJEVIC: But it's a backup for the first system.

MR. GIBSON: Yes, it can itself initiate a plant event, initiate itself, because it can trigger the plant, right? If it's a backup reactor protection system, it itself can fail and trip the plant, initiating an event.

MEMBER MARCH-LEUBA: I find that hard to believe.

MEMBER DIMITRIJEVIC: It doesn't make sense.

MR. GIBSON: Why?

MEMBER DIMITRIJEVIC: You're adding a redundant system. So, you're making the system more reliable. Now how important does --

MR. GIBSON: You're not making it more reliable. You're not making it more. You're controlling for one failure mode.

MEMBER DIMITRIJEVIC: What do you mean by "failure mode"?

MR. GIBSON: See, the reliability of --

MEMBER DIMITRIJEVIC: It's a software failure.

MR. GIBSON: We'll get to this in a second.

If you plug systems into a fault tree, and you assign probabilities to them, okay, the most reliable thing is where you have a system and it never fails. But what really happens is now you have these different components and systems coming up through your fault tree with different probabilities. Now if you assume a CCF, right, if you assume a CCF, and you say the redundancies will appear on the fault tree -- if you say, okay, instead of giving that equipment

reliability figures like 10 to the minus something, but I'll say that I'm going to accept a software common-cause failure and force it to fail on the fault tree. You will get a probability and you say, okay, that's bad because it will always go to an event. I need to add something in line with that on the fault tree that, if I assume that CCF, then it will prevent me from taking a consequence. Well, that new thing you put on there in itself can fail, and it has a reliability metric all by itself. So, while you've controlled for one fault, you've actually added the potential of other faults in the fault tree.

MEMBER DIMITRIJEVIC: Okay, but we added to mitigate these faults. So, it may only add spurious operation or initiating event, but that's usually very low risk. So, therefore, by preventing your common-cause failure, it actually helps you. It's an "and" gate, not an "or" gate. You're discussing it like it's an "or" gate, but it's actually an "and" gate with your software failure. And therefore, it helps you with that. You need to fail them both in order to fail.

MR. GIBSON: You need to fail them both to reach the event that you're protecting against --

MEMBER DIMITRIJEVIC: Yes.

MR. GIBSON: -- for the CCF. But that thing you added, all right, has to be able to, well --

MEMBER BLEY: Independently actuate a trip as well.

MR. GIBSON: Yes, it's independent, right? So, it's not an "or" (sic) with the thing, "and" -- this is "or". So, you'll have to be able to trip the plant if the conditions, if the primary system doesn't trip the plant.

MEMBER MARCH-LEUBA: Yes, but you're telling me that adding a protection system to the reactor is really, really bad.

MR. GIBSON: Really what?

MEMBER MARCH-LEUBA: Really bad.

MR. GIBSON: It's not really bad, but it might not be doing what you think it's doing. That's all we're saying.

CHAIRMAN BROWN: He's just simply saying the backup system could initiate a trip independent of whether the other system --

MEMBER DIMITRIJEVIC: But that's --

CHAIRMAN BROWN: -- independent of an event occurring. It can trip the plant regardless --

MEMBER MARCH-LEUBA: Everybody keeps talking risk-informed and they forget about the risk.

I mean, you always keep talking probabilities/frequencies instead of talking consequence. The consequence of a scam is nothing --

MR. GIBSON: Consequence is not risk. Risk is consequence and probability.

MEMBER MARCH-LEUBA: Right.

MR. GIBSON: So, when you change the probability that you could potentially have a bad outcome broadly, then --

MEMBER MARCH-LEUBA: It's late; I'm not buying.

MR. GIBSON: That's okay.

CHAIRMAN BROWN: I can't believe this; I think I'm even agreeing with Vesna and Jose, in that the backup was added. You've got a system to take care of a particular event. That's what it's designed to do, and it's a software -- because we're going to terminate this discussion after I finish.

(Laughter.)

Because we've got to get on with it.

You've got a system that's in there that's supposed to respond to a thing, but it may have a common-cause failure --

MR. GIBSON: That's right.

CHAIRMAN BROWN: -- of some type that

prevents it. So, you add another system, diverse, that will also perform the same function. Okay. There's two things that can happen. One, in the absence of an event, the other system can cause the plant to trip on its own.

MR. GIBSON: That's true.

CHAIRMAN BROWN: It can fail and it can cause a problem. Okay? Now you don't have an event occurring. All you've done is put the plant in a safe condition when you do that, theoretically.

MR. GIBSON: Theoretically.

CHAIRMAN BROWN: So, that's a reliability issue. What you're preventing is the failure of either one of those two systems to not operate when you actually have an event that could damage the plant. And so, I think that's the way I view it. So, the argument that you're increasing the probability of something, to me, doesn't --

MEMBER MARCH-LEUBA: Would you allow 20 seconds?

CHAIRMAN BROWN: No, but go ahead. You're going to take it anyway.

MEMBER MARCH-LEUBA: I'm going to talk anyway.

(Laughter.)

By adding a second scram system, at most you double the probability of a full spurious actuation. Factor of two. Factor of two, as my colleagues tell me, is nothing. I mean, you need 10 to the minus 4. Two is non-existent. So, I mean, you just doubled the probability of having a spurious actuation.

But, on the common cause, you went from 10 to the minus 4 to 10 to the minus 8. I'm not buying.

CHAIRMAN BROWN: Yes, I'm agreeing with you. If you didn't get that out of my comments --

MEMBER DIMITRIJEVIC: Basically, the risk associated with spurious trip, whereas, the risk associated not to trip on demand, it's totally different.

MR. GIBSON: Okay. So, I see where your failure mode is here.

(Laughter.)

So, if you are viewing this strictly as I'm going to take a CCF, and therefore, my diverse thing helps me, that's one way you can look at it. But, reality, your CCF does not have a zero, I mean, a one probability. So, let's say the probability of that CCF is really -- I'm just making this up -- 10 to the minus 3. When you add that other device in there,

and you plug in those other reliability numbers, that's where you see the impact of your diverse system. Because it's only theoretical that a CCF will always happen.

CHAIRMAN BROWN: All it's doing is increasing the possibility that you may have a response that is not unsafe; it's just it's unreliable. It takes you offline. Whereas, the other system, if it didn't have the backup, if it had the failure when you had a demand, then you damage something, the plant. You melt something or you have whatever the circumstance is.

MEMBER MARCH-LEUBA: But in my car, I have a car that only has brakes and two front tires. And now, I've got a second system; the brakes are also on the back tires. Tell me what's wrong with that. I mean, what is this problem with having two --

MR. GIBSON: Well, we could probably move on.

CHAIRMAN BROWN: We're going to move on.

MR. GIBSON: The data to support that is in that report.

CHAIRMAN BROWN: Okay, we're terminating all this. Go on to the next slide, Matt.

MR. GIBSON: All right.

CHAIRMAN BROWN: Okay?

MR. GIBSON: I'll do the best I can.

The dependability, we did some research on dependability, and we call it "methods for assuring safety and dependability when applying visual instrumentation and control system". We pursued developing specific preventive and limiting measures that could be used to reduce the likelihood that you would have a CCF. And we brought those out in this report.

We also furthered the research we did in the previous one and looked at dealing with those CCFs, software CCFs, and other CCFs, would have a nexus to your safety analysis in your PRA. And that's all in this report, and I think some of this was advanced on NEI 16-16. But, you know, for whatever reasons, I'm not familiar with all the reasons why that didn't go forward.

We'll move on to the next research we did, our most recent research, where we went and got reliability data from the industry for equipment that had been SIL-certified, Safety Integrity Level certified, using the requirements in IEC 61508. So, the previous OE data that we had was good, but it was small as far as the amount of data we had, amount of

operation that we had. There was also a broad diversity of systematic controls applied to that equipment.

So, you know, software is not just software. I mean, you have to understand how it was made, under what circumstances it was made, and what requirements were applied to it, because the software reliability in your home router is different than it's going to be in the one in your protection system in your plant. It is.

And so, we figured out that we would have to move on from nuclear information. There's just not enough. There's enough digital in nuclear, and nuclear is not that big of an industry comparative to petrochemical and others.

So, through a series of NDAs, we were able to get a fairly large amount of data, about 2 billion hours or so of operating data off of 12 logic solvers. And we analyzed those things.

What we were able to do with this research is control for reliability. So, if you're doing a research project and you want some highly reliable software, you can only compare software that's been created using the same process, even though it's different software. Because if it's created with

different systematic processes, the information you get might not be accurate.

So, by comparing software -- well, this was software and hardware, but the software that had been certified or created through the requirements of IEC 61508, which had detailed specific implementation requirements for software and hardware to drive reliability. Then, we can compare, well, how did that turn out? Did that process actually result in reliable systems? And I think it did, because we didn't find any platform-level issues that were correlated to the software itself having a latent failure out of those 2 billion hours.

So, that gives some statistical idea about the platform software. I think Neil was talking about what's a platform. In the case of this, it's your hardware. It's your system software; that is, the infrastructure software that's running that particular program logic controller. It's also the library that you subsequently use to make your software with. It's the tools that you use to make those risks. So, it's all those are included in the certification.

And that's also reflected in these hours, too. Because the way this data is reported back through the processes and the various pathways we use

to get the data, had there been a failure in, say, the library, a function block, it would have been reported back through this. Application failure, though, would not be reported this way.

Let's see if there's anything more that we can tell you.

MR. HECHT: Can I ask a question about that data?

MR. GIBSON: Sure.

MR. HECHT: You said that some of it was from SIL 3-certified platforms, some of it?

MR. GIBSON: It's all from SIL 3, in SIL 3.

MR. HECHT: So, all those 2 billion operating hours come --

MR. GIBSON: All from that, yes.

MR. HECHT: I see. But that would be a pretty large sample, and it's pretty homogeneous within that.

MR. GIBSON: Of course, that was the point of it. See, we were actually testing -- you have systematic controls on software resulting in high reliability statistically. And that's what we were able, we think, to demonstrate.

The only way you can do that is have a

consistent process for producing the software. It's just like a mechanical thing. If you have some steel and you produce it one way, and you have some more steel and you produce it a different way, you can't compare the structural reliability of steel without knowing how it was made and its metallurgy, and all that sort of thing. And we did that here.

We controlled, basically, in sort of a scientific method for how the software was made. And so, what this tells you is that the systematic controls required by IEC 61508 do result in a highly reliable platform. I mean, that's the gist of what our data showed.

MR. HECHT: Two billion hours is a lot of data and should result in a fairly low or fairly narrow confidence interval. Do you have the numerical value for the platform?

MR. GIBSON: You know what? I don't. I don't have it. We did not calculate a 10 to the minus frequency. And I'll tell you why. We'll talk about it because I have a little more time.

CHAIRMAN BROWN: Why don't you move on?

MR. GIBSON: Well, this is an important tie-in to something else I'm going to say.

The researchers, the team researching

this, we did not want to claim a 10-to-the-minus or a frequency-type conclusion for this because the academic community and the practitioner community, when you do this, do not support ever doing that.

So, really -- and this is something maybe you guys can think about -- what we really did with this is prove the effectiveness of the systematic control, not necessarily reliability of the software in general. So, this data that we have only mattered or has relevance if you're talking about an IEC 61508-certified device. It doesn't really mean anything otherwise, right, because that's what we controlled for.

So, in the future, if you want to do integration of risk reliability for software, you're really going to have to control for how it was made, because that's really the reliability metric you're measuring, is the reliability of that process, not the intrinsic reliability of software, because it's all over the place.

Any more?

MR. HECHT: I think we're limited by time.

MR. GIBSON: All right. Well, there we go.

You've seen this before. I'll just

concentrate on a little bit about the insight we got from doing that was that your platforms and your integration activities and your applications are really three distinct layers of the composition. And in the broader world, they're really done by different people usually. Platforms are currently bought. Most people, even in our current nuclear industry, buy their platforms from somebody and they add integration applications to it.

So, we think that even potentially for any retroactivity you're doing that, if you separate these out a little bit and potentially have maybe different criteria for the different platforms, integrations, and applications, it will make it more straightforward to analyze something you get to read. So, that's something to think about.

When you actually build one of these, when you build a system, this is how you build it. This is how you really put it together and make it and test it and do stuff. You start with the platform, you integrate, you add applications to the top of it.

We'll move on to HAZCADS. You know, folks mentioned that a little bit. We've published HAZCADS and you have a copy of it in-house. Revision 1 is coming out in the summer next year. We published it

in the version you see, so we could get started doing blind studies. So, we have done blind studies with this product with utility and some vendor participants.

So, if you can see this, okay, if you look closely at this -- on your handout it's gray, so that's good -- but if you look on your handout, you'll see the gray squares that are on the fault tree. So, what we're able to do with this process is to use a process called System Theoretic Process Analysis, which is a hazard analysis developed by MIT. It's being proven to be very favored in other industries. And it gives you a structured way to find the problems with your system at whatever level of decomposition you need.

So, what we do with this process is we look for those hazards through this process. Again, that's something we can talk about in some detail later. But, if we find what's called an unsafe control latch, which is a result of this analysis, we can then insert it into the fault tree. See where these gray slots are.

This is a qualitative idea. So, what we do is we put the qualitative node into the fault tree and, then we do sensitivity analysis on it, again, by

setting it to always true and always false. And that gives an idea of what kind of impact that particular piece of equipment would have on your top event frequency. So now, we know what the hazards are, which is one big thing, and the next thing we know is how sensitive that that digital hazard will be to the final consequence.

Now, in our estimation, in our research, this provides a risk-informed infrastructure for digital I&C because it combines qualitative and quantitative analysis, gives you a sensitivity for your qualitative ideas, and from that, then, you can decide on the degree of qualitative or systematic controls you want to apply to achieve a high degree of reliability for a software-based system.

And we talk about a little in the bottom, the next thing you press on after this is look at your causal factors, which gives you your initiating causes for each one of these function blocks. That's sort of below this block in the fault tree. So now, we know why this particular node in the fault tree -- what things are driving it. And we include all manner of reliability issues, including cybersecurity, in that.

We just finished blind studies doing this, as I mentioned. We got a darn good insight with that.

We found out that STPA worked really well in finding the faults or the hazards -- let's put it that way -- all kinds of hazards. Design hazards mainly is what we're looking at here.

We did that by crafting a scenario where we knew there was a problem with the system and asking the participants to find that problem using this process, and they did. They were 100 percent successful finding the unknown problem that they were faced with.

What we did find out is engineering and risk analysis -- and I'll say, you know, that's the challenge we face all around -- engineering, a lot of folks, the engineers aren't that familiar with how to do risk and fault trees, and the fault tree people aren't really comfortable with saying, well, if it's 10 to the minus X, then we're done, the actual analysts themselves.

So, we think this process is going to have to be a team process where your engineering folks do the hazard analysis and the causal factors, and then, the risk analysts will, then, apply that and do sensitivity analyses to give you the risk insights you need.

And depending on the level at which you do

it, your risk insights can come from simply knowing the hazards and the likelihood and the causal factors. So, there's a little triangle here that you can see on your thing. It's kind of like the risk triangle. If you break any one of these sides, you've prevented the consequence. You've eliminated a hazard. You've eliminated the causal factors. Or you reduced the likelihood to a very low level.

MR. HECHT: Can I ask a question about the HAZCADS methodology?

MR. GIBSON: You sure can.

MR. HECHT: You say it provides a basis for risk-informed I&C infrastructure. Are you advocating that the NRC consider using HAZCADS, and if so, I guess I would have a lot of questions about how STPA is being applied. And specifically, you have --

MR. GIBSON: EPRI doesn't do policy advocation. So, we do this and we provide it to our community of interest, which is you guys and our utility members. So, I think if you want to do risk-informed, you ought to look at it.

MR. HECHT: Okay. Thank you.

MR. GIBSON: Any other questions you might have in the future, feel free to reach out.

DRAM is part of this process. It's a

modular process. This is where we look for the causal factors. These are the things that would contribute to the reliability issues that you have in any digital system. This will be a replacement for our 300, 200-5326 process, and it will give it structure, a three-step structure; and also, leverage the terminology and requirements of 61508. So now, you'll be working towards the industry standards that have been proved very effective in achieving high reliability in like PLCs and other types of safety devices.

I'll just flash this. We can move on to the next one.

This is something we're working on, is to more clearly define software common-cause failure. Common-cause failures really have a context. I think Steve Vaughn talked about it. They're really part of the decomposition of your system and they exist in various levels of your system composition and decomposition.

And we think it's important to have a good, crisp definition, at least in our research. So, we're trying to do some research on what that would actually mean. What is a software common-cause failure? Certainly, we have to have some redundancy expectation to achieve a common cause because it has

to have that, but we also want to separate and help people identify the difference between a software common-cause failure and a single point vulnerability, because that gets conflated a little bit sometimes.

This is how it's put together. The HAZCADS you just were looking at, which has the STPA and FDA. The reliability is integrated into a systems engineering process. This is the process that I think Neil Archambo mentioned that U.S. industry has adopted. The CNOs have created a recommendation that every utility adopt these. So, the industry is in the process of adopting this process using the Digital Engineering Guide to improve the execution or do the modification. And they will be using these components when they do it.

I think maybe the last thing to see -- and you can study these, I guess -- this is a reliability model. And also, it's risk-informed. Your HAZCADS and your DRAM come together. You get your hazards inventory and sensitivity results, and you can take actions on those. You can make design changes and other compensatory measures to ensure that the consequence is not actualized.

(Announcement of alarm condition in building.)

MR. GIBSON: All right. I'll try to speak over our AI that's speaking to us.

(Laughter.)

Our overall insights -- we probably just should have started with this slide -- are that your software reliability is really proportional to systematic controls and design and implementation constraints. You've got to constrain the design, too. You can't do things that are inherently unreliable to do. It's just one of those things.

CCF is a subset of total software design and implementation errors. You can't have a software CCF unless you have a software failure in the first place. Your software CCF really needs to be more narrowly defined. I mean, just as a practitioner, it helps to have it narrowly defined because then you can work on the actual failure mechanisms that caused that particular thing to happen, not a more broad idea of software common-cause failure. And you need to be really aware of where in the decomposition of the system the software common-cause failure occurred, whether it's in the application or in the platform.

(Announcement of alarm condition in building continues.)

MR. GIBSON: Why don't you all guys read

this? Because I can't do it with this guy talking in my head.

(Laughter.)

So, questions, anybody?

MEMBER BLEY: That's all right. Your voice cuts right through it.

MR. GIBSON: Oh, does it now.

(Laughter.)

I guess the last one, the last thing, maybe the last two, is we get a lot of value -- this is a good point to make. If you look at the IEC stuff, if you look at NUREG-0800, and you look at Chapter 7, all of the standard references in there are about 30 years old. I mean, they are. We froze them in time. The rest of the industry worldwide, the safety industry, has moved along, because more and more things are done with software.

So, what we find when we look out in the other industries, the non-nuclear safety industries which primarily use the IEC standard, they potentially -- I mean this is for your consideration -- have eclipsed us in their ability to ensure reliability of a system or a component that's software-based. They have good processes. They have an active community of academics, vendors, and experts working on these

standards all the time, integrating their operational experience into it. Our research indicates that they're achieving a pretty good degree of reliability. IEC is the primary standard body that's working with folks for autonomous cars, autonomous cranes, and they're integrating all that OE. They're getting software reliability back into those standards. So, they're pretty good.

It's also where, if we need data, if you need data to support adopting any of these things, you're really going to have to go after non-nuclear databases because they're big. Maybe you can get at them. But I think that would be something to consider.

CHAIRMAN BROWN: Okay. The next round, we need to get public comment. So, why don't you get the phone, and I'll ask, is there anybody in the room that would like to provide comments?

(No response.)

Hearing none, we will wait for the line. Is the line open? Or are you going to open it?

Thank you, Matt.

MR. GIBSON: You're welcome.

CHAIRMAN BROWN: We're going through the rest of the dog-and-pony show right now.

MR. GIBSON: I understand.

CHAIRMAN BROWN: Is there anyone on the public line who would like to make a comment for this meeting? If so, say something.

(No response.)

Hearing none, we will close the public line.

Are there any other comments from members? Anybody? I'll start with Dennis, on your side.

MEMBER BLEY: Nothing to add. It was a good day. I learned a lot and look forward to seeing the next round.

CHAIRMAN BROWN: Okay. Jose?

MEMBER MARCH-LEUBA: Nothing to add.

CHAIRMAN BROWN: Joy?

MEMBER REMPE: I just wanted to thank the presenters for their patience today. This was an unusually different day for our abilities to have a meeting.

CHAIRMAN BROWN: I guess we lost Ron.

Does our consultant have any additional comments?

MR. HECHT: Just to reiterate the fact that I think Matt said that we should be using non-nuclear data sources. ORNL tried; it didn't work.

Perhaps it would work better.

CHAIRMAN BROWN: Oh, okay.

MR. HECHT: Perhaps we could get some help from EPRI or others, I guess primarily EPRI. I think that, irrespective of whether EPRI is able to get their NDA data to us, perhaps some guidance for how the NRC might be able to acquire it on its own might be valuable.

With respect to the HAZCADS methodology and the integration with FDA for probabilistic risk assessments, Nancy Leveson probably would not approve of that, saying that anytime she has a box with a software probability failure, she would say, "Just make it one."

But STPA certainly can be valuable in terms of defining requirements for failure mitigation and for hazard mitigation, what they call "constraints," and should be considered.

And finally, with respect to the comments about, whether it's 61508 or BTP 7-19, the underlying principles I think haven't changed in 30 or 40 years, which is, basically, define good requirements; create a design traceable to those requirements; implement code traceable to the design, and test at all levels. I would say that it might be instructive to look at

the differences between 7-19 and 61508 to see if there are any really significant differences from those principles.

MR. GIBSON: So, I did want to mention that we are bringing HAZCADS to the STPA conference this coming year. And so, we think Ms. Leveson will allow us to present.

MR. HECHT: I'm sure she will.

CHAIRMAN BROWN: Okay. Thank you very much, Myron.

With that, I don't have any additional comments to make, either.

So, with that, we are adjourned.

(Whereupon, at 4:49 p.m., the Subcommittee was adjourned.)

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

Branch Technical Position 7-19 Draft Revision 8

Advisory Committee on Reactor Safeguards

Subcommittee Meeting

NRC Staff Presentation

November 21, 2019

Agenda

- Background on Commission's Common Cause Failure (CCF) Policy
- Objective of Branch Technical Position (BTP) 7-19 Modifications
- Key Changes:
  - Categorization Scheme and Graded Approach
  - Defense-in-Depth and Diversity (D3) Assessment
  - Means to Eliminate CCF from Further Consideration
  - Qualitative Assessment
  - Spurious Operation Assessment
  - Re-structuring of BTP

Objective

- Present the modifications proposed for the next draft of BTP 7-19 regarding the review of license applications and amendments addressing CCFs due to latent software defects
- Obtain ACRS Subcommittee feedback for draft BTP-19, Revision 8

Background: Commission's Policy on CCF

- SRM-SECY-93-087 presents the Commission's policy on how potential CCFs should be addressed in DI&C systems
- Provides four positions for addressing potential CCFs
  - Perform D3 assessment to demonstrate that vulnerabilities to CCF have been adequately addressed
  - Analyze each postulated CCF for each event evaluated in the SAR accident analysis using best estimate methods
  - If the assessment shows a CCF could disable a safety function, provide a diverse means with a documented basis that the diverse means is unlikely to be subject to the same CCF
  - Provide a set of diverse displays and controls located in the main control room for manual, system-level actuation of critical safety functions and monitoring of critical plant parameters to support the performance of these safety functions

Background: SECY-18-0090

- SECY-18-0090 clarifies the application of the Commission's direction in the four positions within SRM-SECY-93-087
  - Recognizes significant effort has been applied to the development of highly reliable DI&C systems but residual faults within digital systems may lead to CCFs
  - Provides five guiding principles for updating the staff's guidance for addressing CCF

Summary of Draft BTP 7-19 Changes

- Incorporates the guiding principles from SECY 18-0090 Alignment
- Clarifies the applicability of the D3 assessment to safety-related systems with high safety significance
- Incorporates qualitative assessment criteria from Supplement 1 to RIS 2002-22 for non-RPS/ESFAS
- Clarifies staff positions on means to address CCF
- Provides additional guidance on spurious operation assessment
- Improves the structure of the BTP to enhance ease of use

Key Changes: Categorization Scheme and Graded Approach

	Safety-Related	NSR
Safety Significant—Significant contributor to plant safety	**A1** Perform D3 Assessment	**B1** Perform Qualitative Assessment
Not Safety Significant—Not a significant contributor to plant safety	**A2** Perform Qualitative Assessment	**B2**

Deterministic Criteria for Categorization of DI&C Systems (1)

- A1: safety-related DI&C system that:
  - Is relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE, or
  - Whose failure could directly lead to accident conditions that may cause unacceptable consequences if not mitigated by other A1 systems
- A2: safety-related DI&C system that:
  - Provides an auxiliary or indirect function in the achievement or maintenance of plant safety, or
  - Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state

Deterministic Criteria for Categorization of DI&C Systems (2)

- B1: NSR DI&C that:
  - Directly controls the reactivity or power level of the reactor, or
  - Whose failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system
- B2: NSR DI&C system that:
  - Does not have direct affect on reactivity or power level of the reactor, or
  - Whose failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin

Use of Risk Insights to Support Categorization

- Risk insights can be used to support the safety-significance determination in categorizing the DI&C system in terms of safety consequences from site-specific PRAs
- Use of risk insights should be an input to an integrated decision-making process for categorizing the proposed DI&C system

Key Changes: D3 Assessment

- D3 assessment should be performed for A1 systems
- D3 assessment includes determination of whether:
  - CCF vulnerability is eliminated from further consideration by use of design attributes, testing, or defensive measures;
  - A diverse means can be used to perform the same or different function than the safety function disabled by the postulated CCF; or
  - Consequence of a DBE concurrent with a CCF of the A1 system is acceptable
- For systems that are not A1 but are integrated with A1 systems, the D3 assessment should be performed on the integrated system unless it can be shown that the non-A1 system will not adversely impact the A1 system upon a postulated CCF

Key Changes: Means to Eliminate CCF from Further Consideration (1)

- Use of design attribute: diversity within the DI&C system or component
  - Provides guidance to use diversity within each safety division or among redundant divisions to address CCF
  - Calls for an analysis to demonstrate sufficient diversity exists in the design, so it is not subject to the same CCF
  - Provides acceptance criteria for use of this attribute

Key Changes: Means to Eliminate CCF from Further Consideration (2)

- Use of testing to demonstrate latent defects are not present
  - Clarifies criteria and terminology associated with use of testing to eliminate CCF from further consideration
  - Emphasizes the limitations on use of testing
  - Provides guidance to establish test methods
  - Provides acceptance criteria

Key Changes: Means to Eliminate CCF from Further Consideration (3)

- Use of defensive measures
  - Provides guidance to use defensive measures to prevent, limit, or mitigate the effects of a potential CCF to eliminate CCF from consideration
  - Provides criteria to use defensive measures based on an NRC-approved methodology
  - Provides criteria for use of other methodologies with the provision of a technical basis and acceptance criteria

Key Changes: Diverse Means (1)

- Clarifies guidance on the use of diverse means to perform the same or different function as the safety function disabled by the postulated CCF
- Clarifies the types of diverse means that can be credited
  - Existing systems
  - Manual operator actions
  - Diverse system
- Identifies acceptance criteria

Key Changes: Diverse Means (2)

- Provides guidance on the use of equipment outside the main control room for the performance of manual operator actions
  - Applies only for use of diverse means to address Position 3 in the SRM-SECY-93-087
- Clarifies guidance to address Position 4 in SRM-SECY-93-087, which calls for manual controls and indications located in the MCR to perform manual system level actuation of critical safety functions

Key Changes: Qualitative Assessment

- Provides guidance for performing a qualitative assessment to evaluate potential CCFs and their effects in A2 and B1 systems
- Identifies three factors can be used to show that the likelihood of CCF is sufficiently low, including:
  - Design attributes
  - Design quality
  - Operating experience
- Provides guidance on the performance of a qualitative assessment on a B2 system that could place the plant in an unanalyzed condition
  - Basis for not performing an assessment should be documented

Key Changes: Spurious Operation Assessment

- Provides bifurcated criteria for addressing spurious operation of SSCs due to a CCF in a DI&C system
- Provides guidance for operating reactors for performing an assessment to demonstrate that the safety analysis of spurious operations is not invalidated by the proposed digital modification
- Provides guidance for new and advanced reactors for performing an assessment to demonstrate that potential spurious operation of SSCs is bounded by events analyzed in the safety analysis
- Clarifies scope and methods for performing the assessment, including use of design attributes, testing, and defensive measures to eliminate CCF from further consideration

Key Changes: Re-Structuring of BTP 7-19

- Simplifies background and incorporates new guidance on CCF
  - SECY-18-0090
  - NUREG/CR 7007
  - RIS 2002-22, Supplement 1
- Maps criteria to four positions in the SRM-SECY-93-087
- Consolidates CCF guidance and corresponding acceptance criteria

Next Steps

- Public comment period ends in February 2020
- Potential public meeting during public comment period to facilitate comments
- Potential second ACRS Subcommittee meeting in Spring 2020 if changes resulting from public comment period are significant
- ACRS Full Committee meeting in Spring 2020
- OMB review and publication of final BTP 7-19, Revision 8 anticipated in 3rd Quarter 2020

Questions

Questions

Acronyms

BTP	Branch Technical Position	NSR	Not safety related
CCF	Common Cause Failure	PRA	Probabilistic Risk Assessment
CFR	Code of Federal Regulations	RIS	Regulatory Issue Summary
D3	Defense-in-Depth and Diversity	RPS	Reactor Protection System
DI&C	Digital Instrumentation and Control	SAR	Safety Analysis Report
ESFAS	Engineered Safety Feature Actuation System	SRM	Staff Requirements Memorandum
MCR	Main Control Room	SSC	Structure, System and component
MP	Modernization Project		

Background Information

Modernization Plans (MPs)

- Developed in accordance with Staff Requirements Memorandum (SRM) to SECY-16-0070
- MP#1 – Common Cause Failure
  - MP#1A: Supplement 1 to RIS 2002-22
  - MP#1D: Update to BTP 7-19
- MP#2 – 10 CFR 50.59 Guidance
- MP#3 – Commercial Grade Dedication
- MP#4A – ISG-06 Revision
- MP#4B – Broader Modernization Activities

SECY-18-0090 – Five Guiding Principles

1. Applicants and licensees for Production and Utilization Facilities under 10 CFR Part 50, “Domestic Licensing of Productions and Utilization Facilities” or under 10 CFR Part 52, “Licensees, Certifications and Approvals for Nuclear Power Plants” should continue to assess and address CCFs due to software for DI&C systems and components.
2. A defense-in-depth and diversity analysis for reactor trip systems and engineered safety features should continue to be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. In performing this analysis, the vendor, applicant, or licensee should analyze each postulated CCF for each event evaluated in the accident analysis section of the safety analysis report. This defense-in-depth and diversity analysis can be either a best estimate analysis or a design-basis analysis.
3. This analyses should also be commensurate with the safety significance of the system. An analysis may not be necessary for some low-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated.

Five Guiding Principles continued

4. If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should perform either the same function or a different function. The diverse or different function may be performed by either a safety or a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions in a reliable manner. Use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. If the defense-in-depth and diversity analysis demonstrates that a CCF, when evaluated in the accident analysis section of the safety analysis report, can be reasonably mitigated through other means (such as with current systems), a diverse means that performs the same or a different function may not be needed.
5. The level of technical justification needed to demonstrate that defensive measures (i.e., prevention and mitigation measures) are adequate to address potential CCFs should be commensurate with the safety significance of the DI&C system. For the systems of higher safety significance, any defensive measures credited need technical justification that demonstrates that an effective alternative to internal diversity and testability has been implemented.

SRM to SECY-93-087

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
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. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.

Graded Approach for Systems Categorization Concept

	Safety-Related	Non-Safety Related
Safety Significant	A1 (e.g. Protection System, Safety Control Systems*, Load Sequencers*)	B1 (e.g. Rod Control System, Feedwater Control system, Certain BOP Control Systems)
Not Safety Significant	A2 (e.g. Safety Chillers, Safety Control Systems*, Load Sequencers*)	B2 (e.g. Plant Computer, Service Water System Controls)

*The staff recognizes actual categorization may be driven by specific plant system configurations, the exact nature in which systems may be interconnected by digital equipment, and the plant's licensing basis. Systems that depend on the overall plant design may be safety significant or non-safety significant.

Common Cause Failure (CCF) and DI&C Systems

ACRS Subcommittee – DI&C

November 21, 2019

NUCLEAR ENERGY INSTITUTE

Background and Context

- Common Cause Failure (CCF) in digital systems:
  - The determination of reasonable assurance with respect to digital and analog systems should be congruent
  - Challenges with using probabilistic terminology in a deterministic context
  - Focus has been on ‘eliminating the consideration of CCF’ as opposed to ‘appropriately addressing CCF’
  - Software vs Hardware reliability

Path Forward

- Align on 1st principles
  - Software quality depends on complete and correct requirements, design, and implementation
  - Concurrent triggering conditions are required to activate a latent software defect
  - The effects and the likelihood of a software CCF can be minimized by design
  - Operating history can support software quality

Path Forward

- Align on Safe Design Objectives
  - Design Requirements Development
  - Design Attributes
  - Quality of the Software Design Process
    - Graded approach to safety
  - Division of Responsibility

Closing Remarks

- If CCF is ‘appropriately addressed’, then a diverse backup is not warranted
- CCF can be ‘appropriately addressed’ by adhering to:
  - 1st principles
  - Safe design objectives
  - Use industry best practices

EPRI R&D Perspectives on Digital I&C Reliability and Software CCF

ELECTRIC POWER RESEARCH INSTITUTE

ACRS Digital I&C Subcommittee Meeting on Draft Branch Technical Position (BTP) 7-19, Revision 8

Matt Gibson
Technical Executive
Digital Instrumentation & Control
mgibson@epri.com

November 21st, Washington DC

Introduction

- Over the past 10 yrs. EPRI has conducted various R&D projects to investigate digital I&C reliability and the nexus to plant safety.
- Today we will review the key R&D products developed over that period, the cumulative conclusions reached, and the methodologies developed to address digital technology.
  - 1016731- US 1E and Non-1E OE on digital systems
  - 1022986- KHNP 1E and Non-1E OE on digital systems
  - 1019183- Sensitivity of digital in D3,PRA, and Safety Analysis
  - 3002005326/DRAM- Safety and dependability Methods for digital systems
  - 3002011817- Safety Integrity Level(SIL) Certification efficacy for nuclear
  - 3002012755 – HAZCADS- Hazards analysis for digital systems
  - 3002011816 – Digital Engineering Guide (DEG)- systems engineering

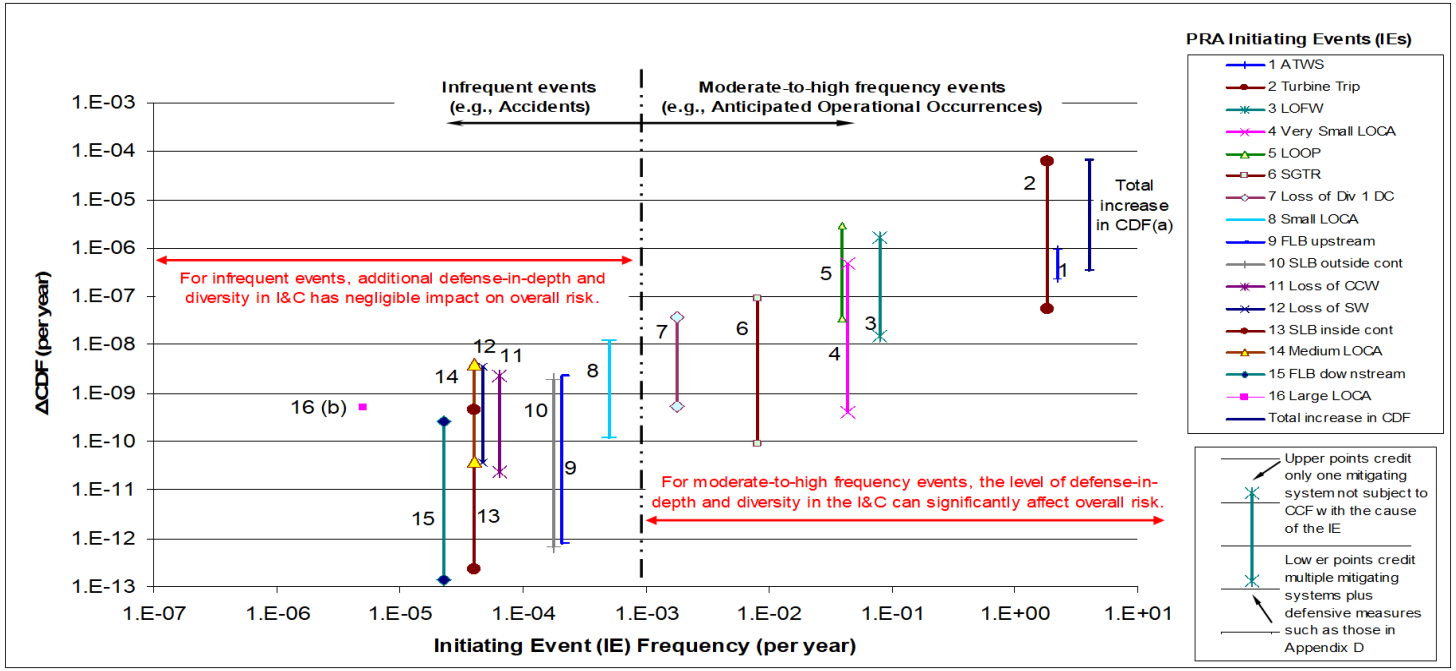
Past Operating Experience Reviews- US and Korea

- EPRI research has looked for software common cause failures in the OE data of 1E and non-1E systems
- CCF not very prevalent in safety-related systems
- Conclusions from 1016731 (US) and 1022986 (KHNP) Data:
  - Software has been no more problematic than other CCF contributors
    - Past methods have been effective in keeping software a minor contributor to potential 1E CCFs
  - EPRI Research has not identified any 1E events where diverse platforms would have been effective in protecting against SCCF. SCCF occurs predominately at the application level.
  - Several identified events confirmed the effectiveness of signal and functional diversity in protecting against CCF

Categories	U.S. 1987 – 2007 (EPRI 1016731)	KHNP 1984 – 2010 (EPRI 1022986)
Safety-related digital events reviewed	**49**	**19**
Single failures	38 (78%)	19 (100%)
Non-software common cause failures	10 (20%)	0 (0%)
Software common cause failures	**1 (2%)**	**0 (0%)**
Non-safety related digital events reviewed	**273**	**78**
Single failures	217 (79%)	61 (78%)
Non-software common cause failures	42 (19%)	14 (18%)
Software common cause failures	**14 (2%)**	**3 (4%)**

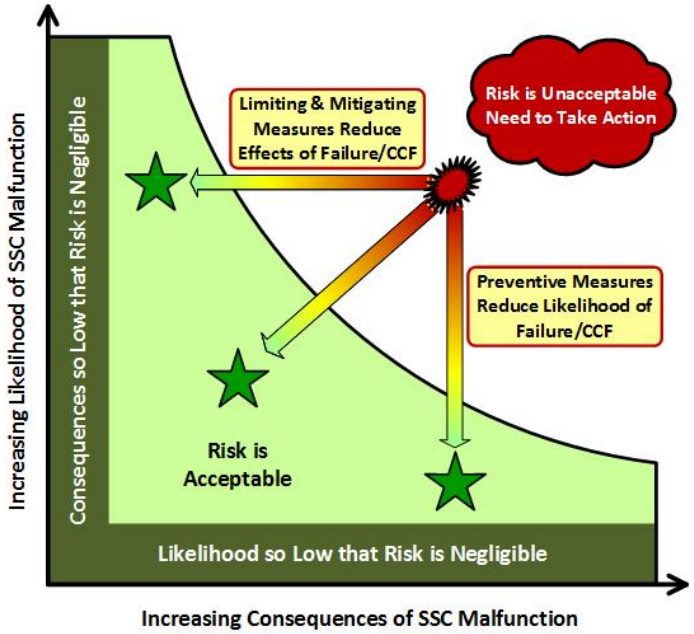
Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants - 1019183

- Eighteen initiating events were analyzed.
- Six sensitivity studies conducted: including addition of diverse platforms.



- **Event and sensitivity analysis concluded that a diverse platform was not more effective in mitigating postulated SCCF than functional diversity or manual operator action.**
- **For low frequency events I&C diversity had even less risk impact.**

Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems- 3002005326

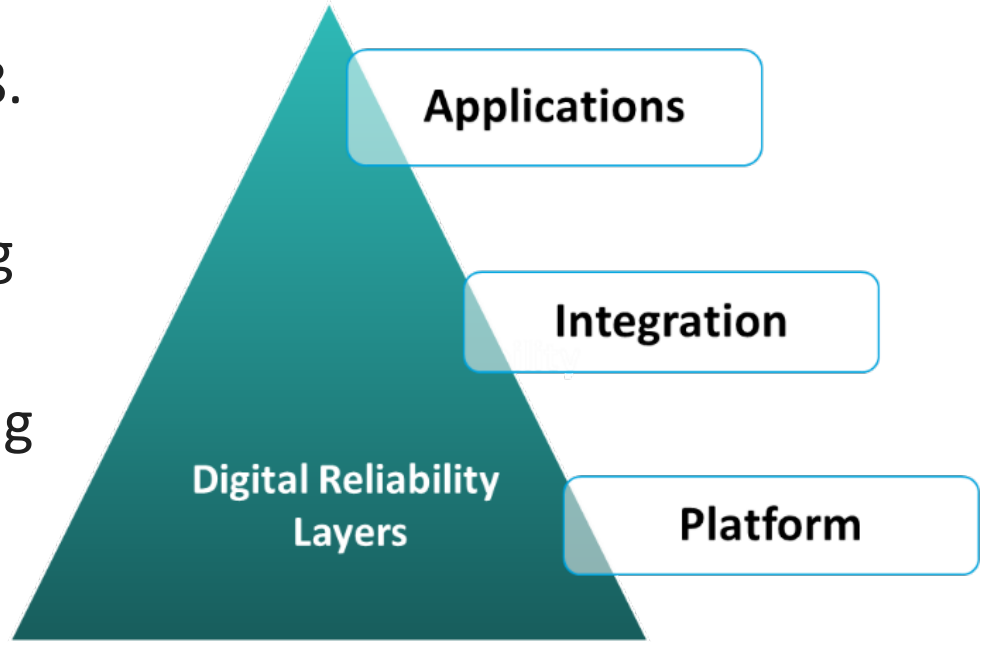


- Developed Preventive and Limiting (P&L) measures based on I&C failure/error modes.
- Developed Safety Analysis and PRA evaluation methods to integrate P&L and risk insights.
- Developed a Safety Significance based graded approach.

- Highlighted the need for more effective hazards analysis.
- Highlighted the need for more effective risk analysis integration.
- Results pointed to a more structured dependability analysis and implementation based on international standards.

Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power- 3002011817

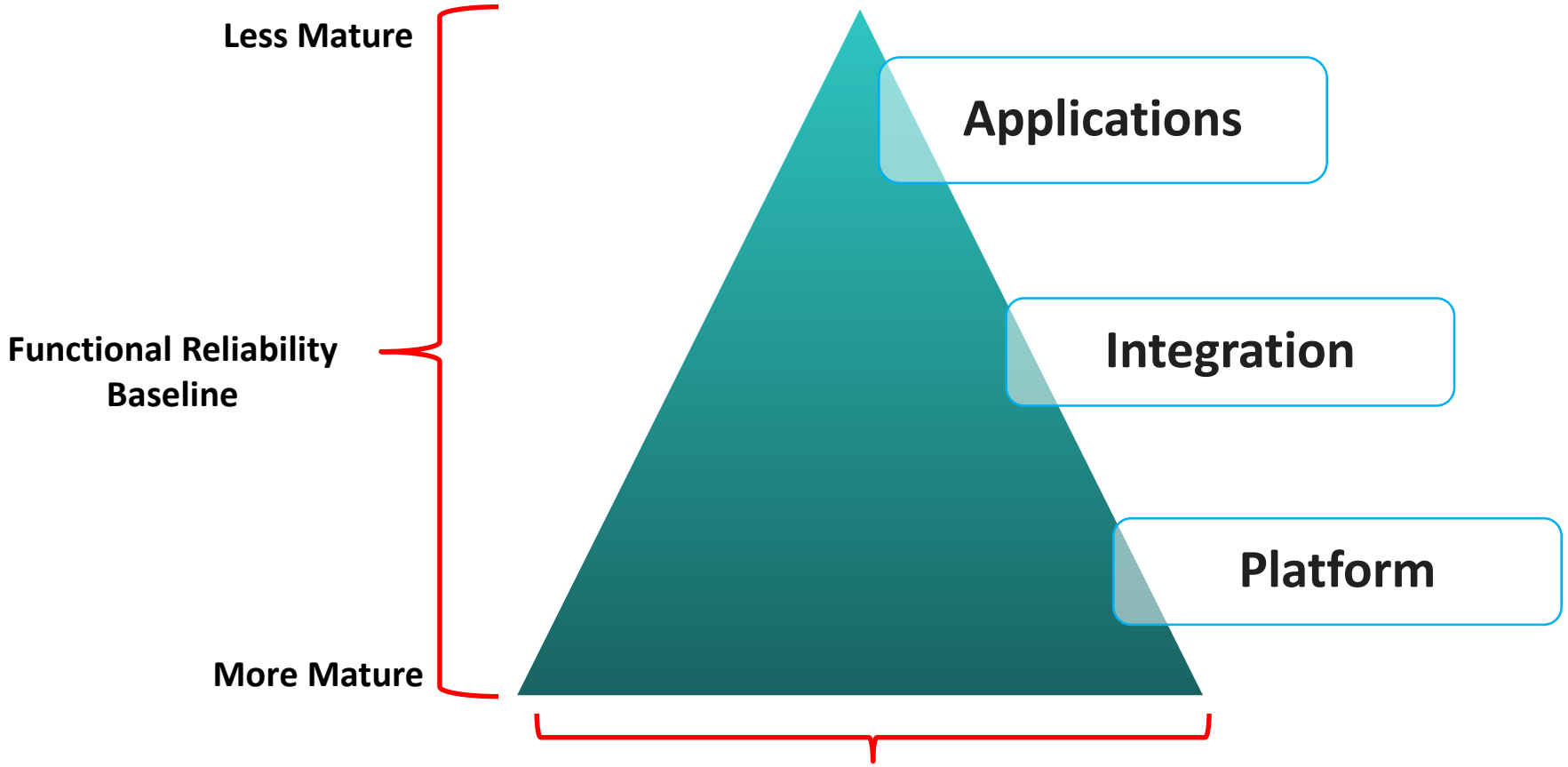
- Studied reliability of platforms certified to IEC-61508.
- Achieved a large data set across 12 safety logic solvers(e.g. PLC's), nearly 2 billion hours of operating data.
- More effective data than traditional OE by controlling for quality.
- Non-nuclear safety platforms proved very reliable, hardware and software, at the ***platform level.***



- **Since SCCF is a subset of all software failures, a high software reliability correlates with a low likelihood of SCCF.**
- **SIL certification has a high efficacy for replacing some existing design and review processes.**
- **Being Leveraged by NEI for MP#3 via NEI 17-06 in US.**

Reliability Layers

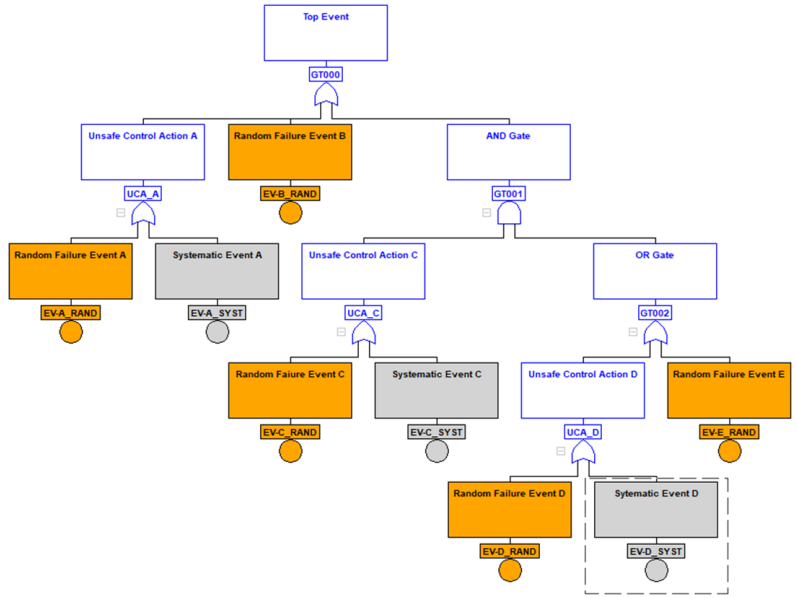
Reliability, especially software reliability, including CCF, should be segmented by *platform, integration, and application*. <u>Then Considered Separately</u>



Production Data and OE Quantity and Quality Dive Maturity and Reliability using IEC-61508/SIL

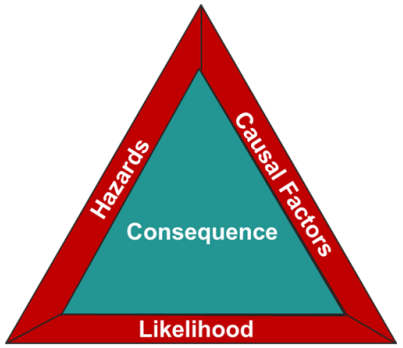
HAZCADS: Hazards and Consequences Analysis for Digital Systems-3002012755

- Advances the use of hazards analysis to identify system and plant level digital I&C design and implementation issues, including CCF and SPV.
- Executed throughout the design and implementation lifecycle.
- Uses System Theoretic Process Analysis(STPA) and FTA.
- Integrates qualitative hazards with random failures with Fault Tree Analysis based sensitivity analysis.



- **Achieves a credible risk informed I&C infrastructure compatible with existing processes.**
- **Dramatically improves hazard detection, resolution, and overall system reliability.**
- **Validated through blind studies and usability workshops.**
- **Used with causal factor analysis methods for a complete reliability assessment and resolution methodology.**

Risk- Informed Process Insights From Blind Studies



Risk Triangle

- **Engineers are Uncomfortable with Probabilities.**
- **Risk Analysts are Uncomfortable with Engineering Decisions.**
- **The blind studies indicate the optimum process:**

Engineering

  - Identify Hazards/Consequences/Losses
  - Identify Causal Factors (DRAM/TAM)
  - Identify Control Measures (DRAM/TAM)

Risk Analyst

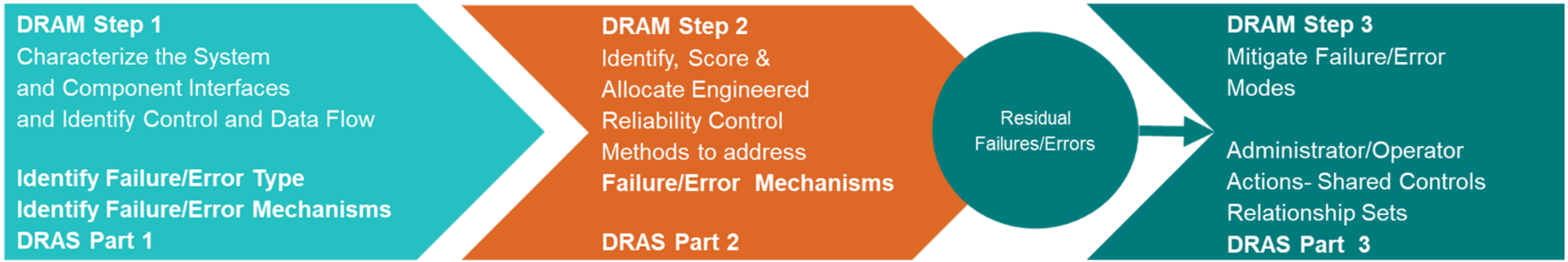
  - Probabilities/likelihood/sensitivity analysis done only if it would provide an ROI with further refinement based on the cost of preliminary control measures

Risk insights can be gleaned from any combination of Hazards, Consequences, or Likelihood.

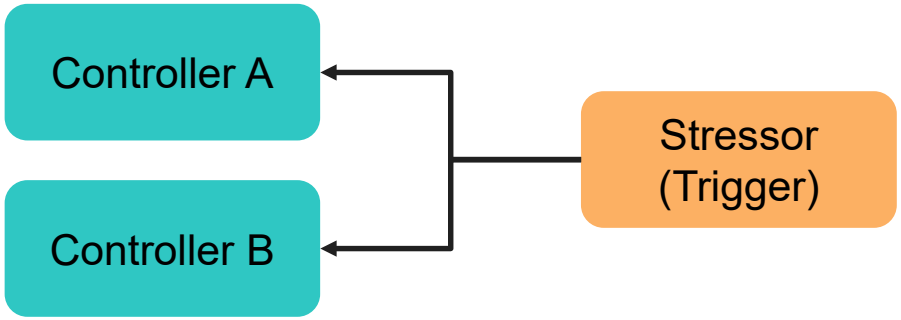
Digital Reliability Assessment Methodology (DRAM) Revision 0

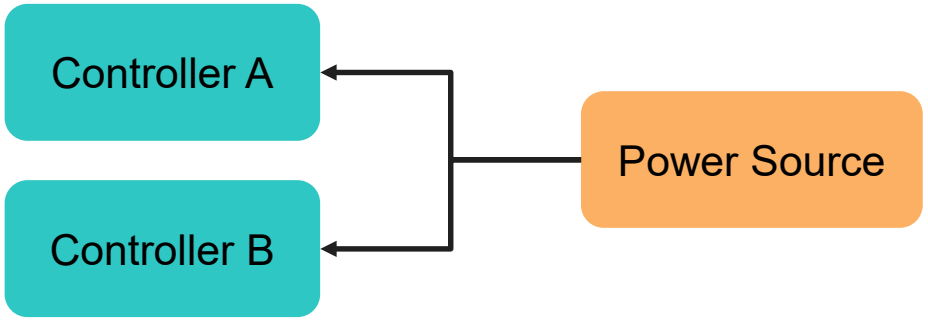
- **Replacement for EPRI 3002005326** - *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems* (June 2016)
  - Development in progress for 2019/2020:
    - Identify, analyze, and resolve digital reliability items.
    - Shift to a hazard analysis based method.
    - P&L measures will become prototypes.
    - Update terminology to match IEC 61508.
    - Integrated into Digital Engineering Guide(DEG).

- **Integration of Hazard/Risk methods**
- **Developed into a field usable methodology**
- **Blind Studies in 2020**



DRAM Software CCF and SPV Type Examples





Software Common Cause Failure

Both Controller A and B must exhibit internal behaviors that negate their design functions. Two failure/errors have occurred, one in each controller. The stressor or trigger must not itself be a failure or error. Likely caused by implicit design or implementation errors. Is systematic.

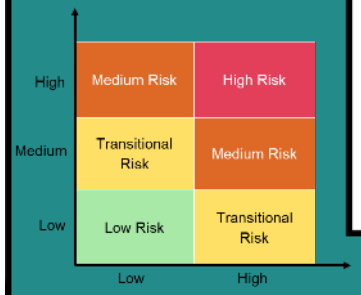
Single Point Vulnerability

Both Controller A and B must exhibit functional failures in their design functions. The Controllers have functioned as designed and are properly implemented. One failure has occurred, loss of a common power source. The stressor or trigger must not itself be a failure or error. May be normal and intended operation. Not a digital problem. Can be systematic or probabilistic.

The EPRI Digital Engineering Guide-3002011816

DEG

Chapter 1 >3



HAZCADS

Risk-Enabled Digital Hazards Identification and Mitigation

- STPA/FTA integration

DRAM

Digital Reliability Analysis Method

Causal Factors

- Systematic
- Random
- Environmental

TAM

Cyber Security Technical Assessment Methodology

- Design Phase
- In-Situ
- Supply Chain

HFE

Human Factors Engineering

- HFE Guide

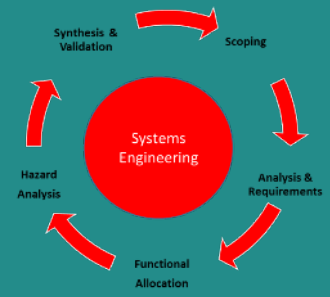
EMCAM

EMI/RFI Graded Methodology

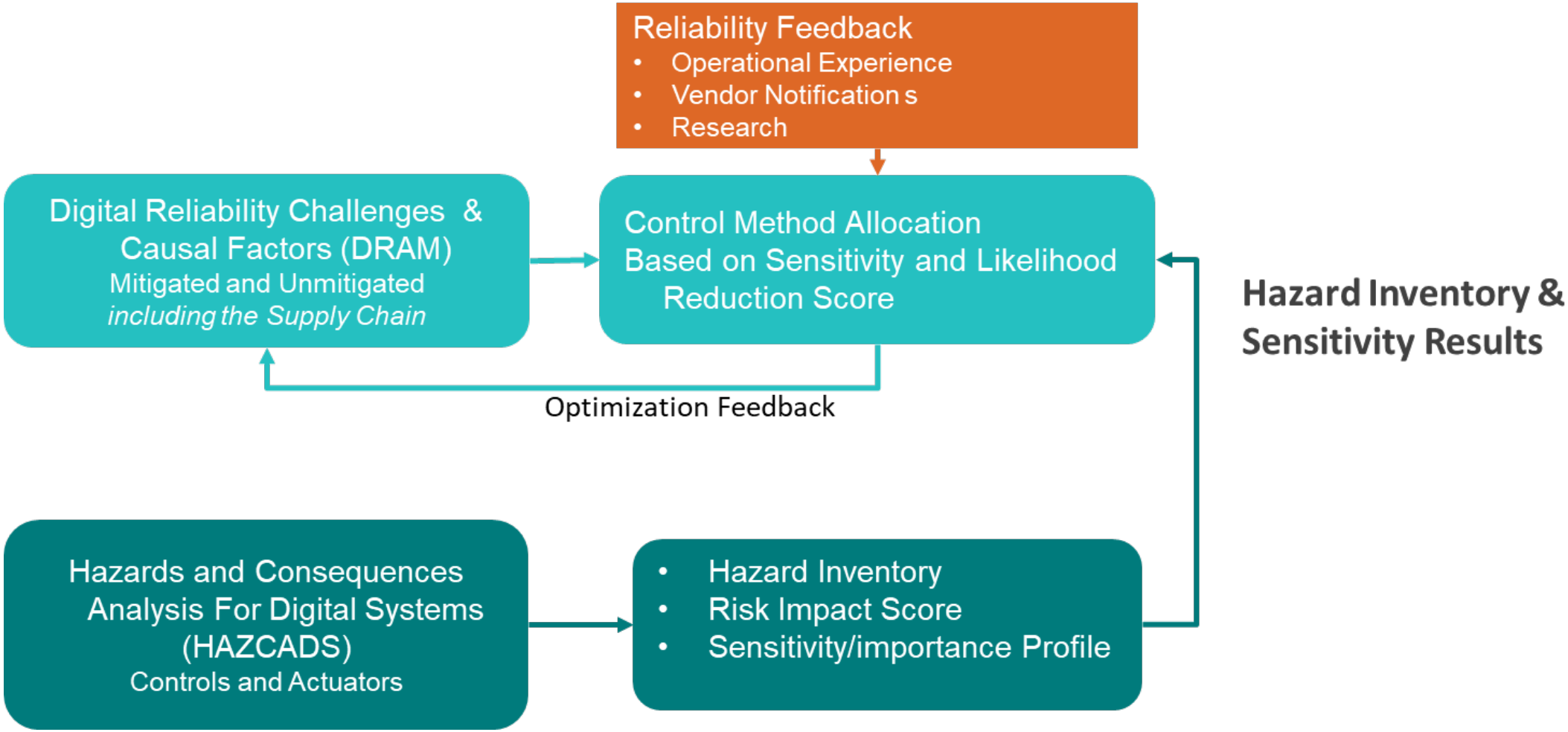
- Identify
- Assess
- Mitigate

. . .

Chapter 4- Systems Engineering



EPRI Risk-Informed Digital Reliability Process Model



Target Reliability based on analyzed hazards, informed by Feedback sources, can dramatically **REDUCE THE SENSITIVITY** of a nuclear facility to the introduction of digital technologies.

EPRI R&D Overall Insights

- ***Software reliability is directly proportional to the systematic controls and design and implementation constraints.***
- ***Software CCF is a subset of total software design and implementation errors.***
- ***Software CCF should be more narrowly defined to improve focus on the actual failure mechanisms of interest.***
- ***An effective Systems Engineering process can ensure digital reliability is considered and resolved at each layer of the design and implementation process.***
- ***Hazards analysis coupled with sensitivity analysis can ensure vulnerabilities are identified, analyzed, and efficiently resolved in the context of overall plant impact.***
- ***Existing non-nuclear safety standards have evolved to a level of completeness, efficacy, and common use that they can enhance I&C reliability beyond that achievable with current nuclear industry methods.***
- ***Existing non-nuclear safety standards can enhance nuclear safety by providing a basis for objective, risk informed criteria for I&C design and implementation.***

Together...Shaping the Future of Electricity

Antonescu, Christina

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Thursday, November 21, 2019 3:10 PM
To: Antonescu, Christina
Subject: [External_Sender] Comments for ACRS meeting

Follow Up Flag: Follow up
Flag Status: Flagged

Christina,
The phone quality is terrible and it keeps cutting out. Below are the comments I would have offered during the public part of the meeting. Please pass them along to the committee members and to the Staff.

1. BTP 7-19 has been limited (and is still limited) to addressing CCF due to software defects. But SECY 93-087 was written to address all new sources of CCF that apply to digital systems that did not apply to analog systems. SECY 93-087 does not limit the new sources of CCF to a software defect. Modern integrated digital systems share numerous resources that are all new sources of CCF – these include digital processors that encompass multiple control or protection functions, and communication networks and soft controls that interface to numerous digital processors. These are all new sources of CCF that did not apply to analog systems, but do apply to modern digital systems. These CCFs can occur due to a single random hardware failure that is much more likely to occur than the triggering of a software defect due to an obscure combination of unanticipated events. Keep in mind that shared hardware resources are identified in the very first paragraph of SECY 93-087 as potential sources of CCF. To revise BTP 7-19 again, without addressing these additional new sources of CCF to the same extent as software defects fails to address the fundamental intent of SECY 93-087, which is to address new sources of CCF in digital systems.

2. This revision to BTP 7-19 differentiates a "D3 Assessment" for A1 systems from a "Qualitative Assessment" for A2 and B1 systems. But the difference is ambiguous. Here are some examples:
    1. For a D3 Assessment, CCF can be eliminated from further consideration through sufficient diversity, testing or defensive measures. "Sufficient" without clear deterministic definitions and acceptance criteria is in fact qualitative.
    2. The D3 Assessment, refers to defensive measures, the Qualitative Assessment refers to design attributes – defensive measures are design attributes. BTP 7-19 does not explain the difference.
    3. The D3 Assessment uses the words "CCF can be eliminated from further consideration", the Qualitative Assessment uses the words "likelihood of CCF is sufficiently low", which also means a CCF can be eliminated from further consideration. BTP 7-19 does not explain the difference. This sounds like legaleze embedded in what is supposed to be technical guidance.

   BTP 7-19 is on revision 8, because it lacked clarity from the first day it was issued. If this ambiguity is not eliminated, revision 9 is certainly inevitable in the short term.

3. For CCFs that cannot be eliminated, SECY 93-087 and BTP 7-19 require an analysis of each event evaluated in the SAR. But the SAR considers all events with a concurrent loss of offsite power (LOOP). For valid technical reasons concurrent LOOP has not been considered in the D3 assessments previously approved by the Staff. On the 8th revision of BTP 7-19, it would seem that we could finally document this valid technical position.

4. Examples of A1 and A2 systems should be provided. If there is any dispute as to whether a diesel load sequencer is an A1 system, then examples should be given to explain when a sequencer would be considered an A1 system and when it is not.

Thank you.

Ken

_____

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192