Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: teleconference

Date: Friday, May 20, 2022

Work Order No.: NRC-1963 Pages 1-175

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL I&C SUBCOMMITTEE

+ + + + +

FRIDAY

MAY 20, 2022

+ + + + +

The Subcommittee met via hybrid Video Teleconference, at 1:00 p.m. EDT, Charles Brown, Jr., Chairman, presiding.

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR. Chair

RONALD G. BALLINGER, Member

VICKI BIER, Member

VESNA DIMITRIJEVIC, Member

WALTER KIRCHNER, Member

DAVID PETTI, Member

JOY L. REMPE, Member

MATTHEW SUNSERI, Member

ACRS CONSULTANT:

DENNIS BLEY

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

ALSO PRESENT:

STEVEN ALFERNIK, NRR

VICTORIA ANDERSON, NEI

NEIL ARCHAMBO, Westinghouse

HAN BAO, Idaho National Laboratory

ERIC BENNER, DEX

ALAN CAMPBELL, NEI

NORBERT CARTE, NRR

MATT GIBSON, EPRI

BAGHWAT JAIN, NRR

SAMIR DARBALI, NRR

SCOTT MOORE, ACRS

WARREN R. ODESS-GILLETT, NEI

CONTENTS

P R O C E E D I N G S

1:20 p.m.

CHAIRMAN BROWN: The meeting will now come to order.

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

ACRS members in attendance are Matt Sunseri, Vesna Dimitrijevic, Ron Ballinger, Dave Petti, Vicki Bier, Walt Kirchner, Joy Rempe, and Consultant Dennis Bley, I believe.

Dennis, are you on? I thought I saw your name.

DR. BLEY: You should have.

CHAIRMAN BROWN: Okay. Thank you.

DR. BLEY: Yes.

CHAIRMAN BROWN: All right. Thank you.

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

Christina, I know the court reporter is on, so I don't have to ask you that one.

The purpose of this meeting is for the staff to brief the Subcommittee on the outline for a Draft SECY paper to allow for consideration of risk-informed alternatives for addressing digital I&C

common-cause failures.

The ACRS was established by statute and is governed by the Federal Advisory Committee Act. That means the Committee can only speak through its published Letter Reports. We hold meetings to gather information to support our deliberations.

Interested parties who wish to provide comments can contact our office requesting time. That said, we set aside 15 minutes for comments from members of the public attending or listening to our meetings. Written comments are also welcome.

The meeting agenda for today's meeting was published on the NRC's public meeting notice website, as well as on the ACRS meeting website.

On the agenda for this meeting and on the ACRS meeting website are instructions as to how the public may participate. No requests for making a statement to the Subcommittee has been received from the public.

Due to COVID-19, we are conducting today's meeting virtually.

A transcript of the meeting is being kept and will be made available on our website. Therefore, we request that participants in this meeting, first, identify themselves, who they are, and if they

represent an organization, to let us know that; and speak with sufficient clarity and volume, so that they can be readily heard.

All presenters, please pause from time to time to allow members to ask questions.

Please also note the slide number you are on when moving to the next slide.

We have the MS Teams phone line audio-only established for the public to listen to the meeting.

Based on our experience from previous virtual meetings, I would like to remind the speakers and presenters to speak slowly.

We will take a short break after each of the presentations to allow time for screen-sharing and changing of presenters, as well as at the Chairman's discretion during longer presentations.

Lastly, please do not use any virtual meeting feature to conduct sidebar technical discussion, but, rather, contact the DFO if you have any technical questions, so we can bring those to the floor.

We now proceed with the meeting. I will ask Mr. Samir Darbali, electronics engineer of the Long Term Operations and Modernization Branch, Division of Engineering and External Hazards, in the

Office of Nuclear Reactor Regulation, to share his screen with us, while Mr. Eric Benner, the Director of the Division of Engineering and External Hazards in the Office of Nuclear Reactor Regulation, will make some introductory comments before we begin today's presentations.

Also, Mr. Bhagwat Jain, known as "BP" normally, Senior Project Manager of the Plant Licensing Branch, the Division of Operating Licensing in the Office of Nuclear Reactor Regulation, will also provide some background information.

With that --

DR. BLEY: Hey, Charlie?

CHAIRMAN BROWN: Yes, Dennis?

DR. BLEY: Yes, just a quick question before we get started. Can you refresh my memory a little. We had meetings and talked about this some time ago. Were we expecting to get a new version here? I guess I would ask the speakers, anything that's really changed substantially to emphasize that, as you go through it.

CHAIRMAN BROWN: You mean a new version of the outline? We do not have a copy of the SECY. That's in preparation.

DR. BLEY: Okay.

CHAIRMAN BROWN: All we have is the outline and the two presentations, or at least the NRC presentation will cover in the slides how they are proposing to address introducing the risk-informed approach, but integrated with the current approach.

DR. BLEY: Okay. Thanks.

CHAIRMAN BROWN: So, I think it's going to be a productive -- it sounds like a productive meeting, and it looks like they responded to our request in terms of how do we identify what we're doing. Okay?

And then, NEI will also be making a presentation, after NRC makes their presentation, with their view of how it should proceed.

Does that answer your question, Dennis?

DR. BLEY: It does. That was very helpful. Thanks, Charlie.

CHAIRMAN BROWN: Okay. Now where am I?

Okay. With that, Eric, would you like to start your comments? And I presume BP is going to be presenting, is that correct?

MR. JAIN: That is correct, yes.

CHAIRMAN BROWN: Okay. Eric, would you like to go ahead and make some opening comments or not?

MR. BENNER: I would. Thank you.

CHAIRMAN BROWN: All right.

MR. BENNER: Thank you, Member Brown.

Your characterization of where we are at in this process is correct. You were, strictly speaking, just provided an outline of the paper, but I think the combination of the outline and the substance in the presentation slides, while you don't have a Commission paper before you, we're going to cover in a fair amount of detail the substance that we are planning on putting into the Commission paper. Now, obviously, we will get feedback through this mechanism and through the full Committee meeting, and we have a public meeting scheduled for June 8th. So, we will assess that feedback to see if course corrections are necessary.

But we think it is time for this. And if you recall, we did a Commission paper in 2018 that said at that time that we didn't believe that the applicable policy which is contained in the Staff Requirements Memorandum to SECY-93-087 needed to be changed because we kind of felt that all the initiatives we had going on, it wasn't an impediment.

Now those initiatives are mostly done. And as we've moved forward, and in addition, with a

proposal we got from industry, we believe it is the right time to take a hard look at that policy and look at how we could better incorporate the use of risk insights.

And we think this has two benefits. One, a more risk-informed approach would be an obvious benefit. The second is, you know, we have all had the discussion about the balance between simplicity and diversity in digital I&C design. So, while diversity is still an important component for addressing software CCF, and certainly, there likely would be situations where we still would require diversity, there may be other situations where requiring diversity is not necessarily the right option because of the increased complexity that comes with that.

So, I think Samir and some of the other staff -- we have a broad set of staff who've been working on the working group for this, and Samir is going to highlight some of those people.

So, we've had people with different skill sets come to this working group to say, what is the best way to incorporate an option for using risk insights, greater use of risk insights, into this policy?

So, with that, I will turn it over to

Samir to kick off the detailed presentation.

CHAIRMAN BROWN: Okay. But, before Samir starts, I would just like -- I did go through your slides. I really appreciated them providing, your staff providing them to us to take a look at, so we would have a sense of where you all were going. Because it wasn't real clear from looking at the outline.

MR. BENNER: That's understandable.

CHAIRMAN BROWN: Okay. And that's not a problem. It's just an observation. And I think the slides provide -- we may have differing opinions in some ways, which we will, but I think that ought to highlight some interesting discussion, as we go through and even at the end.

My intention -- I have hardly any restraint at all during these meetings, as you've probably observed before -- I will try to restrain myself, as I go through, because I think the slides do present a good, complete picture of how you're trying to accomplish it.

Actually, one of my main concerns was losing 7-19 because I don't want to lose that. But, yet, you all addressed that, and how you do it is presented in these slides. And we may have a few

questions on that, but at least the words you had in there say, hey, we're not throwing away the baby with the bath water here, which I think is an important thing to have done.

So, anyway, I'll go ahead and pass on, and I will try to restrain myself. Hopefully, Dennis will also. That's okay, Dennis, do what you want.

MR. BENNER: No, no restraining. We like the rank conversation. We appreciate the feedback from the Committee on previous activities.

CHAIRMAN BROWN: Okay.

DR. BLEY: We can go to that when you speak for yourself, Charlie.

(Laughter.)

CHAIRMAN BROWN: I have a hard time, as you're well aware of.

So, go ahead. Samir, you have the floor.

Thank you, Eric.

MR. BENNER: Thank you.

MR. JAIN: This is BP, then. I will introduce --

CHAIRMAN BROWN: Oh, BP, I'm sorry, I forgot. I knew you wanted to do some intro also.

MR. JAIN: Yes, yes.

CHAIRMAN BROWN: Go ahead.

MR. JAIN: Yes, yes.

Well, good afternoon, Charlie and everybody else.

My name is BP Jain, and I'm the Senior Project Manager in NRR's Division of Operating Reactor Licensing. Along with Michael Marshall, we perform the project management of all things digital in NRR.

In today's meeting, the NRR staff will present an outline of a SECY paper on potential expansion of the current policy regarding CCF in the digital I&C system.

Today's presentation is led by Samir Darbali and is supported by Steve Alfernik and Norbert Carte.

Norbert will present and discuss the current path and the staff-proposed expanded CCF. But, as you can see, the SECY paper is a collaborative effort of several -- next slide, Samir -- yes, it's a collaborative effort of several NRR Divisions and the Office of Research and the Office of General Counsel.

Samir, the lead presenter, is I&C tech staff in the Division of Engineering and External Hazards, the DEX. Mr. Darbali is highly experienced, as you know, in licensing and inspection of digital I&C upgrades. He led the Division in Interim Staff

Guidance, ISG-06, and has made a significant contribution to organize the agency's digital I&C regulatory infrastructure.

Norbert, who will be presenting as well, he's a Senior I&C Tech Staff Reviewer. He has a wide range of nuclear and non-nuclear industry experience in licensing and modification of the digital I&C system. Norbert will present and discuss the current path in the staff's proposed expanded CCF policy.

The third presenter who will assist Samir is Dr. Steve Alfernik. He's a Reliability and Risk Analyst in the Division of Risk Assessment. He's an expert in risk assessment and is experienced in risk-informed methods to support resolution of regulatory issues. He will present and discuss the risk-informing aspect of the staff's proposed expanded CCF policy.

Now, with that, as we said before, the staff is requesting the Committee's feedback on the staff's proposed expanded CCF policy, and we look forward to your comments and engagement.

With that, I will turn to Samir for his presentation.

Samir?

CHAIRMAN BROWN: Before Samir starts, in

response, I do have a few thoughts on how you do your implementation, but it's in line with what you all are doing and I will save those for the end, so that they're just compacting in one place in the transcript.

So, we should go ahead and get started. I just wanted to let you know that, as you probably suspected, I am not without thought processes here.

MR. JAIN: Thank you. Thank you, Charlie.

CHAIRMAN BROWN: Okay. No, thank you. Appreciate it.

MR. JAIN: Samir?

MR. DARBALI: Okay. Thank you.

So, this slide shows the topics that we'll be presenting today. We'll cover the key messages; the background of our work activities; the subject and purpose of the Draft SECY paper, and the proposed expanded policy that allows for following the current path or a risk-informed path. And we'll end with a status update on the Draft SECY paper and the next steps.

I am now on slide 5.

As we all know, nuclear power plants continue to replace aging I&C safety systems with modern digital I&C technology. While digital I&C

technologies provide increased reliability and safety benefits, they can also introduce new types of potential systematic and non-random concurrent failures of redundant elements; also known as common-cause failures or CCFs.

SRM-SECY-93-087 describes the NRC position on defense against potential common-cause failures and digital I&C systems. And we recognize that the SRM and the SECY both use the term common-mode failure, and we'll talk about these in a later slide.

The SRM directs that, if the defense-in-depth and diversity assessment show that a postulated CCF could disable a safety function, then a diverse means, which may include manual actions, shall be provided to perform that safety function or a different function.

Now the staff has been expanding the use of risk-informed approaches as much as it is allowed by SRM-SECY-93-087. However, this SRM, which we recognize is about 30 years old, does not allow for the use of a risk-informed approach to determine specific circumstances that would not require a diverse means for addressing digital I&C CCF.

Because of this, the staff is developing a SECY paper that will provide recommended language

for an expanded policy which allows for greater use of risk-informed approaches to address digital I&C CCF for high safety-significant systems.

I am now on slide 6.

So, this slide shows the key messages for the staff's work to expand the policy. The proposed expanded policy will encompass the current points of SRM-SECY-93-087 with clarifications and expand the use of risk-informed approaches. And the use of risk-informed approaches will be expected to be consistent with the Commission's safety goal policy statement; the Commission's PRA policy statement, which provides the Commission's direction on the use of PRA methods in regulatory matters, and SRM-SECY-98-144, which provides the Commission's expectation and definition of key terms for risk-informed and performance-based regulations. And finally, the current underlying CCF policy will continue to remain a valid option for licensees and applicants.

I am now on slide 7, and we'll discuss some background information.

So, consideration of the possibility of CCFs in the design protection system has been an NRC concern since the mid-1960s. In the late 1970s, the NRC started receiving applications that included

digital I&C as part of the protection systems, which differ significantly from the analog systems previously used.

In the early 1990s, digital I&C rose to a new level of concern as a new source of potential CCF. SECY-91-292 explained the staff's concern regarding the use of digital I&C in evolutionary and advanced light water reactors.

The NRC's current digital I&C CCF policy is expressed in various documents, which include SRM-SECY-93-087, SECY-18-0090, and BTP 7-19, the latest revision being Revision 8.

Again, the staff recognizes that SRM-SECY-93-087 was issued almost 30 years ago, and since then, there have been many advances in the digital I&C design development practices and quality assurance tools. Given that, digital I&C CCFs still remains an area of concern.

I am now on slide 8.

So, the current effort is being driven by the agency's move towards being a modern, risk-informed regulator. And so, the staff is following the 1995 PRA policy statement and the SRM-SECY-98-144.

This work is also part of the agency's effort to modernize the digital I&C regulatory

infrastructure. As I mentioned earlier, the staff has been expanding the use of risk-informed approaches as much as it is allowed by SRM-SECY-93-087.

As part of the Digital I&C Integrated Action Plan, the staff issued guidance in BTP 7-19, Revision 8, and RIS 2002-22, Supplement 1, on risk-informed graded approaches to address digital I&C CCF for low safety-significant safety systems.

The staff believes that this is an appropriate time to expand the current policy on the underlying CCF to include the use of risk-informed approaches for high safety-significant safety systems.

So, I am now on slide 9, which covers the subject and the purpose of the SECY paper.

The subject of the SECY paper is "Expansion of Current Policy Regarding Potential Common-Cause Failures in Digital I&C Systems" --

DR. BLEY: Samir?

MR. DARBALI: Go ahead.

DR. BLEY: This is Dennis Bley.

Not to be argumentative, but in that history you just went through, it wasn't so much a characteristic of digital I&C systems common-cause failure, I think, but that, with the digital I&C systems, we were seeing levels of integration of

controlling safety systems that we never saw before, such that common-cause failure could affect many more parts of the plant at one time. I think that was really the concern that drove it.

What do you think about that?

MR. DARBALI: That's correct, Dennis. We agree with that.

Any other questions, comments?

CHAIRMAN BROWN: Yes. Me.

I wanted to expand on Dennis' comment because he's right on the mark.

Just to provide a mental calibration, if you can think about it this way, in the analog systems, each and every instrument had its own channel with a detector, an amplifier, and then, it fed some information out to meters and/or a voting unit of some kind -- normally, relays.

In a typical plant -- and I will pick on plants I know -- you could have up to four or five pressure detectors, four or five level items for -- sometimes, depending on how much you wanted, you had four or five temperature between cold and hot legs. Then, you had level detectors, where you also had to integrate those into the system. So, you, effectively, had somewhere in the neighborhood of 30

to 40 defense-in-depth, independent items.

I will tell you, when I had to start introducing this into the Navy program -- and this is not naval nuclear propulsion information at all; it's strictly in the design-type stuff -- we had to make a decision, how do we start out? And we made the decision to literally just take out the amplifier and put in a microprocessor. That's all we did.

So, we still had 30 or 40 independent paths, which, then, could send out, actually, a hardware-based, fast-able-type up, you know, high or low signal to a voting unit. No voting units were microprocessors -- with one exception, but that's a side point, another project.

So, Dennis was right on because now, after we did that first project, another project came along, and we had to figure out how we now know what we did and how do we integrate, you know, go down to four divisions, similar to what you have in the commercial world or what you're looking at with the integration of processors.

So now, you've got four major paths, and the only way you can complement that is by having independent detectors for each of those divisions, which, then, provides you some additional defense-in-

depth. And by running those asynchronously, so that they're not timed the same, you have an additional path, that not everything's being processed the same in every channel going through it. So, there's a lot of delays.

So, the point there comes at, what are the vulnerabilities once you integrate? And you have to kind of figure out, where is the problem with the integration? And the real problem with the integration now, you've got better algorithms, you've got all the other better stuff you can do, but some improvements even that that integration brings you.

And fundamentally, if you look at it, the biggest efficiency with the processors is they can lock up, based on corrupt data, or if you have an interrupt-driven microprocessor, you never know what it's doing. And you might be in the process of doing something and it stops and runs off somewhere; it doesn't come back because it gets confused. Just like when you move your mouse or your touchpad, and all of a sudden, the pointer's not moving anymore, the only way to recover is turn everything off.

And so, you bring in the thought process of watchdog timers, such that, if you don't complete a cycle within 100-200 milliseconds, it resets

everything automatically. Sometimes it's more than that time, depending on the nature -- it depends on how much complex software you have. Today's commercial software can take, as we've known on one project, 5 to 10 minutes to reset.

And if you have a simple software operating system where you don't have all the stuff branching up and doing stuff you don't need to to meet a commercial need, you can do it in the matter of 200 to 300 milliseconds, which is consistent with analog equipment.

So, those were the major real failure modes that you had to look at and how you address. Now we came down in terms of looking, there was no way, even with our resources, of making sure that every line of code, which we did examine, was going to be perfect all the time and not have some glitch somewhere.

So, the diverse thought process rolls into the picture about that point. So, from our standpoint, we understood -- and we were looking at what the commercial world was thinking about when they just came in, although they didn't do much back in the late seventies and early eighties; whereas, we did.

So, how do you introduce that diversity is

an interesting thing. We've at this point -- and I'll just introduce this now -- we've had four new design projects: AP1000, APR-1400, NuScale, and Diablo Canyon.

The struggle on AP1000 was a struggle because there was very little detail.

On APR-1400, or on Diablo Canyon rather, I guess they springboarded from some of the stuff we did, and they came in. It was pretty simple, very straightforward, easy to understand.

APR-1400 was more complex, much more complex. It had a lot of diversity in it --

Can somebody turn off their mic in the background? Thank you.

Who is that, anyway?

MR. BENNER: It looks like Aaron Green. Can you mute your mic?

CHAIRMAN BROWN: He's obviously on the phone.

Thank you.

I lost my train of thought here. Where was I?

MR. DARBALI: You were going through the past examples, I think --

CHAIRMAN BROWN: Oh, yes, yes.

DR. BLEY: You were on 1400.

CHAIRMAN BROWN: Oh, APR-1400, I said it works nicely, but it is more complex. There's a lot of diversity in there.

NuScale took a separate thing with the FPGAs and were able to simplify the amount of diversity they have -- much more straightforward, and you don't have "software software." It's literally you program it and it's burned in, depending on how you want to look at volatile and non-volatile Field-programmable Gate Arrays.

So, I guess I'm just trying to get people to think about bearing that in mind, that diversity is all in the eyes of the beholder. You can go overboard or you can use a design approach that really ends up -- and that's about all they have. But it went through the design, your all's approval process, and the ACRS review -- APR-1400 and NuScale and Diablo Canyon -- through the Subcommittee, one full Committee. Everything was approved.

Very, very smooth, because they took what we talked about in ISG-06, when we started to introduce the focus on the architecture. It's got to be the lead-in on all of these. You can't do defense-in-depth; you can't diversity, without having a well-

defined architecture.

And when I saw your all's proposals, that's what I was worried about, that we would somehow deviate and move away from the thought process of how we start.

So, anyway, that's just a little background of my thought process.

So, I'll let you go on now. Please go on. Thank you for bearing with me.

MR. DARBALI: I appreciate the background, Chairman, because I think you characterize very well that each common-cause failure and how it's addressed has been done in different ways in the last 30 years. And so, that's one of the things we've been considering as we've been working on expanding the policy. So, I appreciate that.

CHAIRMAN BROWN: We did do that in the naval nuclear program, but I can't tell you how we did it. That's classified. And it worked. And it was very simple.

All right. Go ahead. I'm sorry.

MR. DARBALI: Yes, thank you.

So, we were going through the purpose of the proposed SECY paper or the Draft SECY paper, which is to provide the Commission a recommendation on

expanding the current policy to include the use of risk-informed approaches for addressing digital I&C and CCFs.

This recommended expanded policy will encompass the current position in SRM-SECY-93-087 and the use of risk-informed approaches to determine the appropriate level of defense-in-depth and diversity to address digital I&C CCF.

We're now on slide 10, to discuss the proposed expanded policy.

The staff is proposing a single expanded policy that will include the current position in SRM-SECY-93-087 and provides for risk-informed approaches. The expanded policy includes the position in points one, two, and three of SRM-SECY-93-087 with appropriate clarifications and corrections from SECY-18-090. It will also include the position in point four of SRM-SECY-93-087 with appropriate clarifications, and will include the addition of risk-informed approaches to points two and three. This expanded policy will provide for the deterministic demonstration of adequate diversity and the flexibility to use risk-informed approaches.

And in the next slide, I will show some --

DR. BLEY: Samir?

MR. DARBALI: Go ahead.

DR. BLEY: May I ask you -- this is Dennis again.

As you were doing this work, did you look at all at the NEI document on the LMP about how they look at those same issues?

MR. DARBALI: Are you referring to NEI 20-07?

DR. BLEY: No. It's something 04.

MEMBER PETTI: NEI 18-04.

DR. BLEY: 18-04, yes.

MR. DARBALI: 18-04? I don't recall. If somebody in the working group --

DR. BLEY: Okay. It's, essentially, a plan for doing a risk-informed approach to licensing. But, in there, they looked at the issues on diversity, and a couple of other things you mention in your last slide, in ways that it combined both administrative and technical thoughts that probably should factor into your paper. I think it would be helpful. Anyway, something you can look at.

MR. DARBALI: Yes, I appreciate that. Thank you.

Okay. So, the next slide will show how the proposed expanded policy will look, and that's on

slide 11.

So, this figure represents the proposed expanded policy. Again, it's composed of four points that provide for two paths to address digital I&C CCF. The text itself in the points will read as four points -- one, two, three, and four. And points two and three will allow for the option to follow the current, the deterministic path or a risk-informed path.

So, on the left in green is the current deterministic path. Again, it's made up of the four points of SRM-SECY-93-087 with some clarifications. And this path allows for the use of best estimate analyses and diverse means to address a potential digital I&C CCF.

On the right, on the orange-peach color, is the risk-informed path, which incorporates points one and four of SRM-SECY-93-087 with clarifications, and provides in points two and three for the use of risk-informed approaches. The risk-informed path allows for the use of risk-informed approaches and other design (audio interference) or measures of the diversity to address a potential digital I&C CCF.

Again, the text will read as four points.

Any questions?

MEMBER PETTI: Yes, just to clarify in my

mind, so this risk-informed path is sort of a thought process similar to 50-69 where one's looking at risk and delta risk to kind of make sure that you've got adequate protection against CCF, but not excessive protection, where you've got, you know, very little increase in risk, and so, you don't need it? So, it helps to balance your design space in a sense to optimize your solution relative to overall risk?

MR. DARBALI: Right. And Steve will cover the details of points two and three in the following slides.

MEMBER PETTI: Oh, great. Great. Thanks.

MR. DARBALI: Yes. Sure.

And again, after this slide, I'll be turning it over to Norbert. He'll be covering the current path, and then, Steve will cover the risk-informed path.

Okay. So, I'll now turn it over to Norbert.

MR. CARTE: Next slide, please. Let's go to slide 13.

So, I'm Norbert Carte, an I&C Technical Reviewer in the Office of NRR. I've been working in NRR for almost 20 years doing licensing of digital I&C systems.

So, as was stated many times previously, we intend to leave the current path in place and as a viable option. And that current path consists of four points and some guiding principles in SECY-18-090.

The four points are, basically, that you will assess the defense-in-depth and diversity of the I&C system; a particular manner in which you'll analyze the impact of common-cause failure -- that is, you postulate the common-cause failure in the presence of a design basis event using best estimate methods. If the CCF could disable a safety function, then the diverse means is required. Finally, the fourth point is that you would have a diverse set of displays and controls.

Next slide, please.

So, one of the things that happens -- and I'll touch a little bit on Charlie's point here; it's a little bit of a deviation -- but, in essence, the whole licensing approach that we have was envisioned in the 1960s, and it was based on a simple set of siloed systems. And in that sense, looking at diversity within a particular echelon, like the I&C, within a particular context, is appropriate.

However, once you start changing your system design or systems of systems design, it may no

longer be appropriate to look just at diversity within a particular echelon, and maybe you want to look at the big picture. And that's kind of why we're looking at doing risk-informed. But that's just addressing Charlie's point a little bit.

Next slide, please. Slide 15.

So, what we're doing is we are providing some clarification of the current policy language. We're not trying to change anything. We're trying to reflect how it's being implemented today.

So, we use the term "common-cause" rather than "common-mode" failure, predominantly. As mentioned with respect to Charlie's point, we want to emphasize that the facility is adequately protected, not that there's adequate diversity within the I&C equipment. There's maybe a little nuance there. And again, we're adding defense-in-depth, where appropriate, to focus on it's the defense depth and diversity of the facility that needs to be ensured to be adequate to provide reasonable assurance of adequate safety.

Next slide, please.

Okay. So, I'll discuss the risk-informed path a little bit.

Well, points one and four are the same.

So, I'll talk about those.

So, next slide, please. We're now on slide 18.

So, right now, the current policy is that you will assess --

CHAIRMAN BROWN: Norbert, could you back up again, please, to 15?

MR. CARTE: Okay.

CHAIRMAN BROWN: Bullet one is fine. Okay? I guess bullet two is where -- it focuses on proposed -- I guess would argue a little, not argue, have a slightly different viewpoint. Right, the current language focuses on the proposed I&C system; that it's the diversity in that system which is used to ensure that you have defense-in-depth within the facility.

I mean, diversity, I don't know what you mean by "diversity of the facility." I mean, you've got --

MR. CARTE: Well --

CHAIRMAN BROWN: Let me finish quick.

I mean, you've got diversity in depth. You've got multiple -- just use an LWR as an example, okay, because that's what we're familiar with right now. You've got multiple trains of safeguards.

You've got multiple trains of reactor trip functions. So, those are defense-in-depth approaches, but in order to make sure they work, what was being done is you had to have some diversity within those in order to get there and make sure the reactor was safe.

So, I struggle a little bit with changing, you know, adding the word "facility" in there, because I'm not quite sure how this defense-in-depth and diversity of the facility, you know, how do you incorporate that into the I&C system? That, I struggle with it. I'm just telling you that right off the bat.

MR. CARTE: Well, right. So, part of the thing which gets difficult here is sometimes the words are used by different disciplines in different manners. So, if you talk to the PRA guys, defense-in-depth includes redundancy and diversity. But if you talk to the I&C guys, we think of redundancy as something separate and diversity is something separate from defense-in-depth.

But the idea of that particular phrase, defense-in-depth at the facility, we want to make sure that the facility is adequately protected. And there will always be some required diversity. 603 and 279 both require a manual actuation of a system-level

actuation, push button. So, you will always need to have the -- the operator will always have the ability, unless they take an exception to 603 or 279, to manually initiate a protective function.

The real question is whether there's sufficient time for the operator to do that, and whether a diverse automatic means is also necessary. So, there will always be diversity. But the question is, when do you need automatic diversity to initiate a protective function?

And we want to encourage looking at the overall facility rather than just -- well, the current philosophy is for a certain set of plants and a certain design scheme, then you make sure you have a certain level of diversity within the protection system.

You may want, for other designs, you may want more diversity or you may want less diversity. For instance, it's been explained to me that the CANDU reactor has a positive power coefficient. And they have two triple-redundant diverse trip systems because they feel they need more diversity than we have. But that's because they have a positive power coefficient.

Now, some plants in the U.S. do have positive power coefficients during a limited range of

operation, but, predominantly, they weren't designed that way. So, you may want more diversity and, given the inherent safety of the facility, you may want less diversity.

So, it's diversity in the context of defense-in-depth to ensure the facility is adequately protected. And I think that's what we're trying to adopt in the risk-informed approach. We're trying to allow for that.

So, by allowing the current approach, that is always acceptable. But if you're going to radically different designs, then maybe you have a risk-informed approach that looks at the bigger picture.

CHAIRMAN BROWN: I don't disagree with -- well, let's put it this way: I agree with your -- not that I don't disagree, since that's a double negative -- I agree with your thought process. But you've commented that defense-in-depth and diversity are different. I, actually, have always viewed diversity as an element of defense-in-depth because there are parts -- you can develop a defense-in-depth design, but, yet, when you look at it, there may be an element where you have some concern, such as replacing all the amplifiers with microprocessors, not using a main

operating loop processing systems, where it's a fixed time, always does it, and there's no interrupts, zero interrupts, and then, you substitute interrupt systems where you never know when the system is going to come back to the main path, or it may lock up and get confused.

So, those are all defense-in-depth paths, but, yet, in order to make the defense-in-depth path work, we've introduced diversity into the individual divisions to ensure that you're okay.

So, I'm just quibbling a little bit with the idea that diversity is not an element of defense-in-depth, because I think it is an element. I'm not saying you can't do without -- I can make a design, I can make an assumption and do a design, and actually made those decisions at one time, did we want to continue doing what we were doing for a diverse trip function? And we decided to do it anyway.

Even though we didn't think we had a problem, based on the design and the elements of the design, and the depth of the defense-in-depth, if you want to call it that, but we went ahead and did what we had been doing otherwise because it was a good idea. So, I mean, that's --

MEMBER DIMITRIJEVIC: If I can add from

the PRA perspective, because it was very well said by the presenter.

From the PRA point of view, having three breakers is not diversity; it's redundancy. Diversity would be if they're made by different manufacturers; they're in a different location; you have different maintenance, you know, use different lubricants. That's diversity.

CHAIRMAN BROWN: I agree.

MEMBER DIMITRIJEVIC: So, PRA has a slightly different, obviously, terminology. So, diversity is there to prevent the common-cause failure. Redundancy is number of available trains. So, both diversity and redundancy contribute to the that.

CHAIRMAN BROWN: Yes, I totally agree with you, Vesna. I don't disagree.

And I can tell you that there were designs where the diversity we cranked in, it was a totally different setup. And it's, actually, that mode of operation is actually implemented in one of the project designs that we looked at.

MEMBER DIMITRIJEVIC: Right.

CHAIRMAN BROWN: So, I mean, it was like having two different design breakers.

MEMBER DIMITRIJEVIC: Right, right.

CHAIRMAN BROWN: Okay?

MEMBER DIMITRIJEVIC: No, I was just referring to the slight differences in the terminology between the PRA folks and the --

CHAIRMAN BROWN: Yes. No, that's good. I appreciate that. I appreciate that.

And I agree with you. Two different design breakers is diversity. Having two or three breakers of the same design is not diversity. It's defense-in-depth. I totally agree with your -- if that's the way you think or the PRA people think. That's the way I think, also.

MEMBER DIMITRIJEVIC: And I said redundancy. Defense-in-depth is both. You have to have redundancy and it has to be diverse.

CHAIRMAN BROWN: Yes, I agree with you.

Okay. Go ahead, Norbert.

DR. BLEY: No, I'd like to interrupt. I'm sorry.

CHAIRMAN BROWN: Oh, go ahead, Dennis. Go ahead.

DR. BLEY: Norbert, you and maybe both the previous speakers have over and over again talked about SRM-SECY-93-087 and points one, two, and three.

And when I look through SRM-SECY-93-087 and its attachment, I'm not quite sure what you're talking about. The nice diagram we had in the previous talk would have made sense if I really understood what points one, two, and three were. Can you give me a short description? Because I don't see them jumping out at me.

MR. CARTE: Can we go to slide 13, Samir?

So, points one, two, three, and four -- in essence, point one is the applicant "shall assess the defense-in-depth and diversity of the system." So, it's really an overarching requirement to do an assessment.

And point two is, in that assessment, they shall analyze -- it's the process for doing the assessment -- they'll analyze each common-mode failure in the presence of each design basis accident using best estimate methods.

DR. BLEY: Okay.

MR. CARTE: And then, point three is sort of the acceptance criteria that, if a CCF could disable a safety function, then a diverse means with a documented basis that it is diverse is required.

And point four is a set of operator displays and controls are needed that are diverse and

independent from the automatic system.

DR. BLEY: Okay. I know we went through this before, but we went kind of fast, and I didn't remember them. And when I looked over the SECY, they didn't jump out at me. So, I guess they're in there somewhere.

MR. BENNER: Yes, Dennis, this is Eric Benner. We can get you that. It's in an attachment.

DR. BLEY: I've got the attachments. I was looking through it. But it didn't jump out clearly at me.

MR. BENNER: Yes, it's 18.II.Q.

DR. BLEY: II.Q. II.Q.

MR. BENNER: Yes, "Defense Against Common-Mode Failures in Digital Instrumentation and Control Systems."

DR. BLEY: Ah, okay. Thank you

MR. BENNER: And then, there's four points under there, and that's the four points we refer to. So, you know, shame on us for not making it painfully clear where it is in that document.

DR. BLEY: Well, that's a big document and --

MR. BENNER: Yes, yes, yes.

DR. BLEY: And they're not even numbered,

you know, when you get over to that document, but they're there.

Okay. Thank you.

MR. BENNER: Okay.

MR. CARTE: And, Vicki, you have your hand up?

MEMBER BIER: Yes. I just wanted to expand briefly on Vesna's point which I thought was excellent.

And, in particular, one of the things that I haven't heard discussed that may at least sometimes be applicable is spatial separation. Obviously, sometimes if you're trying to sense a certain thing, there's only one place you can put the sensor or the control, or whatever. But there are circumstances where putting a device in a different location could reduce the risk of high heat or dust, or whatever. And is that relevant to this or not really?

MR. CARTE: It's not necessarily relevant to this particular policy. So, in reality, what happens is the current plants have their sensors in the current locations. So, we're not going to change that.

In new plants, 603 does require separation in order to achieve independence. So, separation is

one of the criterias to achieve independence, but that's not really what we think of in terms of diversity.

MEMBER BIER: Yes. Okay.

CHAIRMAN BROWN: Vicki, the separation -- correct me if I'm incorrect, Norbert -- I thought on one of my visits I was at the one plants and they actually had parts of the I&C system in different rooms to separate them, so that they couldn't both be taken out with fire.

MR. CARTE: Some of the facilities have that, yes.

CHAIRMAN BROWN: Yes. Okay.

MR. CARTE: AP1000 I think has that. Oh, no, I mean APR-1400 has that; I know that.

CHAIRMAN BROWN: Yes.

MR. CARTE: I just forget which facilities do.

But one of the problems is that they all, in general, the cabinets end up being in the control room in the end, anyway.

CHAIRMAN BROWN: Yes.

MR. CARTE: Part of all core divisions.

CHAIRMAN BROWN: That's what I've seen, based on what I've seen in most of the new

applications. It's they're all up -- they're separated. They're behind all the maintenance -- they're in a little separate area, but they are virtually next to each other. If the control room goes out, they go out.

MR. DARBALI: Digital I&C common-cause failure, that's a hardware aspect. And that's not changed, and that physical separation or hardware common-cause failure is addressed in other documents.

CHAIRMAN BROWN: That's correct. Thank you for reminding us.

Is that okay? Are you good with that, Vicki, for right now?

MEMBER BIER: Yes. No, I appreciate the explanation. I just wanted to raise that as a point.

CHAIRMAN BROWN: That's fine. That's the purpose of the meeting here -- to get everybody on the same page.

MR. CARTE: Samir, can we go to slide 15 again?

Vicki, your hand is still up.

MEMBER BIER: Sorry. Thanks for the reminder.

MR. CARTE: Not to belabor the point too much.

The difference between -- I agree with what you said about diversity and being part of defense-in-depth. It sometimes is sort of a pragmatic issue.

So, the reason we sometimes think about them differently is, when someone is replacing a particular system, we don't really reevaluate the other echelons of defense at the facility. We're just looking that particular replacement system and whether diversity is needed.

So, in that sense, we're not evaluating, reevaluating the defense-in-depth of the facility. We're just evaluating whether diversity is needed for this particular set of equipment. So, in that way, that's how we come to think of it as different things.

But, yes, I agree that defense-in-depth is a philosophical mindset when you approach any problem. And it's approached at the facility level, and then, also needs to be addressed within the I&C equipment at the I&C level.

But, yes, all right. That's kind of why we sometimes talk about it differently, though. But let's --

MR. DARBALI: Yes, if I could add to that?

So, another reason why we focus on the

facility is, if the facility already has another diverse system which could be ATWS, it could be credited. Then, that could be credited as diverse to the digital I&C safety system. And so, that's, in a sense, why we look at the defense-in-depth and diversity of the facility with the incorporated digital I&C system.

CHAIRMAN BROWN: Manual scram also falls into that category.

MR. DARBALI: Correct. Timely manual actuation also falls --

CHAIRMAN BROWN: Okay. You can proceed, Norbert.

MR. CARTE: Next slide, please.

MR. DARBALI: Eighteen.

MR. CARTE: Fifteen to 18. Okay. I forgot what --

(Laughter.)

MR. DARBALI: Yes, I'll show what we skipped.

CHAIRMAN BROWN: What happened to 16?

MR. DARBALI: Sixteen is risk-informed path.

CHAIRMAN BROWN: Oh, there it is. So, you're on 17 now, right?

MR. CARTE: Right. And so, we're now transitioning into the risk-informed path, but we're actually going to talk -- I'll talk a little bit about points one and four, since they're the same. And Steve will, then, talk about points two and three.

So, we believe point one does not preclude the use of the risk-informed approaches to do a D3 assessment. And so, in essence, it doesn't need to be changed. So, that's why we're not proposing any real changes, except the minor wording changes we mentioned previously.

And in point four -- go to the next slide, slide 19 -- point four is consistent with current regulations, and there's not much you would do to change point four that wouldn't conflict with regulations. So, effectively, there's no reason to change point four.

Most plants are required to either -- in operation today -- either meet 279-1968 or 279-1971, and both of those require a manual scram or a manual division-level actuation for every automatic actuation there is. 603 requires the same thing. 279 requires safety-related displays. 603 has slightly different display requirements. Both 279 and 603 require the use of minimum equipment in the manual actuation.

Now, that is open a little bit to interpretation about what is minimal equipment. But using the whole reactor trip system may not be minimal.

And then, if you go to the general design criteria, again, for light water reactors --

CHAIRMAN BROWN: Norbert? Norbert?

MR. CARTE: Yes?

CHAIRMAN BROWN: Go back to that point you just made. First, I want you to explain -- I'll give my pitch or my perspective on that, but I want to make sure I get it right.

You said it's -- I've forgotten your words now. The manual actuations, it's a debate as to what we mean by the most direct, or something like that.

MR. CARTE: Minimal of equipment is the --

CHAIRMAN BROWN: Minimal equipment. And for those who aren't familiar with that, arguments have been made that, if an operator actuates a switch in the main control room that, then, processes through part of the electronics before it goes to the reactor trip or the pumps or the SFAS system, whatever the switch is, that is not direct enough.

In other words, typically, a manual -- the diverse approach is you've got to have a hardware switch. You bypass all the electronics. All the

stuff that could give you a problem from CCF is bypassed. So, you've got a switch in the control room that de-energizes -- if you've got a (audio interference) in your scram breakers, it de-energizes the scram breakers. That's the direct path.

Some have argued that they can get away with putting some other electronics in between, and it's always a nasty discussion when they try that.

MR. CARTE: Right.

CHAIRMAN BROWN: Did I get that right, Norbert?

MR. CARTE: That's correct. And what happens, it's mostly a distinction between new facilities and existing facilities.

Existing facilities predominantly have simple, independent, hard-wired manual switches today. So, when they're replacing the reactor trip or SFAS system, they're not going to rip out their switches and put in something else. So, in general, for digital upgrades of existing facilities, this manual switch is not an issue because they're just not going to touch them.

The problem comes in new reactor designs and, as Charlie has pointed out, some people have proposed that the manual trip switch is just another

digital input into the reactor trip system, which then decides to trip, based on the operator's suggestion that it should trip.

And I haven't been involved in the new reactor designs, but, for certain things like a reactor trip, it's really not that onerous to run a pair of wires. There are other functions that could get a little bit more complicated. Some of the ESF functions, especially when you have sequenced actions, you're talking about more wires, but, in essence, it's really not that hard. And it's very practical.

So, let's go to the next slide to GDC 22. Oh, sorry, we're there.

So, one of the things about GDC 22, it says, "to the extent practical." And is it practical to run one set of wires out to the trip breakers to disconnect them? Yes, that's pretty practical. It's hard to argue that that's not practical. So, there's a strong case that can be made for a certain level of diverse manual actuations.

Anyway, so we don't think that point four needs to be changed and we think it's consistent with current regulations. SECY 3 was -- the SRM was issued in '93; 603 was incorporated into regulations in '99. So, it was a little premature. So, the regulations

have been updated, but the regulations are consistent. So, there's no need to change point four in our current position.

With that, I think we can transition to Steve and point two. Next slide.

MR. ALFERNIK: Thank you, Norbert.

My name is Steven Alfernik. I'm a Reliability and Risk Analyst in the Division of Risk Assessment.

I am now on slide 20, and I will address points two and three on the risk-informed path.

When discussing point two, it is important to note that the current approach focuses on the consequences of the digital I&C CCFs, but it does not consider the likelihood of the accidents evaluated in the Safety Analysis Report.

The staff considers point two to be appropriate for risk-informing the evaluation of postulated digital I&C CCFs. As Norbert discussed earlier, point two contains acceptance criteria for the evaluation of the postulated CCFs.

In developing the proposed expanded policy, the staff's goal is that risk-informed approaches will be consistent with all five principles of risk-informed decisionmaking, as listed in

Regulatory Guide 1.174.

Next slide, please. I am now on slide 21.

When discussing point three, it is important to note that the current approach only provides one way of addressing undesirable outcomes, and that is diverse means.

The staff considers point three to be appropriate for risk-informing the evaluation of design techniques or prevention and mitigation measures other than diversity that are implemented to reduce the risk from a digital I&C CCF. Point three addresses the measures used to address the CCFs.

In developing the proposed expanded policy, the staff's goal is to apply a graded approach for the level of justification needed for design techniques or measures other than diversity. The staff's intent is that a graded approach for point three will be based on the risk significance of the postulated CCF, not the risk significance of the digital I&C system.

A graded approach can allow a distinction between digital I&C CCFs that constitute failures, misbehaviors, or spurious operations of the system. In practice, the staff expects that the risk significance of CCFs will be determined via the change

in risk to a facility -- for example, change in CDF alert -- from each postulated digital I&C CCF, and that this risk significance will be determined using a bounding risk assessment.

The use of a bounding risk assessment will address uncertainties in quantifying the probability of occurrence of the digital I&C CCFs.

CHAIRMAN BROWN: Your slides are being blanked for a minute by admissions. Can we get those admissions cleared? Can I do that?

DR. BLEY: No, on my screen they're still showing. I guess it's controlled --

CHAIRMAN BROWN: Yes, it just disappeared on mine finally. Okay. I didn't know whether anybody else -- does Norbert need to repeat something because of that block that was in there?

DR. BLEY: No, but I have a question, if I might.

CHAIRMAN BROWN: Go ahead.

DR. BLEY: You mentioned a bounding risk assessment. I certainly agree with that, but I don't know if you've been following it. The folks developing Part 53 seem to have had some trouble describing a bounding risk assessment, and they've kind of moved -- well, I won't say any more than that.

It hasn't been transparent for them.

Do you have any definitions or is there some guidance you're going to be giving on what that means?

MR. CARTE: Well, I'll let Steve take it first.

MR. ALFERNIK: Yes, go ahead.

MR. CARTE: I was going to let Steven take a first crack at that.

MR. ALFERNIK: The short answer is, at this point, we're looking at revising the policy to allow for that, recognizing that there may be some difficulties defining it.

At this point, a bounding risk assessment doesn't necessarily need to assume that the digital I&C CCF will occur, nor we don't necessarily need to assume a probability of one. But we do recognize that, if you propose other numbers, there needs to be some kind of technical justification for it.

DR. BLEY: Okay. That will be interesting to see how that goes. I agree with you and I think it's a reasonable approach, but it may run into difficulties along the way.

MR. CARTE: So, one of the thoughts on this is, we wanted to use a simple bounding approach,

and hopefully, we can arrive at alignment on what that is. But since the likelihood of CCF or the reliability of software is sort of a hot potato or hard to quantify, has a lot of uncertainty, it would be easier not to argue about the reliability of digital I&C if you could get away with a bounding approach, and that was our thinking.

MEMBER DIMITRIJEVIC: Yes, the bounding approach is used in some of those advanced reactors. Does that mean, actually, using the selected number for the common cause, not advanced. Somebody mentioned (audio interference). If you use (audio interference), I mean, you have -- you know, that changes in CDF and LOCA big. So, like 10 to the minus 7 or 10 to minus 6 is the common number. Is that what you mean by bounding approach?

MR. ALFERNIK: I would say the bounding approach would not necessarily involve the best estimate of the number; just some value where there is a technical justification that we're comfortable that it will not exceed that.

MEMBER DIMITRIJEVIC: Okay. So, that number was not selected, that's what you mean, in the -- I mean, there is no number in the mind when we discuss the bounding approach?

MR. ALFERNIK: Correct. At this point, we are just looking at revising the policy to see if we can approach it from this manner. We have not developed a technique yet.

CHAIRMAN BROWN: So, you don't know whether it's going to be -- I'm struggling a little bit. I'm not a PRA or a statistician. So, I'm trying to figure out how you ever come up to, well, that's not likely and it's only about 10 to the minus 5th or 10 to the minus 6th. I have a hard time seeing how you can ever come up with a number like that to address a CCF for software-based systems. Okay?

I mean, I can make an argument that, once you've programmed, it's going to do what it's programmed to do unless it gets confused, in which case, if you've got a watchdog timer, you will catch it. The question is, do you catch it in two or three minutes or do you catch it in 300 or 400 milliseconds? That makes a difference from an accident standpoint. So, that's, to me, where you would make the judgment on the risk involved in doing anything other than just having the watchdog timer operate, if it takes five minutes to finally reset and/or trip the system, or at least trip one division.

I'm obviously talking outside of my area

of expertise, but that's the old engineering judgment approach that I would have used back in my old days.

MR. CARTE: Charlie, if I could comment?

So, in essence, what this SRM or what this SECY is doing is it's opening the door and it's starting the work.

(Laughter.)

Well, no, see, the problem is that we can't evaluate alternatives to diversity or the acceptability of alternatives to diversity because the policy doesn't allow it. So now, if we get the policy to allow it, then we can have the discussions of what would be acceptable. We haven't had those discussions, and we don't have the answer yet. But this policy change is to allow us to try and find an answer that is different than diversity is the only way.

CHAIRMAN BROWN: I don't disagree. I mean, I agree with you. Okay?

I'm not against getting rid -- if you could get rid of diversity, I'd be happy. I'm not against that. I'm all for that.

Just stepping back, I'll talk about this later, after we have the NEI one. I've got a couple of thoughts that I'll throw out at the table at that

time, instead of doing it now. I'll go ahead and let you finish this, and let NEI finish.

But that's my thought, is that I don't want you to think I'm against finding a way to not have to use diverse means. That would be great, in my estimation.

But I start getting a little nervous when I start hearing the 10 to the minus 5th and 6th getting thrown into this ballpark. Engineering judgment I can live with, but basing my thought process or judgment on a number, when we don't have any idea what the input looks like, I'd probably do it anyway, but it would be on a judgment basis, not because it was 10 to the minus 6th, when somebody says it's really 10 to the minus 2 for some reason.

MR. BENNER: Member Brown, we share that concern. And I don't want to get too far ahead because I think you're right that, when NEI makes their presentation, we'll have a little more there.

Because we're looking at it from the other direction, not to do that sort of quantification of a CCF. But, in reality, right now, even if we assumed that the likelihood of the CCF was one, we don't have a mechanism to consider other likelihoods as a reason to not do diversity. So, if nothing else --

CHAIRMAN BROWN: I got that.

MR. BENNER: -- this opens up the door for us to sort of rank, right, hey, there might be a CCF that, yes, if you have that CCF and you go straight to core damage, that's not good. But you may have a CCF that you need other things to go wrong before you get to core damage, and that might be a situation where we don't want to impose diversity. And we don't even have the flexibility now to do that.

CHAIRMAN BROWN: I'm onboard with that. I probably sound like I'm an old curmudgeon sometimes, but I've always worried about diversity getting in the way of a simple design, as opposed to a more complex design. And that's a double-edge sword, as you can well imagine.

I often have a difficult time thinking that I've got four channels, even though I've got -- as long as I maintain a strong defense-in-depth architecture, I think an argument can be made; I'm not so sure you can quantify it, because once you're running all these things on a different clock asynchronously, it's hard to imagine some of these things occurring all simultaneously in all four divisions.

But we've never taken -- we've never gone

after that path. And that's what you're all trying to do, from what I can see. Is that correct -- sort of?

MR. BENNER: Yes. Yes.

CHAIRMAN BROWN: Okay. All right. Go on. Sorry.

Good conversation. I think it's a good discussion. Thank you all. Go ahead.

MR. ALFERNIK: So, I'll go ahead and address the last bullet here. And this has just emphasized that diverse means will continue to be an acceptable method to address digital I&C CCFs. And as discussed earlier, diverse means may include manual actions.

Next slide, please. So, I'm on slide 22.

As we've been discussing, the staff is providing recommended language for an expanded policy which will allow greater use of risk-informed approaches to address digital I&C CCFs.

CHAIRMAN BROWN: Steve?

MR. ALFERNIK: Yes?

CHAIRMAN BROWN: How about backing that one up a minute? Okay? Go back to that last slide, that last item.

Let me get this phrased correctly. When you look at the analysis that's done for DBAs and all

the other critical accidents that we address, and you look at how they're calculated and the conservatisms that are involved, we've never attempted to try to say, what's the likelihood of all those really coming together all at once, all those super-conservatisms, such that a manual operator action, based on indications that he's seeing, would not be adequate to shut down the plant? We've never really gone after it that hard.

So, that's another area of what other things would you look at to determine, do we need to do something or are manual means okay? And we've always faced that, what it was -- it's the 30-second rule, or something like that -- for taking action. But it's always based on these accident analyses that occur faster than 30 seconds.

So, anyway, I'm just rambling on. I'll let you go on now.

MEMBER PETTI: This is Dave.

I just want to say that, when you look at some of the stuff and think about advanced reactors, where time constants are very different from light water reactors in many cases, because of the combination of the moderator and the coolants, this is a really nice approach. Because I think it can give

some flexibility while still assuring safety. So, it makes some sense to see where it evolves to for advanced reactors.

CHAIRMAN BROWN: Yes, Dave's got a good point. They are all different from what we're used to dealing with.

Okay. Thank you for letting me interrupt. Go ahead, Norbert -- or Steve. I'm sorry.

MR. ALFERNIK: Norbert has his hand raised. I'll let him jump in first.

MR. CARTE: Yes, the other thing that comes up with diverse means is it's being done using best estimate. But sometimes best estimate can also be debated.

So, for instance, does best estimate mean taking your accident analysis code and putting in realistic values and running it? Or does best estimate mean, well, in a large break LOCA, we really have leak before break; therefore, there's plenty of time to do it manually? Because if you don't have leak before break, you don't have time to do it manually, right? So, what does best estimate mean?

So, there's a lot of dimensions on these things that people can discuss also.

Sorry.

MR. ALFERNIK: Okay. I'm on slide 22 now.

Okay. As I was saying, the staff envisioned several potential benefits in expanding the current policy.

First, risk-informed approaches can provide flexibility to address digital I&C CCFs and are consistent with the PRA policy statement.

Risk-informed approaches can have different levels of PRA use, and they could support a graded approach in determining the level of justification needed for design techniques or measures other than diversity.

Next, PRA models can be used to systematically assess the need to reduce the risk introduced by the digital I&C system, and the PRA models can identify initiators or scenarios for a lack of digital I&C diversity that does not compromise safety.

Taken together, risk-informed approaches can provide licensees and the staff the flexibility to expend resources commensurate with safety and risk significance.

Next slide, please. I am now on slide 23.

If the Commission approves the staff's recommendation, the staff will apply the following

guiding principles to ensure consistent implementation of the expanded policy:

First, the expanded policy will not conflict with existing regulatory requirements. Therefore, a rule change or exemption will not be required to implement it.

Second, the expanded policy will be implemented consistent with the Commission's PRA policy statement, SRM-SECY-98-144, and the current agency focus on expanding risk-informed decisionmaking.

Implementation of the expanded policy will continue to provide reasonable assurance of adequate protection of public health and safety.

Next slide, please. I'm now on slide 24.

And the last two guiding principles are that:

The use of risk-informed approaches will be consistent with all five principles of risk-informed decisionmaking.

And then, PRAs used for risk-informed approaches will be technically acceptable. For example, read the guidance in Regulatory Guide 1.200 and included in the affected PRA configuration control and feedback mechanism.

And now, I'll turn the presentation back to Samir.

MR. DARBALI: Thank you, Steve.

So, to summarize the proposed expanded policy, it's composed of four points that provide for a deterministic path or a risk-informed path to address digital I&C CCFs. And Norbert and Steve covered the details of those points.

And here again, on slide 26, are the key messages, and the policy will encompass the current points in SRM-SECY-93-087, with clarifications, and expanded use of risk-informed approaches. Any use of risk-informed approaches will be expected to be consistent with the safety goal policy statement, the PRA policy statement, and SRM-SECY-98-144; and that the current underlying CCF policy will continue to remain a valid option for licensees and applicants.

DR. BLEY: Thanks. Can I ask you another question?

This SECY you're putting together, I guess -- I think from what you said earlier -- the main purpose is to get something beyond the SRM on SECY-93-987 to allow more flexibility, is that correct?

MR. DARBALI: Yes, that's correct.

DR. BLEY: Okay. Thanks.

Will we get to see your draft before it goes to the Commission or is this our only chance to give you some thoughts on it?

MR. DARBALI: I believe that the current process doesn't have the SECY being shared before it goes to the Commission.

DR. BLEY: Okay. Thanks.

CHAIRMAN BROWN: That's why we're doing this, Dennis.

MEMBER REMPE: So, as a follow, then, if it does go to the Commission, I assume it would be available to us and we could write our letter at that point. Is that what your process would accommodate?

CHAIRMAN BROWN: Yes. That's me talking.

MEMBER REMPE: I just am wondering if the staff realizes -- I mean, you can do it the way you're planning, but, then, of course, the downside is that, although we've got some slides here and their supporting information, what's finally submitted to the Commission, the only way we'll weigh into it is after you submit it to the Commission.

DR. BLEY: Joy?

MEMBER REMPE: Yes?

DR. BLEY: I thought the intent --

Charlie's on the hook for a letter, I think, for next week. It would be based on this, but I think you folks would have to say that it's based on discussions with the staff, but not on a review of the related SRM.

MEMBER REMPE: Okay. So, if the --

DR. BLEY: But I think it's to write a letter.

MEMBER REMPE: Well, as a clarification, during P&P, I asked Charlie explicitly, "Are we going to do a letter?" And he said, "No, I don't know." I know it's on the AWS, but, no, he wasn't sure.

And, yes, we can do a letter and say all we have are the slides and this discussion, but one of the outcomes of this meeting is, are we going to do a letter? Because it wasn't clear.

And two, just so everybody understands, then, of course, if there's something that comes up in what's submitted to the Commission, by omitting ACRS -- I mean, I heard earlier today you're going to have another meeting with public comments that you'll consider before you finalize things, even after this ACRS discussion. So, you know, you may hear a public comment and put something in that we would have no clue about in what we write.

And I just am kind of exploring that concept a bit more to understand that everybody understands where we are in this process, because it just seems a little different than what we usually have an opportunity and when we have an opportunity to comment on it.

CHAIRMAN BROWN: Joy, what I commented on or the way I presented it on "Do we or don't we do a letter on it," it was because I didn't know any of this at the time.

MEMBER REMPE: Right. I understand that.

CHAIRMAN BROWN: And my biggest concern was we've put a lot of effort into, over the last few years, into a number of -- like ISG-06, for instance, was initially focusing on architecture, getting that concept in to how we evaluate these systems. The ISG-06 is a prelicensing evaluation. So, the applicant knows what to expect or what the NRC expects.

And then, BTP 7-19, Rev. 8, while they didn't put everything in that we recommended, that was largely on the cyber -- not on the cyber -- but on the control of the access issue, which we had discussions concerning. It's a very good document relative to defense-in-depth and diversity evaluations.

So, my basic concern was this SECY was going to decimate part of BTP 7-19. I believe that's not the case from what I saw in either this presentation or in my review of the NEI presentation. I don't know that the staff has looked at the NEI presentation or not, but that was my take out of their brief also.

Am I correct in that assumption, Samir or Eric?

MR. DARBALI: Right.

CHAIRMAN BROWN: Whoever wants to answer it?

MR. DARBALI: Right. The NRC's work on this Draft SECY to expand the current policy will not decimate -- BTP 7-19 will still, as you can see in the last bullet here, the current policy will continue to remain a valid option.

CHAIRMAN BROWN: Yes, I haven't asked you how you were going to implement this yet. Are you going to make changes to BTP 7-19 or, once you get the SRM back from the Commission, you have to get this out in the world of regulation, right, or guidance?

MR. DARBALI: That's correct. That goes into the next slide for the next steps.

CHAIRMAN BROWN: Okay. Let me finish my

thought process first here, if you don't mind.

One of the things we did with ISG-06 -- and I've forgotten how long -- it was a couple of years ago, four years ago or so -- we were advised that and incorporated an alternate review path. We didn't decimate what as there, but we provided an alternate review path, which provided a different approach in several areas. It simplified the process.

And I guess my thought was, in going in and modifying 7-19, you ought to leave it intact and attach an appendix which, then, incorporates the parts of 7-19 that stay the same, but how steps two and three get executed in a different manner before it comes back. But keep them separate, so that you don't have to wade through and decide what you're looking at. Depending on what the applicant wants to do, it's just a matter of how you present the information.

I was going to make that comment later, but since we got into that now, I just went ahead and said it.

And, Joy, that was my big concern. If we wrote a letter, I would have been objecting to something. Right now, I don't have any particular problem with what they're doing. I do understand that, if they change it from what they're telling us,

then that's a different issue and we won't find out until after the fact.

MEMBER REMPE: And that was my concern, is we're not going to find out until after the fact. And the timing of how this process is going just seems a little more susceptible.

Why is it that you didn't do a draft before it went up to the Commissioners and have us review at that time? I guess that is what I am curious and that I was going to ask the staff. And I was going to wait until the last slide. But since Dennis opened that door, can the staff explain to us why we weren't engaged later or given another opportunity?

MR. BENNER: This is Eric Benner.

I mean, we have been working within the management chain and within Commission expectations of a schedule. So, we are trying to meet those expectations while maximizing the ability of the Committee to weigh in.

Getting to the mechanics, we acknowledge that this is a little unusual. We certainly have tried to put as much in here, such that, you know, you have the substance of what would be in the paper. In having both this meeting and the full Committee

meeting and the public meeting, you know, I suspect our presentation at the public meeting is going to be very similar to this presentation, such that we're just telling stakeholders what we are doing, and we are not expecting any significant changes.

So, from the Committee's standpoint, we certainly respect your decision as to doing a letter after the full Committee meeting back to the EDO. And certainly, if the paper, in your mind, does not align with the presentations we'll be making today and at the full Committee, we certainly acknowledge that you have the authority to do a letter to the Commission.

I think we certainly would be open to, after we do our public meeting on June 8th -- because I'm sure we will be briefing internally on any changes we made as a result of that public meeting -- we would also provide that summary to the Committee, so they knew of any changes we have made as a result of that public meeting.

MEMBER REMPE: Yes, I'm glad you explained what's going on. Again, this is something that I wanted to explore more, and we'll just have to decide. But thank you.

CHAIRMAN BROWN: We can discuss after the NEI presentation, I think, on a path forward relative

to our June full Committee meeting. I was going to bring that up amongst the Committee here, so we can figure out what do you want me to do. I mean, I could write a letter, but, right now, it would be giving suggestions of which one of them -- is just what I just said.

MEMBER REMPE: Well, that's an idea, but, then, I'm just thinking about what goes up to the Commissioners in the long term, and if it gets changed, do we write a second letter?

CHAIRMAN BROWN: Yes --

MEMBER REMPE: But, anyway, let's wait --

CHAIRMAN BROWN: -- we could do that.

MEMBER REMPE: -- until all the presentations are over.

CHAIRMAN BROWN: But we could see the SECY afterwards, and if we think something's out of line, we could -- I have no problem with writing another letter with Committee input.

MEMBER REMPE: Okay. Yes, let's go ahead and hear the rest of the presentations.

Thank you.

CHAIRMAN BROWN: Yes.

MR. DARBALI: All right. So, I think we've, essentially, covered the bullets in this slide,

but I'll just repeat them.

So, we're currently drafting the SECY. And we're going to have a public meeting in early June. We are planning to send to the Commission the SECY paper by the end of July of this year. And upon approval of the expanded policy, then we will begin work on however a BTP 7-19 update would look like to implement the guidance on the expanded policy.

CHAIRMAN BROWN: And that's why I made the suggestion of what it would look like. I think you could use ISG-06 as an approach with an altered, like an appendix, just 7-19. So, you don't intertwine the risk stuff with the current path. That's all right.

MR. DARBALI: Understood. Thank you.

CHAIRMAN BROWN: But that's after the fact. We will review 7-19.

MR. DARBALI: Understood.

CHAIRMAN BROWN: Okay. Thank you.

I wasn't trying to be demanding. We would expect to review 7-19.

MR. DARBALI: Yes, right. Right. Yes. And based on our past presentations, we understand that expectation.

CHAIRMAN BROWN: Okay. Thank you, Samir.

MR. DARBALI: All right. So, that

concludes the staff's presentation.

CHAIRMAN BROWN: Okay. We have another presentation.

Are there any other questions from the Committee before we segue into the next presentation by NEI?

(No response.)

I'm not going to do public comments until NEI finishes their presentation.

DR. BLEY: Are you going to do a break, Charlie?

CHAIRMAN BROWN: Yes, I am. I was just making sure we didn't have any questions.

So, if no other questions from the Committee members, we will break until 2:50. That's 15 minutes.

That will give people time to -- if you're at home, Walt, get your dog out. I'll get mine out. And we can get set up; NEI can get set up to have their presentation ready to go at 2:50. Is that okay?

MEMBER KIRCHNER: Yes. Thank you, Charlie.

CHAIRMAN BROWN: Okay. We're recessed until 2:50.

(Whereupon, at 2:35 p.m., the foregoing

matter went off the record and went back on the record at 2:54 p.m.)

CHAIRMAN BROWN: All right. We're up with NEI.

And, Alan, are you there?

MR. CAMPBELL: I am online. Can everybody -- just need to adjust just one -- okay, can everybody see my slides?

CHAIRMAN BROWN: Okay. Are you going to be the sole presenter in this circumstance?

MR. CAMPBELL: I will be the primary presenter, and I have a few individuals that will be supporting me.

CHAIRMAN BROWN: Okay.

MR. CAMPBELL: I have Warren Odess-Gillett --

CHAIRMAN BROWN: Oh, okay.

MR. CAMPBELL: -- who's a fellow engineer at Westinghouse, and Neil Archambo, who's an industry digital subject matter expert, as well as Victoria Anderson with NEI, who is our risk applications subject matter expert as well.

CHAIRMAN BROWN: Okay.

MR. CAMPBELL: They'll be helpful in responding to any questions, but I'll be the sole

presenter.

CHAIRMAN BROWN: Okay. Since Joy asked me if I was here, I haven't checked to see if everybody else is back. Is anybody missing?

(Laughter.)

That's the wrong way to ask the question, but I thought I'd try it anyway. We needed some humor here.

We'll go ahead and get started. They'll come in when they show up. Go ahead, Alan, and have at it. Okay?

MR. CAMPBELL: Understood.

And good afternoon. And thank you very much for extending an invitation for NEI to provide some input on this important matter.

Again, my name is Alan Campbell. I am a Technical Advisor with NEI. I started almost a year ago. It was the end of last June. Prior to my role at NEI, I was also a Cybersecurity Manager at Vogtle 3 and 4, where we were building the first fully digital plant. And then, prior to that, I worked in the industry on digital modifications for various AE firms. So, I appreciate the time this afternoon.

I already introduced some supporting members today to help out. Warren Odess-Gillett, who

is, as I mentioned, a fellow engineer with Westinghouse, and Neil Archambo, who is an industry SME. Both of these individuals have been instrumental in NEI support of the Integrated Action Plan and the various initiatives that have stemmed from that. We also have Victoria Anderson, who I mentioned is our Risk Specialist at NEI.

The purpose for NEI's involvement today, we really would like to provide industry input on how we propose to address digital CCFs. So, taking a look at our proposed implementation that was provided last September, NEI's 20-07, Rev. D.; and also, recognize the impacts that this policy has on the guidance, and vice versa. So, take a look at how we're proposing to address CCF, and then, its implications into policy.

We did provide a white paper in April that describes our perspectives on how we can address common-cause failure within policy. We do plan to issue a revision to that white paper. I was hopeful to get that out prior to this meeting, but I was not successful in that. But we plan to submit that or transmit that early next week for review as well.

Some of the, well, all of the clarifications that we plan to provide in the white paper revision will be covered today. And those

include recognizing some of the limitations of how we apply risk and as it pertains to digital I&C. So, some of the points that were brought up earlier in the NRC presentation. And also, another point of clarification is our treatment of manual actions.

Okay.

CHAIRMAN BROWN: I have one question, Alan.

MR. CAMPBELL: Yes, sir?

CHAIRMAN BROWN: I got a copy of this -- let me check. It was a couple of days ago, I think. Yes, oh, it was yesterday. Is this paper representative of the copy we got, by the way, just for my reference purposes?

MR. CAMPBELL: Yes, sir, the presentation you're looking at should be the exact same as what you received yesterday.

CHAIRMAN BROWN: Okay. Thank you.

MR. CAMPBELL: Okay. I wanted to start with just recognition of all the work that has gone into digital I&C, this topic in general. So, the Digital Integrated Action Plan has been successful in driving change throughout the industry related to digital. The items that we have listed here have really helped spur new digital projects and improved

guidance for the regulatory activities supporting these projects.

We appreciate the efforts, and including the public interactions, that have supported this over the past six years. Notably, the RIS Supplement and BTP 7-19 revision have provided improved guidance for addressing common-cause failure, primarily focused on changes to what are safety-significant and safety-related systems and non-safety systems. The scope of our discussion today is updating the policy for protection systems; more specifically, RPS and SFAS.

So, we appreciate the openness that I've heard in this, the initial presentation, and pursuing other design techniques, in addition to diversity. My discussion today is not intended to be critical of diversity. Diversity is a useful tool that is very helpful to design engineers and to the plants, but we believe that, when it's used, it should be performed out of or used with engineering basis, and it has limitations like any other tool that could be used.

So, why digital safety systems? We just want to reemphasize the point -- I think it's worth belaboring -- how digital technology really supports the long-term and safe operation of our fleet.

As an industry, we're reaching system

obsolescence on the existing analog technologies, and really the benefits of the digital safety systems can't be understated -- with the system diagnostic capabilities, the availability of data to end-users within the plant, and just better overall knowledge of what the plant is doing and when. It also helps to reduce the hardware inventory compared to other existing systems.

Our landscape today has improved dramatically from the time that the original common-cause failure policy was written. The SRM-SECY-93-087 was informed greatly by the SECY-91-292 titled, "Digital Computer Systems for Advanced Light Water Reactors."

In that SECY paper, the NRC describes some of the concerns that were present at the time with digital instrumentation control technology. Those included lack of experience in nuclear applications; the absence of requirements and standards, and the lack of guidance and standards for software development processes. That SECY, as I mentioned, helped inform the policy that we have today that's documented in the SRM, and helped create those positions back in 1993.

The landscape that we have today, the

digital I&C technology has improved, both on the technological front and, also, on the production process front, resulting in more deterministic behaviors. We also have a mature community of international standards, such as IEC and IEEE, that are widely accepted. They have stable processes for updates and reflect our current understanding and approaches.

Lastly, the hazards analysis techniques have really matured from what we had back in the nineties, and we'll go through some of the new processes that we're proposing today,

So, I wanted to start by taking a look at the applicable regulation. I think this helps me at least bound the description of where we're at, why we're there, and what is stated within the regulations.

There are two primary focus items on the next three slides that we'll take a look at. So, one, how is diversity addressed in the existing regulation? And two, how is manual initiation of protection functions addressed in existing regulation? So, focusing in on point four, which is the manual main control room initiation of protective functions.

The first point is to address the use of

diversity as the benchmark against which all other means are compared. So, while diversity can be an effective design technique, it is not the only effective design technique.

The second point, as I mentioned, is to address the NRC's SECY outline, which describes the limitations of using risk-based upon the existing regulation. Specifically, policy point four, which addresses diverse and independent main control room displays and controls for manual system-level actuation of critical safety functions is stated to have a regulatory requirement which restricts the ability to use risk insights.

This first slide takes a look at 10 CFR 50.55(a)(h), which was addressed within the NRC staff presentation. As the NRC staff mentioned, both of these IEEE requirements do require a means to implement manual initiation of protection actions. However, within these IEEE standards, neither of these require a diversity aspect to the means of manual initiation.

Reg. Guide 1.62 provides guidance for how to implement these IEEE requirements, and there is a position in there that states that diversity should be addressed. However, the basis for that position is

that diversity is required, based on meeting BTP 7-19, which is based on the policy that we're here to discuss today. So, ultimately, the codes and standards do specify a means of manual initiation protection actions, but these do not specify diversity as a requirement in accomplishing that.

I thought I heard somebody chiming in. Okay.

Okay. We are on slide 6 now.

We also discussed previously the ATWS systems. So, ATWS, 10 CFR 50.62 addresses regulatory requirements and does provide a diversity requirement for functions that are shown on this slide specific to PWRs and BWRs. And for the BWRs, we should note that the second and third requirements do not have diversity requirements within the regulation.

The ATWS systems are not part of the protection systems, and these systems were created for specific vulnerabilities where diversity did demonstrate effectiveness. So, per the regulation here, these systems do require diversity, but neither -- I'm sorry. This requirement does not have any specific manual actuation requirements contained within it.

Lastly, we have GDC 22. GDC 22 provides

design criteria to prevent loss of protection functions. The text you see on this page is directly from the GDC with some emphasis added.

BTP 7-19, Rev. 8, states that, for high safety-significant, safety-related systems, GDC 22 requires functional diversity to the extent practical. We believe this interpretation of the GDC is too narrow. As shown on the slide, the text from the GDC states design techniques shall be used to the extent practical to prevent loss of the protection function. References to diversity are used as examples of design techniques that can be used, not required design techniques.

So, to summarize, how is diversity addressed in existing regulation? It's addressed in 10 CFR 50.62 for specific ATWS functions which are not part of the protection systems. For protection systems, it is described as an example of a design technique and not a requirement nor a benchmark for comparison.

Then, how is manual initiation of the protection functions addressed in existing regulation? It is required by 10 CFR 50.55(a)(h) and their endorsed standards. However, diversity is not an element required within these standards.

CHAIRMAN BROWN: Before you go on, let's go back to that again.

MR. CAMPBELL: Yes.

CHAIRMAN BROWN: Diversity is not required with these standards. I mean, manual actuation is manual actuation. I mean, it's hard to comprehend. I mean, a switch is a switch. And if you want to do something different, then that's different. But if you use something other than a switch, you would probably end up having it, you know, direct-wired. You'd probably end up with an argument.

The constant issue about that diversity is not required is correct. Okay? It's not explicitly stated. It's just a part of the overall evaluation. But it's obvious that the desire to de-emphasize any diversity at all, that's been the function of all -- whatever the slide number is right now -- the first four or five slides.

So, I understand that, but just be a little bit careful. Just because nothing is specifically required, it's hard to argue that manual, direct manual connection and tripping either safeguards, or your scram breakers. Whatever the shutdown method is in the new reactors, it's hard to argue that that's not a good thing to have, regardless

that nobody has, quote, "mandated" it in terms of a requirement or a guidance in a Reg. Guide or rule.

I just wanted to throw that out there as a counter to the four pages' worth of emphasis on nothing is required for diversity, other than the SRM, it sounds like.

MEMBER KIRCHNER: Yes, Charlie, this is Walt. I'd like to join in on this.

Manual trip, scram, is, by its very design and nature, a diverse way of achieving the shutdown in the event that the reactor protection system malfunctions or doesn't do its job, or whatever situation arises in the plant.

So, yes, I don't get this connection with diversity here, when you're referring back to manual initiation. And I just second what Charlie says, especially for new designs. I hope that that manual initiation is as simple as possible and it's at the very end of the line, and that trips the scram breakers, or whatever the mechanism is, without any electronics in between.

Just one person's opinion, but I don't think those requirements on manual initiation have anything to do with the diversity argument, other than the fact that this is a diverse means to achieve a

plant shutdown.

CHAIRMAN BROWN: It's a facility defense-in-depth, based on the NRC's thought process, as opposed to an I&C focus.

MR. CAMPBELL: And I understand and appreciate your points. I just wanted to -- the intent of these slides is to clarify what is and is not in the regulation. We just want to make sure that there's a clear delineation of where there are diversity requirements and where there are not.

And going back to the point of where diversity, outside of manual initiation, is required, it can be a useful tool, and we're not proposing eliminating it. We're just proposing complementing that approach as well, where deemed necessary.

CHAIRMAN BROWN: Well --

MR. CAMPBELL: Warren or Neil, do you have any other thoughts on that?

MR. ODESS-GILLETT: I'll let Charlie speak first.

CHAIRMAN BROWN: No, I was just going to say, based on the last discussion from the staff, I think I made it clear I'm not against simplifying the diversity wherever you can. Some of the designs we've looked at had a lot. I thought it was overdone, but

we weren't going to tell them not to use it. The design was there. There was one that was very simple, relatively simple, and we didn't tell them to make it more complex.

So, there's been a wide range, if you look at those four projects I referenced. I don't know whether you all can see those or not, but at least we saw them. And I took a lot out of that. And some applicants have really taken that diverse approach to quite a level of design incorporation, where I thought it was probably overdone. But the system worked and it was clear, and it met the fundamentals that we keep advocating here on the Committee, and that we've tried to do relative to architecture -- redundancy, independence, determinate processing, defense-in-depth, and whatever diversity is thrown in there, and then, finally, the control of accessing.

In other words, you always have hardware-based, not-configured-by-software data communication devices out of the reactor trip and safeguard systems to your main control rooms or to any other distribution points for data, just to protect them from -- you know, it's like having a door that's always shut relative to it.

But that's the one big problem that the

microprocessor stuff introduces into this world. You now no longer just can take care of control of access with physical access. You now have to take care of electronic access, and I don't mean cybersecurity. You want a door that nobody can open.

The plant, overall facility, needs to be cognizant of the cyber issues, but system design inside the safety systems should have no doors. So, that's the last of the five of the majors. So, those are the fundamental pillars that we use in evaluating it.

You notice I did not emphasize the diversity because I think, just like the staff is trying to do, I think they're trying to be very responsive to the thought process and simplifying this process in the diverse world, so that we don't go overboard; and that the staff and NRC don't require more than what really meets the needs -- the needs, not requirements, but needs.

MR. CAMPBELL: Right.

MR. ODESS-GILLETT: So, yes, Alan, this is Warren Odess-Gillett. I'm a loaned employee to NEI from Westinghouse.

The purpose of bringing these regulations forward is that, in regards to the staff's proposal

for position four, it's their position that there's no need to risk-inform position four, which means that, arbitrarily, diverse and independent displays and controls will still be a requirement without any kind of risk insight aspect of it.

And the reason that's given is that, because these applicable regulations that are presented here really call for those independent and diverse displays and controls, that we just saw it differently; that's all.

CHAIRMAN BROWN: I will provide one insight on that. From '77 until 1999, December 31st, I was responsible for at least seven different integrated designs, which are now trucking around in naval nuclear power plants. And in every one of those, we had diverse and independent displays and controls, every one of them.

Now, you've got sailors crunching around under the ocean. So, you really want to make sure you can see stuff. Does that mean it's different for the commercial plants? If I saw some plant that had nothing but touchscreen displays, I would choke myself to death. I'd find a rope and go hang myself from a bridge.

That just doesn't make any sense. You

should not have all your -- they can be very erratic. It depends on what's going on. It depends on the size and how many, and how many of them you have in terms of redundancy.

But I think the position that the staff takes is about valid one on that point, on point four; that when you get to the controls and displays, you need to make sure you are not locked into one path only, whatever that means.

And I understand your desire to point out what the guidance is that people are looking at when they're reviewing the designs. It's just I just want to make sure it's clear that elimination of some of those basic tenets does not sound like a really good idea to me in terms of how they're cranked into the design.

I did read your other white paper, also, and I'll have some comments on that later, after you finish your presentation, because you incorporated some of the white paper into the end, I think the end of this slide presentation, if I'm correct.

MR. CAMPBELL: Yes.

CHAIRMAN BROWN: I think you didn't eliminate that, I presume.

MR. CAMPBELL: That's correct.

CHAIRMAN BROWN: Okay. Sorry, when I get on a roll, I can't stop sometimes.

Nice to see you again, hear from you again, Warren.

MR. ODESS-GILLETT: Thank you, Charlie. Nice to hear you, too.

CHAIRMAN BROWN: Okay. Go ahead, Alan. I'm sorry.

MR. CAMPBELL: We appreciate the commentary throughout. That's helpful.

Okay. So, we are on side 8 now.

Slide 8 will take a look at how we're addressing common-cause failure today. So, Branch Technical Position 7-19 provides the review guidance, based upon the existing CCF policy.

The outline you see here closely mirrors the outline of the actual BTP for addressing common-cause failure in high safety-significant, safety-related systems. Some of the excluded sections did not meet that criteria.

CHAIRMAN BROWN: Can I ask a question before you hit the bullets?

MR. CAMPBELL: Yes, sir.

CHAIRMAN BROWN: The first bullet says "eliminate," and then, "diversity, testing, and

alternative methods." Are you trying to eliminate all those or does the BTP eliminate CCFs through the use of those?

MR. CAMPBELL: It eliminates CCF through the use of those. I appreciate the clarification.

CHAIRMAN BROWN: Matter of fact, yes, I thought we were off-topic here.

(Laughter.)

MR. CAMPBELL: No. I apologize for that. When I was writing it and had the BTP in front of me, it made complete sense.

But, yes, just to clarify here, those secondary bullets, the round ones, for "eliminate, mitigate, and acceptance," those are the primary sections with BTP 7-19, Rev. 8 --

CHAIRMAN BROWN: Right.

MR. CAMPBELL: -- and addresses how to treat common-cause failure. The bulleted -- or I'm sorry -- the diamond bullets are the submethods that are the proposed methods for eliminating common-cause failure, mitigating, or accepting it.

CHAIRMAN BROWN: Got it.

MR. CAMPBELL: Thank you.

Okay. So, this slide, it's the same overall method, but I do want to address that, for the

types of systems that we're discussing today, testing is not really a plausible option, due to the system complexity. The approach is intended for simple designs and quoted as such within the BTP.

The alternative methods, as stated in the BTP, those methods either need to be preapproved by the NRC or requested in the application. And so, we're aware that some alternate methods have been used throughout the industry. We are not aware, or I'm not aware, of any that have a blanket preapproval from the NRC.

And one of the really limiting factors on using alternate methods is that, through requesting approval through the application process, this increases the regulatory risk for a given project and may challenge the application review process as well.

Each of the guidance topics within the mitigate CCF portion of the process requires diversity to mitigate the potential common-cause failure as well. So, what we have in BTP 7-19, the preferred guidance for addressing common-cause failure is diversity or acceptance through those techniques. We do recognize that there are other methods described in there, but these are the primary methods that have been used to date and we're aware of moving forward as

well.

So, BTP 7-19 does provide us helpful guidance on how to meet the existing policy, but, as mentioned, it's largely dependent on diversity as the design technique. So, the natural question we should ask ourselves here is, is diversity always the right tool that we should be dependent upon?

This diagram is taken from -- sorry, we're on slide 11 now -- this diagrams is taken from the NRC digital I&C training material that's made publicly available on the NRC website and is used to describe how the international community views system failures. Typically, the term "systematic failure," or in this case, "systematic fault," bounds the introduction of CCF or other latent design failures. As you can see, the picture addresses many sources that can introduce failures into a system, including systematic random faults, incorrect requirements, and others.

One addition I'd like to make to the diagram is system interactions. We develop requirements and specifications based upon our understanding of system interactions, both controlled and uncontrolled. Safety and hazards analysis experts outside of nuclear believe that these system interactions one of the leading causes of events

outside of the nuclear industry.

On slide 13, here we've added a diverse system. Note that I did remove the random fault and trigger boxes, just to simplify the diagram. The first item to note on this slide is that we do not address the ultimate source of our problems where systematic failures are introduced.

Both designs are based on the same understanding of the system and its interactions. Sometimes the same requirements can even be used to create both systems. An error at this phase may not provide the protection that we expect.

The next noteworthy item is that we have introduced a new failure pathway to the plant. While a failure in either system should result in a safe plant state, we also consider the potential challenges to plant operating staff during that scenario, as well as the plant reliability, since it has a direct nexus to safety as well.

I liken the approach to a standard Swiss cheese model. We have added a layer of defense, but each layer introduces new failure possibilities and does not address the source of the failure all the time.

So, as we discussed, our OE indicates that

latent design defects from inadequate requirements and uncontrolled system interactions are the primary contributors to systematic failures, including common cause failure.

EPRI performed a study of 17 nuclear events to identify their contributing causes, and from this study, EPRI identified that the primary contributing cause, close to 50 percent of the factors found, were requirements errors.

So, what can we learn from how we're addressing CCF today? Diversity may be helpful in addressing hazards. However, it has its tradeoffs. It can introduce complexity and a different set of failures. It also may not address the sources of systematic failure, such as requirements errors.

Diversity, as I've mentioned, can be a useful technique, but it should be used when supported by engineering analysis.

CHAIRMAN BROWN: Comment.

MR. CAMPBELL: Yes, sir?

CHAIRMAN BROWN: This is Charlie.

Latent design defects have been a problem, whether you've got analog systems or you've got software-based systems. It makes no difference. It's easy to get those wrong.

I would like to say that all the systems we ever developed prior to me becoming the head of the program, as well as those after I became head of the program, that we put into ships never required a field change to fix a latent design feature that we found that we made a mistake. So, that's a different issue. Okay?

In diversity, a latent design defect in a hardware system is everywhere, everywhere it's duplicated. And if you've got a specification in terms of how the software is processed, that's latent also. I mean, it's there; if the branch is not correct to what you're going off to seek for some reason, and you missed it in your design and reviews, that is a design defect. I don't call that a CCF. That's not a failure. It's a we screwed up when we designed the system issue, and those are human errors. And all the diversity in the world won't necessarily fix those. So, neither will a hazards analysis ever do that because you probably can't spend four years doing it.

Anyway, it's just a thought, and I just wanted to make that point. Latent defects are different in terms of how you have to recognize that they're there.

I'm finished.

MR. CAMPBELL: Yes, and I was just being thoughtful.

So, I agree with you that not all latent design defects are common-cause failures. What we're stating here, systematic failures -- so, that includes common-cause failures -- can be a result of latent design defects. So, latent design defects can include common-cause failures.

CHAIRMAN BROWN: Yes, but an engineered system can also compensate for those if it's totally and completely independent. Because once you're processing data, if that latent software design defect doesn't get hit in the same way because you're running asynchronously or the data coming into it from the previous A-to-D converters, and then, the processing through, whatever, they're all out of synch. And so, the likelihood -- I hate to echo this from the NRC thing -- but that's where you say, hey, look, it's not likely that they're going to all occur at the same time. And you will notice something in one and start getting suspicious, and that's where the operator comes in, if he sees something funny.

Anyway, it's just we're going to have to deal with that forever. Just a point.

MR. CAMPBELL: Okay. Let's see, Myron, you have your hand up.

MR. HECHT: Yes, Charlie -- Yes, I did.

The point is that requirements or erroneous requirements do lead to defects that can cause CCFs.

CHAIRMAN BROWN: Oh, I got that.

MR. HECHT: It's not that erroneous -- so, I just wanted to make -- yes, okay, if you got that --

CHAIRMAN BROWN: No, I understand.

MR. HECHT: -- then that's okay, too.

CHAIRMAN BROWN: I understand that. Future requirements run your toast.

MR. HECHT: Yes.

CHAIRMAN BROWN: I'm sorry, Alan, go ahead. I just get carried away.

MR. CAMPBELL: I appreciate it.

Okay. Okay. So, NEI is proposing the use of modern hazards analysis techniques and risk insights to provide a graded approach to addressing the common-cause failure and protection systems. This approach has been proven effective in research, and the techniques are being used widely in other safety-critical industries.

And, Charlie, just to address your point

that no hazards analysis technique is perfect, we'll walk through the technique that we plan on utilizing. It combines different hazards analysis methodologies and complements the strengths of those, and has been proven effective in identifying important issues that lead to hazards or system losses.

CHAIRMAN BROWN: Are you on slide --

MR. CAMPBELL: So, we'll address that.

CHAIRMAN BROWN: Are you on slide 16 or 15?

MR. CAMPBELL: I'm on slide 15 right now.

CHAIRMAN BROWN: Oh, okay.

MR. CAMPBELL: Yes.

DR. BLEY: Alan, this is -- oh, well, go ahead. Go ahead.

CHAIRMAN BROWN: Go ahead, Dennis.

DR. BLEY: It's Dennis Bley.

You heard the staff's presentation of what they intend to include in their SECY paper. And they seem to, if I recall correctly, have left the door open to a variety of approaches to do simplified or complex hazard and risk studies within that approach. Are you critical of what they're doing or do you see it as it will open the door to try some of these techniques you're arguing for?

MR. CAMPBELL: I think the primary message is that we are aligned with the overall intent of what the NRC staff provided today. There are a few items that I think that we still need to better understand the positions on -- those, namely, being how we use risk and how it's treated throughout the process, and how we address the manual initiation, really the requirement for diversity, the prescribed environment -- sorry -- prescribed requirement for diversity within that.

I think those are the two primary items where we would like to better understand, but the intent here is, for the next few slides, we've made a proposal on more implementation-level guidance. And so, we found it helpful to walk through how something could be applied using risk insights, hazards analysis techniques, and how effective it could be in addressing digital common-cause failure, and then, use that how-to implementation guidance to informing important policy points that would enable that sort of method.

DR. BLEY: I'd make two comments.

The first is I found the discussion of diversity requirements more legalistic than safety-oriented and engineering-based.

But, two, the other things you're suggesting, at least to me, seem to fit within the framework of what the staff is proposing. So, maybe at some point later the staff could make a comment on that, too.

MR. CAMPBELL: And I would agree with you, especially on the second point on the overall methodology, just with a couple of nuances in there that we got some new information today, and then, we look forward to engaging with the staff during future public engagements as well, to have more direct engagement.

DR. BLEY: Yes, and I understand you haven't seen very much of this, either.

MR. CAMPBELL: Right.

DR. BLEY: It's kind of hot off the press here. Okay.

MR. CAMPBELL: Right. Much of what you see today has been developed without seeing what the NRC outline was.

Okay. Okay. I'm on slide 16 now.

So, NEI provided NEI 20-07, Rev. D, in September of 2021, providing guidance on how to leverage existing EPRI processes to address systematic failures such as common-cause failure. These

approaches, known colloquially as HAZCADS and DRAM, provide a diagnostic approach and use multidiscipline teams throughout the design process, starting early in the conceptual phase -- sorry -- throughout the design process to identify missing, inadequate, or incorrect requirements.

Through this approach, the system architecture is analyzed to identify unsafe control actions which could lead to hazards. Then, it uses risk insights to address the unique loss scenarios commensurate with the risk to the plant.

CHAIRMAN BROWN: I presume in all these analyses and design approaches, and everything that you're all talking about, you're not advocating the elimination of redundancy or independence of divisions? Or how do you demonstrate that you've got repeatable and predictable processing times?

MR. CAMPBELL: That's correct, we are not proposing eliminating those concepts.

CHAIRMAN BROWN: I mean, if you don't even have an architecture that lays those out, you can't do that on what I call a -- and I also don't quite understand where you're going to apply the hazards analysis. Is it on an architecture one-line diagram-type level? Because you certainly can't get down into

the bits and bytes. That doesn't even make any sense.

MR. CAMPBELL: And that is correct. The process starts from a conceptual design. So, you don't start with a blank sheet of paper. This is a diagnostic tool. It's not a design tool.

CHAIRMAN BROWN: Okay.

MR. CAMPBELL: And so, you have to have a design to start. You also start at high levels of abstraction to understand the overall system and its implications to other systems. And then, as you progress in design decisionmaking, the diagnostic tools then reflect the level of analysis of the information you have at your availability. And so, you have multiple iterations of modeling the control structure, and each one of those gets more detailed as the design progresses and is finetuned.

Does that address the comment?

CHAIRMAN BROWN: Yes.

MR. CAMPBELL: Okay. Okay. So, the research basis -- the HAZCADS and DRAM process were developed by EPRI after an EPRI study that investigated multiple hazards analysis methodologies used within nuclear and other safety-critical industries.

The findings that are cited in the EPRI

report display the strengths and limitations of each methodology used on its own. EPRI, then, used this research to develop the HAZCADS and DRAM processes by combining two of the methodologies -- the Fault Tree Analysis, or FTA, and Systems Theoretic Process Analysis, or STPA. The strengths of these two methodologies complemented each other and also reduced the limitations of each method when used on its own.

On slide 18, unfortunately, one hour is not enough time to fully discuss these processes. I'm actually in the middle of a two-and-a-half-week training on these processes right now. So, they are very detailed. This slide is intended to show at a very high level the overall process and where these methodologies are applied. We will discuss some of the unique portions of this methodology in some of the upcoming slides as well.

So, using NEI 20-07, the applicant will apply STPA, which, again, will be presented in a little bit more detail in the next few slides. Within that process, the intent is to identify unique scenarios that could lead to possible plant hazards. From there, a Fault Tree Analysis is used to understand the risk consequences of each of those loss scenarios and conservatively bound the analysis.

Reg. Guide 1.174, figures 4 and 5, these figures describe the delta CDF and LERF requirements when using risk to justify licensing basis changes. Those figures are used to address each loss scenario and help determine a graded approach in which to address each of those loss scenarios. Ultimately, control methods, or in other words, design techniques, are applied to each of the loss scenarios commensurate with the Fault Tree Analysis mapping exercise.

Okay. I'm on slide 19 now.

So, STPA is one of the methods used to analyze and diagnose system architectures. It is a multi-step process that uses, again, multidisciplinary teams to analyze systems, their control structures, and potential unsafe control actions. This is a top-down approach using systems engineering principles to diagnose the requirements, design, and system interactions.

So, is STPA effective? Many blind studies have been performed to determine if STPA would have been effective in preventing previous events. One such example of a study had a team of people that were familiar with STPA, but unfamiliar with nuclear power plants, analyze the design of a nuclear plant system as it existed prior to an event documented in industry

OE. This was a real incident that the participants had no knowledge of.

The team used STPA to diagnose the system, and they anticipated the exact flaw that led to the OE, as well as nine other scenarios that were unaccounted for. This is one example, but the results from other studies have shown that STPA has found flaws that were either previously never found by design teams or were found earlier in the design process using this STPA methodology.

CHAIRMAN BROWN: Which digital I&C systems did this occur in? I don't want to know whose, but which type? Was this we're talking about electric plant, governors, voltage regulators? There's not a whole lot of digital systems in the reactor trip and safeguards area that have been replaced in the plants.

So, I mean, I'm sitting here struggling a little bit to -- I mean, it's a single point, not -- always worried about single points.

MR. CAMPBELL: Right. Understood. My understanding is this was actually a non-safety system in which the STPA analysis was performed. Matt Gibson, I believe, from EPRI is on the line as well and can provide any additional insights into the actual study details.

CHAIRMAN BROWN: I don't think we need to do that. My point being, is this a single-focus, single-function control system that's a digital system? It is obviously more susceptible when it doesn't have redundancy and independence cranked into it in order to achieve a common control output.

So, you're saying, with this process you're looking at, you're addressing reactor trip and safeguard systems. So, I'm not trying to discount it, but single-function control systems, very, very difficult if you make them too complex, if it didn't work right.

MR. CAMPBELL: Understood.

Oh, go ahead.

CHAIRMAN BROWN: I'm just saying sometimes everybody gets carried away with the software approach to doing something. They use it where a simple amplifier and relay and a switch would turn the system on, and they put a microprocessor in place anyway, which is not very thoughtful, when you get down to it. But it sends lots of data out. So, everybody is happy because they're getting lots of data.

I'm being a little bit -- I'm exaggerating to a certain extent, but it is just I get nervous when I -- it's apples and apples -- it's an apples-and-

oranges comparison.

MR. CAMPBELL: And I understand your point, and especially, it's not the apples-to-apples. We do have only one example of where a digital system has been applied in the manner that we're talking about today, at least that I'm aware of.

But the intent here is to discuss or show the efficacy of the process, of the STPA process, and not that of the system under analysis. The process without knowing the event, without the individuals knowing the system, resulted in identification of flaws that led to that event, as well as nine other potential flaws or scenarios.

CHAIRMAN BROWN: I only bring this up because I was familiar with one specific circumstance where I had recommended that -- this was on a turbine generator set governor system. And the vendor had optioneered two power supplies to feed both the governor and the overspeed trip system. So, they always would have a supply.

Unfortunately, the machine started hunting. They couldn't figure out why. So, they started troubleshooting, pulled out one of the power supplies, and the machine immediately oversped and somehow disabled the overspeed trip, and they barely

caught it because an operator was standing right beside it and tripped the throttle valve.

And that was somehow the noise from the one defective power supply, and they were now immediately back into the mode of providing, quote, "independent power supplies" for each of the functions.

MR. CAMPBELL: Uh-hum.

CHAIRMAN BROWN: So, I mean, the rules of independence and redundancy just work wonders and override the need to do a lot of detailed "how does one piece within it fail going to affect something?" I'm not saying you don't do some of that. It's just you've got to be careful you don't lose sight of your reliance on some good judgment in terms of the overall design.

I couldn't help myself again. I'm sorry.

(Laughter.)

MR. CAMPBELL: Again, always appreciated.

CHAIRMAN BROWN: Myron, do you have your hand up? No? Okay. Somebody's got their hand up. I don't --

MR. HECHT: Charlie, yes, I do. Yes, I do.

And I was just looking at the previous

slide to this one, where you identified the methodology, and basically, it starts out with STPA to identify the hazards, and then, FTA to quantify them, quantify the probabilities.

And you pointed out that -- or somebody pointed out -- maybe it was Charlie who pointed out that no hazard analysis technique is flawless. And that's true of STPA as well. In principle, it's fine. In practice, particularly identifying those loss scenarios can be difficult. And you may end up with a complete -- with an incomplete set of loss scenarios, which, then, affect your quantification aspects and affect your overall basis for a risk-informed decision.

I'm just making that point because sometimes I would have hoped that you would have included a diverse means to mitigate the likelihood of overlooking these loss scenarios in this DBA.

CHAIRMAN BROWN: I'm going to make a similar comment at the end of your presentation about the two approaches. I'm not against the thought process, but just to make sure you understand where I'm coming from, and you can refute it if it's wrong.

MR. CAMPBELL: Understood.

CHAIRMAN BROWN: Put your hand down,

Myron.

(Laughter.)

MR. HECHT: I did.

CHAIRMAN BROWN: Okay.

MR. HECHT: I did. Thank you.

CHAIRMAN BROWN: All right.

MR. CAMPBELL: Just one point. I think this is coming up here shortly, but I want to put a pin -- I was taking some notes here on the quantification of the risk. We will talk about that. I know that's been a topic in the prior presentation as well. We do have many slides on that. So, I'll address that piece of this within a few slides here.

But thank you both for the comments.

CHAIRMAN BROWN: That's okay. Go on. Thank you.

Which slide are we on now?

MR. CAMPBELL: We are on slide 21.

CHAIRMAN BROWN: So, 21? Okay.

MR. CAMPBELL: Twenty-one, yes. I was just verifying that was the right one to land on here.

Okay. So, STPA is being used extensively in other non-nuclear industries with safety-critical applications. NEI 20-07 provides a sample of organizations using STPA in these types of

applications today. These companies include, or organizations include: Ford, GM, NASA, Google, Tesla, and many other military branches. You can also see on this slide that many other industries have already or are in the process of adopting STPA into industry standards.

CHAIRMAN BROWN: I guess Boeing didn't fare so well with the 737, did it?

MR. CAMPBELL: Boeing, I don't know how that was -- I know they have been listed as using STPA. I'm not 100 percent confident on where that's been.

CHAIRMAN BROWN: I wasn't trying to say they used STPA. I'm just saying --

MR. CAMPBELL: Oh, yes.

CHAIRMAN BROWN: -- it was the fundamental thought process of the control function that got them in trouble. Okay?

MR. CAMPBELL: That's right.

CHAIRMAN BROWN: It took the man out of loop somehow.

MR. ODESS-GILLETT: Yes, it sort of reinforced -- this is Warren -- it sort of reinforces the concept that these systematic failures often are at the high level of defining requirements.

CHAIRMAN BROWN: Yes.

MR. CAMPBELL: Yes, thank you, Warren.

Okay. I'm on slide 22.

STPA has also been used within nuclear in the NuScale Chapter 7, "Design Certification and Safety Evaluation." The excerpt shown on this slide was taken from the SCR report and concludes that, "The hazards analysis performed by NuScale was effective and acceptable." The hazards analysis that they're referring to is described at length in the DCA, and that DCA describes the STPA process which was used.

Okay. Moving on from STPA, we'll describe or discuss how we can and cannot use risk in addressing digital common-cause failure. In previous discussions and white papers, NEI has used the term "risk-informed" in the context described from the NRC glossary, which describes or defines risk-informed decisionmaking as "an approach to regulatory decisionmaking in which insights from probabilistic risk assessment are considered with other engineering insights."

This term is frequently associated with specific regulatory guidance; namely, Reg. Guide 1.174. So, we've changed the terminology that we're using to "risk insights," rather than "risk-informed,"

to improve the clarity of what we're intending to communicate. And we'll go into a little bit more detail in the next few slides on some of the unique aspects of that.

So, we do understand the benefits of using risk insights. And Steve with the NRC staff did a great job in describing how using risk allows us to have a better focus-in on important system functions. And within the context of digital I&C, it allows us to have a better understanding of system architectural decisions and inform what design techniques we use to address common-cause failure.

I'm on slide 24.

The NRC staff SECY paper outline provides a number of guiding principles in developing the SECY paper. Three of these guiding principles are provided here that describe how the staff proposes to use risk information. Additionally, the SECY outline states that PRA models can be used to systematically compare the effectiveness to diversity -- or as an alternative to diversity. And I'd like to discuss some of the challenges in meeting these principles and concepts.

I'm on slide 25.

I think through the discussion we've recognized that digital I&C software reliability is

challenged regarding how we model it within PRA space. In order to model software reliability, significant assumptions are used to quantify software failure rates. Because of this, the results produced by -- or I'm sorry -- the results produced based on the digital technology have substantial uncertainties and little insight to the significance to plant risk. For this reason, the absolute risk impact of software reliability determining the effectiveness of design techniques and comparing to full diversity are not plausible.

Lastly, while NEI 20-07, Rev. D, leverages concepts from Reg. Guide 1.74, it does not meet the scope of the full application of Reg. Guide 1.74. This Reg. Guide provides guidance for justifying licensing basis changes, based on the risk impact of the change. NEI 20-07, Rev. D, proposes using conservative risk insights for each unique loss scenario to inform design decisions, not to justify the overall impact of the modification or application.

Okay. I'm on slide 26.

So, how do we propose to use these risk insights? NEI 20-07 uses risk sensitivity analysis to determine a conservative bounding impact for specific scenarios. These unique scenarios are modeled to

determine their specific impacts to the CDF and LERF, and then, are mapped to the associated figures in Reg. Guide 1.174 as a conservative means of prioritizing the treatment of each of these scenarios.

This analysis assumes the failure of the loss scenario -- or assumes the loss scenario occurs. So, it assumes failure and determines the impact to the plant based on that failure, and then, we apply the graded approach based on that. So, based on those risk insights, the design team applies various control measures or design techniques or design requirements, in accordance with GDC 22.

The result of this process is a conservative bounding analysis of the modification that assumes the failure. So, we are not proposing that the absolute risk impact of the digital system or its unique design techniques can or will be determined.

For these reasons, the risk-related guiding principles and concepts listed in the NRC SECY outline are not aligned with the proposed use of risk using this technique. In other words, full application of Reg. Guide 1.174 requires one of the guiding -- or one of the principles stated within that is to minimize the risk of the modification, and we

cannot accurately -- I'm sorry. Because of the assumptions with the software that we've all referred to, this would not be possible to describe within absolute means.

MEMBER DIMITRIJEVIC: Can you repeat this? Because I nearly failed to understand this last point. Can you just tell again? And what are you actually trying to tell us, that you are using the Reg. Guide 1.174 without numerical values? Is that what you're trying to explain?

MR. CAMPBELL: Yes, we are -- so, the process, when we develop the loss scenarios for specific hazards or for a modification, we assume each of those loss scenarios occurs and do a risk sensitivity. So, when this loss scenario occurs, what is the impact on the plant?

Based on that, we leverage -- we recognize that Reg. Guide 1.174 provides means that already informs, you know, within the regions, how to address that for modifications of the plant. So, since that's already defined, we're leveraging that concept that's described in 1.174, but we're not claiming compliance with it because the software failure, as we've acknowledged, cannot be defined within the PRA model without significant assumptions baked into the

process.

Does that answer your question?

MEMBER DIMITRIJEVIC: Well, it was very well around it. So, let me just discuss with you something. And then, I will see exactly what I don't understand.

MR. CAMPBELL: Okay.

MEMBER DIMITRIJEVIC: See, the Reg. Guide 1.174 evaluates things, the changes, something before and after, right? Right, that's what it is. To justify what is now, you evaluate, you could evaluate what it should be or what it was, right? So, what is actually -- when you say that those scenarios are assumed to read what they need to say, now what are we evaluating? We are evaluating if the common cause doesn't have a -- what are we evaluating, actually, in this process through the 1.174? What is the delta risk between? Between what?

MR. CAMPBELL: The delta risk is between the existing design, and then, we do a sensitivity -- the delta is the sensitivity to any given loss scenario. So, we assume the loss occurs. The sensitivity --

MEMBER DIMITRIJEVIC: Loss of what?

MR. CAMPBELL: The loss of function. And

then, we use that --

MEMBER DIMITRIJEVIC: Loss of function which will be lost if you have a common-cause failure? Is that what -- loss of what?

MR. CAMPBELL: Can you repeat your question? I'm sorry.

MEMBER DIMITRIJEVIC: Yes, I will. So, you are calculating loss of scenario, which will be loss due to the common-cause failure?

MR. CAMPBELL: That is correct.

MEMBER DIMITRIJEVIC: So, you evaluate all possible combinations of common-cause failure, and those scenarios are -- those probabilities of common-cause failure couldn't bear a set to one? Is that what you do? I'm trying to see how this evaluation works in my head, and I haven't really because you're discussing it on an abstract level instead of -- if you show some specific scenario, it will be much more clear to me.

So, is that what you're doing? You're assuming the common-cause failure occurs with probability of one?

MR. CAMPBELL: That is correct.

MEMBER DIMITRIJEVIC: But failure of the parts of that common-cause failure are not one, right?

MR. CAMPBELL: That is correct.

MEMBER DIMITRIJEVIC: Let's say that you have a sense in terms of some failure probability, where you're actually setting failure of two sensors to that failure probability, or are you setting a failure of two sensors to one? That's what I'm trying to see.

MR. CAMPBELL: We're setting the failure -- and Matt Gibson with EPRI is, again, on the line. And, Matt, if I'm misspeaking for the "how to" on the HAZCADS and DRAM process, please correct me.

The failures are -- the functional failure or the loss scenario is set to one. And so, we evaluate the impact of a common-cause failure on the plant, and then, prioritize our treatment in a graded approach to either prevent, to the extent that we can; mitigate, or if it's low enough, accept the impacts of that.

MEMBER DIMITRIJEVIC: Do you have examples in your white paper of this process?

MR. CAMPBELL: Not in the white paper, but within NEI 20-07, Rev. D, which is available within ADAMS. It's described within there.

MEMBER DIMITRIJEVIC: Okay. I will check that. Thanks.

MR. CAMPBELL: Okay. Matt, I heard you speaking in.

MR. GIBSON: Yes, Alan. We can expand on that, but I guess, in the interest of time, probably we won't at this point.

MR. CAMPBELL: Okay.

MR. GIBSON: So, just I guess move on.

MR. CAMPBELL: Okay. Thank you.

I see Han Bao has -- do you have your hand up?

MR. BAO: Hi, Alan. This is Han Bao from Idaho National Laboratory. Long time, no see.

MR. CAMPBELL: Yes.

MR. BAO: And I have one question for your previous slide. If you can go back to -- yes.

So here, the challenge is in the modeling by using PRA tools was already discussed. So, how should we define or how did you define the substantial uncertainties? Which kind of uncertainty can be considered as substantial?

MR. CAMPBELL: Your question is regarding the magnitude of uncertainty?

MR. BAO: Yes.

MR. CAMPBELL: Okay.

MR. BAO: Yes.

MR. CAMPBELL: Victoria, are you online? Can you speak to what a substantial uncertainty would be?

MS. ANDERSON: Yes. I mean, I think what we were thinking when we said, "substantial uncertainty," it's where you get to the point where the uncertainty is greater than the point estimate you make, if that makes sense.

MR. BAO: Okay. Thank you.

MR. CAMPBELL: Okay. I am on slide 27.

So, NEI believes that the approach that we've described today is effective and will result in safe digital protection systems. We believe that diversity can be an effective tool when engineering analysis supports its use, but it is not required in all circumstances, except for ATWS, nor is it a benchmark against which other options are compared based upon existing regulation.

We believe that the risk insights should be used to apply a graded approach. But, because of challenges in modeling software reliability in PRA models, its use is limited to performing conservative bounding analysis on specific functional losses.

The policy considerations listed on this page summarize these points that we've made throughout

today's presentation and were provided within the white paper. And these have remained unchanged, I believe, except for the term "risk-informed" changed to "risk insights" from the version that has previously been sent.

The next two slides provide an example policy using the considerations that we just discussed. We are aligned with the NRC staff in preserving and updating the existing policy statements in SRM-SECY-93-087. That said, NEI believes a supplemental pathway that should be established, such that the concepts that we've expressed today can be applied with what's currently described as points two, three, and four to reflect what we've discussed. Our analysis of the existing regulation does not preclude us from addressing point four, as we've discussed throughout the presentation.

The example policy that you see here maintains the overall concept of the existing SRM-SECY-93-087, point one, but does specify the scope to RPS and SFAS. We believe this terminology better defines the scope of the policy and is aligned with the original intent of the common-cause failure concern. This point also broadens the defense-in-depth term to fully specify the plant's defense-in-

depth, as was discussed during the NRC presentation as well.

Point two describes the overall methodology using risk insights and hazards or reliability analysis.

And lastly, our example, point three allows for broader application of design techniques, not just limited to the diversity. So, this is consistent with current policy and, also, consistent with that non-safety-significant -- I'm sorry -- non-safety SSCs can still be used.

Monitoring and manual operator action are options for design techniques, but not prescriptively required unless already done so by 10 CFR 50.55(a)(h).

So, this completes my prepared comments on the topic today. I want to thank the NRC staff for their work on this topic. While there are still some points for us to better understand each other's position, I know that, based on our previous interactions, that we'll continue to have meaningful public dialog and look forward to further engagements on the topic.

I also want to thank the ACRS Subcommittee for generously allowing me to present NEI and its members' perspectives today.

Thank you.

CHAIRMAN BROWN: Okay. Thank you, Alan.

I've got a couple of observations I would like to make. But, before I do that, I was going to go back through the members here and see if they have any additional comments. I want to make sure we get those on the record, so that I can find them, if I have to do anything, in the transcript.

(Laughter.)

So, do members have any comments that they would like to make? Just start chiming in. Or do you want me to call you out name by name? So, somebody can start, if they want to.

MEMBER KIRCHNER: Well, Charlie, I'll take a stab, having sat next to you all these years at the table.

It seems to me I haven't heard anything that addresses -- what I think we're looking at is addressing systems, architectures, and reliability, and maybe looking for places where you have common-mode or common-cause failure potential. But I haven't heard anything to obviate the need for diversity in the reactor protection systems and the SFAS systems. Just an observation.

CHAIRMAN BROWN: Yes.

MEMBER KIRCHNER: I can see the use of these risk techniques to enhance the overall robustness and resilience of the plant to upsets and cases where the upset may be, yes, you have common-cause failure of your choice of electronic digital I&C systems, or whatever, but I haven't heard anything that would, from my perspective, suggest an alternate route to address the fundamentals of, you know, the architectural fundamentals for the reactor protection system and the SFAS systems. That's just an observation, not a question.

MR. CAMPBELL: I'd like to respond to that, if that's appropriate.

CHAIRMAN BROWN: Yes, go ahead.

MR. CAMPBELL: Okay. And it's difficult to get down to a granular level of detail within an hour and a half or so. But the methodology that we're looking at today using STPA and the Fault Tree Analysis, we're not prescribing the use of one design technique over another. What we are suggesting is that all design techniques should be applied, where it's appropriate within the results of the analysis and its impact on risk to the plant.

And so, when we look at the example primary and diverse architectures here, the process

that we are looking, or the STPA and Fault Tree Analysis of HAZCADS and DRAM evaluates the system architecture, but, in doing so, it diagnoses issues with the specification and requirements. It addresses issues on the understanding of your systems. It looks at the system interactions.

You know, it starts from a place of everything is possible to occur, and then, it evaluates from there, you know, what the impacts of that are, and then, provides the design techniques that are applicable to it. So, there are a number of things that we could do to eliminate, prevent, or accept those, but what should we do commensurate with this risk impact?

MEMBER KIRCHNER: No, I agree, Alan, with your application of this methodology. It sounds pretty sound to me. This diagram is a good diagram.

Charlie made an excellent point. It doesn't matter with this diagram whether you have an analog system or a digital system that's prone to common-cause failure. That could be true in an analog system, too.

And then, if the specification errors are wrong for both diverse systems, well, you're in big trouble. But, hopefully, your techniques maybe would

help you sort that out diagnostically.

So, I'm not at all critical of the approach you're taking or anything. I'm just making an observation that I think, if this, for example, were two divisions of a reactor protection system, yes, you could get the specs wrong on both, and then, you tie them together and get an uncontrolled or controlled interaction. Yes.

So, going through, whether it's the Fault Tree Analysis or the other, the STPA methodology, and seeing if you're vulnerable to that second box on the bottom, I think a very worthwhile design exercise. So, I'm not criticizing at all.

CHAIRMAN BROWN: Anybody else --

MR. CAMPBELL: Thank you. I appreciate your observation.

CHAIRMAN BROWN: Any other members have another comment?

(No response.)

Okay, I guess it's my turn. It's the five-second rule.

How do I start this off here? Let me address the big-picture part of this first, the diversity versus not diversity, and the approach that you show in your example policy-type thing, which

replicates what was in your white paper.

I'll look at it from a higher level. To me, the path you're asking, in order to get away from or eliminate or minimize the use of diversity because of the complication of the additional equipment, and everything else that it may entail, it takes what I would call a micro-approach to doing that. You say, hold it; we're going to use these tools to meet, to assess what failures we may have to deal with.

And I take your policy statement No. 2, where it says, "The applicant shall identify each digital common-cause failure that could adversely impact a safety function using risk insights and hazards and/or reliability analyses techniques."

You'll never know whether you've found each digital common-cause failure that could adversely impact a safety function. I mean, the analysis would be so complex and have to go down into the bowels and the intestines to sift through every little tendril that's branching off anywhere.

Not that you don't take a higher-level approach to some of that as opposed to -- you know, it just depends on the depth you go to. But that's kind of the microscopic approach to figuring out what your CCFs are, and then, addressing each CCF and doing

something with it.

The diverse approach is what I'll refer to as a micro, a coverall-type approach to doing business. Not saying it's perfect, but it bounds it, to use a terminology that the staff used earlier a little bit.

In other words, you look at your overall architecture that's been designed with the fundamental principles. Then, you figure out, okay, what may go wrong with those? We can't figure out what they all are. But if we do this with something that looks different than the techniques we use in those four divisions, then we have -- or in two devices of the other two -- we at least obviate and reduce the likelihood -- again, a risk assessment -- of having anyone CCF damage me.

So, that's my view of, do I grovel down in the bowels and get my hands dirty or do I look at the top-level picture and say, look, I've got to bound this stuff. I cannot ever find each and every CCF, and then, make a design change to fix that. It's just never going to happen.

I threw that out in my program 20 years ago, or 22 years ago now -- actually, 40 years ago, when we first started doing these. It was awful hard.

And I had far more resources in my hands than the commercial world did.

You can't build engineering models that replicate exactly what's going into each and every one of the plants; hook it up to a massive computer system, and then, test every line of code to see that you get the right result.

But it's just a different approach. That's what you're stuck with in the commercial world. You don't have any choice. You use very complex computer platforms which have -- Warren, you can correct me if I'm wrong -- hundreds of thousands of lines of code, because the guy that designs the platform wants to be able to apply it and make money off of it, and there's nothing wrong with that, either. But that means you have to determine whether all those, the parts of that code that you don't use, but yet the interrupt calls them up sometime, but maybe it interferes. And how do you determine that? It's very, very difficult to figure out what that is.

So, it's just different approaches. It doesn't mean some of the techniques can't be used. And it looks like the staff has, I think, tried to take maybe a more cautious approach to say, hey, look, right now, we're prohibited, you know, based on the

rules that say we have to do diverse in these circumstances. And they're trying to open the door to say, "We need to have some flexibility to use our heads during the design process."

So, the stress, the problem we've got here is trying to get the Commission to agree with a more flexible approach and not be so prescriptive. People accuse me of being prescriptive all the time, and I am in some circumstances, as Warren and others well know. Okay?

So, that's my view of the two thought processes that you're doing going forward or proposing. I don't believe anybody disagrees with me on that, but the critical notion is, obviously, to try to get the Commission to allow the staff to start using their head in terms of how they assess the need for less diversity, which I think is a thing we ought to be doing. I don't know whether all the rest of the Committee members agree with me, but that's my personal opinion.

MR. CAMPBELL: Can I take the opportunity to --

CHAIRMAN BROWN: Of course.

MR. CAMPBELL: -- respond to that?

I appreciate the comment. The statements

that you see on the screen here and on the next screen -- obviously, we don't write policy. And so, this was just our saying, hey, this is how you could apply the overall considerations that we would need in order to apply a scenario such as the NEI 20-07, which has been described today.

The language that you pointed out is consistent with the existing policy and how it's been applied within BTP 7-19. So, where it states to demonstrate the vulnerabilities to CCF have been addressed, and to identify each digital CCF, that's consistent with what's described in SRM-SECY-93-087 and BTP 7-19 today.

And to your point of what the staff is doing, I'm aligned fairly closely with the overall approach that the NRC staff is taking. I think reserving the existing pathway and expanding that to allow the use of risk is important and does allow -- it does open the door for further conversations where we can look at NEI 20-07 and challenge it, and understand where other challenges may lie. So, we're aligned on the overall approach.

We just want to ensure that the methodologies that we are proposing with 20-07 are clearly understood; specifically, within how we're

using risk and what some of the limitations there are, and where should we have to show absolute risk impact; where the challenges with that may lie.

CHAIRMAN BROWN: Okay. No, I understand that.

The concern one could have is, by the time you finish some of these complex analyses, a diverse approach is less expensive than spending months and months and months going through and identifying 22 things that could happen. And now, I've got to have 22 design changes -- I'm exaggerating just to make the point -- to correct all those.

And diversity has stood us in good stead. Like I said before, I had the opportunity to not do the diversity and opted -- I can't tell you exactly what because it's in that program. I can't tell you the actual details. But because it simplified an overall argument, we were able to say like, what's our worst circumstance we deal with that we have to worry about getting hit with from an accident standpoint? And so, you can address things like that.

There are different approaches. When you look at the DBAs, why beat yourself to death on some, when the worst one we have to care about, use the risk approach to doing that, the likelihood of it

occurring. But if it's more critical, put something in for that, but be more flexible in the other areas.

And it seems to me that the staff needs to have some flexibility at doing that and working with industry and NEI, so that we don't overdo it. We need to get these systems into the plants.

I mean, I could build new analog hardware. I integrated circuits that are out there. You could design the entire systems with integrated circuits and off-ramps, and it would work just fine. You just don't have transistorized amplifiers.

But that's not the right way to do it. You get far more information to the applicants -- I mean the drift is almost zero, the accuracy of these things. All your drift is the A-to-D converters, basically. There's probably someplace else in there. So, somebody could kill me.

So, I'm all in favor and I just want to make sure that we help encourage the staff in the right way to not only to be able to stick their toe in the water and address this thing in a coordinated manner, along with industry.

The other point is that -- I may be more administrative -- is that, if somebody starts trying to get the risk-informed or risk insights into

eliminating designing equipment with the fundamentals, the five fundamentals, then I get real nervous about that, because I don't see that as being a good idea.

If somebody comes in and says, in one of these new plants, that we only need two protection channels, I just can't see me recommending to the Committee members agreeing with that approach.

I remember operating with plants that were one out of two. And it was a pain to try to keep the plants operating when you needed to start up. We finally migrated to four for everything, and the crews never have a problem with operating the plants under those circumstances. So, flexibility is important.

So, those are my concerns. That's why I wanted to hear these presentations in the first place, so that the Committee could understand a little bit more, the members could understand a little bit more of what's involved in these overall thought processes.

And I think we've gotten a good set of presentations today. You have a couple of viewpoints, a lot of them the same, and some of them with some variations. The staff did a good job, and I think you all did a good job in presenting some thought processes of how you all have been thinking about it also.

A big question now for the Committee in our discussions, I guess, is, how do we want to address this in the future?

Did you have anything else to say, Alan, or can I address the Committee members now?

MR. CAMPBELL: I see that Warren has his hand up. I wasn't --

CHAIRMAN BROWN: Oh, thank you. I didn't see that.

Go ahead, Warren.

MR. ODESS-GILLETT: Yes, I just want to make it really clear that NEI has no intention of using risk insights to eliminate what's required in the current set of regulations for independent, single-failure criterion, redundancy, and so on.

CHAIRMAN BROWN: Deterministic processing, control --

MR. ODESS-GILLETT: Deterministic processing, exactly. And defense-in-depth, exactly. Exactly. Right. We have no intention of using risk insights to eliminate any of that.

CHAIRMAN BROWN: Yes, I think there are defense-in-depth approaches that don't require you to have diversity. That's one of the areas we have never really addressed fully, but there are approaches that

you can consider that those work well.

So, anyway, thanks, Warren. I appreciate it.

Anybody else?

Joy, are you still there?

Oh, a hand went up. Whose hand is that?

MR. CAMPBELL: It looks like Myron.

CHAIRMAN BROWN: Oh, is that you, Myron?

MR. HECHT: No, it's Vicki.

CHAIRMAN BROWN: Oh, Myron and Vicki. Okay.

Vicki, do you want to go first, please? Did you hear?

MEMBER BIER: Sorry, I raised my hand second. So, if Myron is ready, he can go first.

CHAIRMAN BROWN: No, you go ahead. Go ahead.

MEMBER BIER: Okay.

CHAIRMAN BROWN: We'll pick up Myron.

MEMBER BIER: Great.

I just have kind of a high-level comment. I did appreciate the discussion that in some cases diversity could actually increase risk, just by increasing the complexity of the plant and making it more difficult to understand everything that could

possibly go wrong. But it seems like the burden for demonstrating that is pretty high; that in many cases it would be the diversity would be a benefit.

And I just wanted to say that I was a little nervous -- I don't want to put too much into it, because it may just be choice of wording -- but with wording like, when do we not want diversity? You know, it seems to be more a matter of like, when is it acceptable to have less diversity, not so much when is it better from a risk point of view to have less diversity. You know, I realize there may be some cases where that's true, but that in most cases I think the diversity probably is risk-beneficial, and the real debate is not is it a bad idea, but is the benefit its providing so small that we can justify having less diversity?

CHAIRMAN BROWN: Yes, good point. Thank goodness you got that into the transcript, because I would have never remembered it.

Thanks, Vicki.

Are you done?

MEMBER BIER: I am done with my comment. Thanks.

CHAIRMAN BROWN: Okay. Myron, you had something else?

MR. HECHT: Yes, I have two, and that's dangerous because, generally, one will be answered and the second one won't, but I'll bring them up anyway.

The first comment that I think, in order for STPA to be a viable approach, NEI or EPRI has got to provide some examples, and the NRC's got to understand them. I'm concentrating, I'm thinking specifically about the loss scenarios, but it might be trying to understand what the control loops are in a four-channel plant might be a little bit more complex than might be originally thought.

And so, providing the staff with a safety case on the basis of STPA without some preparations and guidance and the ability of the staff to evaluate the STPA is going to be a problem. And, of course, that is the foundation of the EPRI/NEI approach.

The second point I wanted to make was in response to the comment you made on chart 25, which, basically, says that, "The absolute risk impact of software reliability cannot be quantitatively measured without substantial uncertainties." Without uncertainties, it's true; without substantial uncertainties, perhaps less so.

And I, you know, point to the experience now that we have in guidance systems and missiles, and

some missiles which are very, very important to national security, which I'm working on now. And in that technique, in those domains, what's long been an acceptable approach has been software-in-the-loop simulations where you can do hundreds of thousands, or even millions, of runs with variations. Of course, the variations have to be proper and representative of the operational profile. And they call that Monte Carlo testing, not to be confused with Monte Carlo simulation the way it's used in some Fault Tree Analysis techniques.

But the point is that there is substantial industrial experience and DOD experience in using those techniques to come up with the correctness of the software. It doesn't handle the issue of crashes and hangs, or what Charlie calls "lockups," but it does address the issue of whether the software is going to respond correctly to a particular challenge.

With respect to the hangs and crashes, and other things that can also affect operation and cause CCFs, we have, at least in the designs that we've seen, underlying the application software is the operating systems, and the operating systems are where we're going to see those effects. And by collecting the data in the right environments and with complete

control and visibility, you can get hundreds of thousands of hours of operating time in a reasonable amount of time and be using that.

Now, you have to set up the right environment to collect that data, and in some cases it has been done. And that can help.

I'm just making the point that, you know, you can't use operational experience because these failures are rare, but you can use tests and simulations to help get a better handle on that. And that's been done in other industries.

MR. CAMPBELL: I appreciate that input. I was taking some notes here.

Just associated with your point one regarding the examples, we do plan on working through some examples once the NEI 20-07 document is available to be reviewed and those conversations can occur. So, supporting the review of an implementation guidance, we would be looking to provide an example to demonstrate the efficacy and what the product of the process would be.

I appreciate your comments on the missile, you specifically within the defense industry. I was unaware of that. I think it will be interesting to take a look at that and see how it's been applied and

where we may be able to use something like that. Where my mind -- well, I don't know much about that, those applications, but we'll be interested in learning more. Appreciate the comment.

MEMBER DIMITRIJEVIC: I thought -- sorry.

CHAIRMAN BROWN: Go ahead, Vesna. Go ahead.

MEMBER DIMITRIJEVIC: I thought you said the examples are provided in the NEI 20-07, Draft D. So, that's what I was counting to see this week, but it is now said the examples will be provided later?

MR. CAMPBELL: So, yes, I'll clarify that. Thank you for that.

There is a high-level example that is in 20-07, Rev. D. It is a limited example that takes a look at just -- it takes one example of each step of the process, but not a fully-fledged example of what a digital modification or digital application using this would take a look at. For your questions, I felt like the example that was provided could be shown in how we apply that there.

MEMBER DIMITRIJEVIC: Okay. Thanks.

MR. HECHT: Vesna, if I could, if you type in "STPA Handbook MIT" into a browser, you will get an STPA Handbook, which was produced by Nancy Leveson and

John Thomas, which describes the process and provides not nuclear examples, but some other examples which could get you educated. It's a very well-written document.

MR. CAMPBELL: And just that it's included within the citations of the presentation that you see today. I will just note that STPA is one part of the overall process. As we discuss, there are other parts using Fault Tree Analysis.

And, Vesna, if I remember correctly, your questions were primarily on how we're utilizing --

MEMBER DIMITRIJEVIC: That's right.

MR. CAMPBELL: -- the risk pieces of it.

MEMBER DIMITRIJEVIC: It's Reg. Guide 1.174. Yes, that was primarily my question, and I'm sure if this was by Dr. Leveson, she wouldn't be in that area.

Okay. All right. Thanks.

MR. CAMPBELL: Thank you.

CHAIRMAN BROWN: Okay. I'd make one observation on that. When we deal with our strategic missiles, there's a few hundred million dollars now in running all those simulations and making them work. Even my program didn't have that kind of money to verify software and make sure every branch was tested,

to do that for our applications.

If we're finished with those discussions, I guess we've got seven of the members here. Any conclusions on how you all would like to proceed relative to a letter or no letter, and have a full Committee meeting, or what?

Joy, do you want to go first?

MEMBER REMPE: I'd have to unmute.

I'm looking some more at the agenda. And before I answer that question -- or I'm sorry, excuse me -- the rainbow chart. And before I answer that question, you've got another meeting that's appearing on the one that was most recently sent to us in September on the CCF SECY, which I assume is this document, right?

CHAIRMAN BROWN: Yes, but --

MEMBER REMPE: It's on September 23rd.

CHAIRMAN BROWN: -- it was a placeholder.

MEMBER REMPE: Okay. So, are you planning to, after the staff -- is that going to be before or after the staff sends it to the Commissioners?

CHAIRMAN BROWN: No, they've already done -- we didn't know, I had no idea of their schedule, the actual schedule they were working to. We put a placeholder because August we don't have a full

Committee meeting.

MEMBER REMPE: Right.

CHAIRMAN BROWN: Okay?

MEMBER REMPE: And so, you're willing to do everything, and your vision is that you're planning to look at whatever they issue and send up to the Commission, and then, write a letter if you feel like it? And that's why you're having this Subcommittee meeting --

CHAIRMAN BROWN: No.

MEMBER REMPE: -- if that were the one scenario?

CHAIRMAN BROWN: No, no. I wanted to know before in case we wanted to intervene and say, "Stop."

DR. BLEY: Charlie, that placeholder happened today, right? That's not a different meeting?

CHAIRMAN BROWN: No, there's one in September also we had.

DR. BLEY: Okay.

CHAIRMAN BROWN: We put a placeholder out in September.

Christina, are you there?

MS. ANTONESCU: Yes, I'm here, Charlie.

CHAIRMAN BROWN: That is a place -- I am

correct, we put that out there. Was that during full Committee week or Subcommittee week?

MS. ANTONESCU: It's Subcommittee week.

CHAIRMAN BROWN: Yes, that was a placeholder, I thought, for what we -- depending on what we got out of this meeting, if we needed to do more from a Subcommittee standpoint.

MS. ANTONESCU: Correct.

CHAIRMAN BROWN: That's why we put it there.

The thing here is, do we want to put out a straightforward letter, a simple letter, that says, "Staff, go forward."? Or do we want to remain silent while they go ahead and prepare their SECY and send it up to the Commission?

The only purpose of the letter would be that we would encourage them to -- the real point is we need to kind of encourage the Commission to buy into some additional flexibility for the staff to evaluate the diverse approaches.

MEMBER REMPE: So now that I kind of understand what you're saying, Charlie, I think it's great for you to write such a simple letter, but I sure would put a caveat that we haven't seen any text --

CHAIRMAN BROWN: Oh, yes, I got you.

MEMBER REMPE: -- and we might change our mind when we see what they send to the Commission. Because, I mean, this is a really awkward position, I think, to put ACRS in. It would have been nice if the staff would have gone ahead and written the paper, and we could say, "This paper looks great, except for item A or B," or "It's perfect. Please, Commission, we fully endorse what the staff has." But now they're putting us in a position to write a letter on some slides and an outline. And that's what I've been trying to convey. This is my other comment in the previous meeting.

CHAIRMAN BROWN: If they reflect the slides in the SECY, it addresses my major concern of maintaining the 7-19 conventional path. Okay? And I just don't want it to get, you know, entangled. That's why any letter I wrote would be a simple letter that says, "Hey, look, we need to go work on this. Get on with it, but here's a couple of points to maintain."

We can't lose sight -- we can't allow risk-informed to supplant the emphasis on architectures and design principles, and we can't -- we do not want it to dismember 7-19 in its current

form, so that you revise 7-19 like an appendix, or something. Those would be our suggestions in the letter, but that we say we agree with going forward.

Even though I'm not a big risk and PRA person, diversity is one of those areas we really ought to be trying to do and not overdo. And I've never taken that up in our previous three or four design applications that we've approved since I've been here.

And this was an opportunity to try to say, okay, yes, we agree with going that way, but let's just be careful about doing it. And I think that appears to be what the staff is doing. So, we could encourage that or support that in our letter, and then, see what they come up with. And if we disagree, we'll write a letter to the Commission.

MEMBER REMPE: Again, I'm sticking with what I said -- a simple letter, which, again, history says that's going to be challenging sometimes with your letters, but a simple letter, but a caveat saying that we've not seen the text.

CHAIRMAN BROWN: You had to say --

MEMBER REMPE: And just go on to the next person.

CHAIRMAN BROWN: You had to stick a spear

in my chest in public, right?

MEMBER REMPE: Always, Charlie, like you do me.

(Laughter.)

Next person, please.

CHAIRMAN BROWN: No, Dennis has volunteered to help me focus my thought processes.

(Laughter.)

So, if he's still on the line, I hope I didn't overstep my bounds, Dennis.

DR. BLEY: I'm still here, Charlie.

CHAIRMAN BROWN: Oh, okay. Did I overstep or --

DR. BLEY: Probably not.

CHAIRMAN BROWN: -- are you willing to help? Okay.

All right. Vicki, you had something else?

MEMBER BIER: Yes. I come down kind of similar to Joy in a way, that it seems like the whole process is still a little amorphous for ACRS to comment intelligently. And maybe that's just that it's amorphous in my head and I haven't understood it thoroughly enough.

But I'm kind of on the fence. You know, I understand Joy's comment about we could write a very

simple letter reiterating a few basic principles and advising caution, or whatever. But it's not clear to me that I have at least enough information and understanding. I could also go with not writing a letter and just waiting to weigh in later, when we know more about what they're doing.

CHAIRMAN BROWN: Do I hear from any other -- that is the other path. We could do that.

The only observation -- I lost my train of thought.

By making some points in this letter, in a letter right now, we at least get some of the fundamental principles reemphasized, as opposed to waiting. I mean, the nice thing about the existing SECY -- what is it? -- 93-087, is it's very clear. Okay? It says these circumstances, diversity. It's very clear.

So, it all depends on how the staff proposes in their SECY, and we have not seen -- they've shown us what they say they're going to say in terms of the dual path. It's not sure, once it gets to the Commissioners, how it will come out of the Commissioners in an SRM. I mean, the Commissioners are the Commissioners.

MEMBER KIRCHNER: Charlie, this is Walt.

CHAIRMAN BROWN: Yes? Yes?

MEMBER KIRCHNER: Is there any compelling reason to write a letter right now?

CHAIRMAN BROWN: No, it --

MEMBER KIRCHNER: It would seem to me --

CHAIRMAN BROWN: No, I'm happy they're not destroying -- don't use that word literally, okay? I'm sorry for saying it that way.

MEMBER KIRCHNER: You seem to be confident in the direction they're taking.

CHAIRMAN BROWN: Yes.

MEMBER KIRCHNER: You agree with, I'll call -- well, there's Charlie's principles, and then, the principles that they put into this outline that we've seen and the viewgraphs.

CHAIRMAN BROWN: Yes, they're not throwing the baby out with the bath water.

MEMBER KIRCHNER: Right. So, there's no indication of that. So, it would seem to me -- I don't know what the estimated date for a draft of the SECY is -- but it would seem to me we could wait until we see a draft version. And we don't even need to have another Subcommittee. We could take it up if you felt -- if you felt that we should write a letter for or against, there's no need for another Subcommittee

meeting. Once we have the document, we could read it in advance; you could walk through it, and you could present a draft letter to the full Committee.

CHAIRMAN BROWN: Well, and they could make a presentation at the full Committee.

MEMBER KIRCHNER: Yes, and if that was warranted, that, too.

CHAIRMAN BROWN: That's fine with me. I do not have to write a letter to express any concerns I had. I think they've put together an approach that maintains the status quo, but opens the door to other considerations without impacting those. So, I'm satisfied from that standpoint. I wasn't a month ago.

MEMBER KIRCHNER: So, when we see the draft, we can write an "attaboy" letter or, if we see in the draft -- you know, trust but verify -- we've got a concern, you can do an "attaboy" and document the concern, and send that on its way.

Is the September-October timeframe for a letter okay?

CHAIRMAN BROWN: If it's after the fact, it could be September-October without any question.

Eric, you said you're going to be trying -- are you still on the line?

MR. BENNER: I am on the line and --

CHAIRMAN BROWN: Can I ask you a question? You said you all were going to be trying to get this to the Commission in July?

MR. BENNER: That is correct.

I wanted to make two points. One, that that is the current timeframe that we have aligned with the Commission on, is to have the paper up to them in the July timeframe.

Another point I wanted to make is that this is the policy. I think Member Brown has accurately captured that what we're trying to do is not make any decisions about methodology, licensing decisions. None of that is today. This is opening the door on the policy because of this hard stop that says, if a safety function could be disabled by a CCF, thou shalt have diversity.

Any implementing guidance that we would subsequently develop or, for that matter, any major licensing action which would adopt that approach would also come before the Committee for review. So, that's not to try to get you not to do something, if you feel you should do something. But, at least from the staff level, this is strictly focused on opening the aperture to use risk insights on this particular aspect that's contained in the current digital I&C CCF

policy.

CHAIRMAN BROWN: Thank you for that, Eric.

That's why I'm comfortable with doing nothing. I would just soon not write another letter.

DR. BLEY: But --

CHAIRMAN BROWN: Yes, Dennis, go ahead.

DR. BLEY: I would just say something, given the discussion the Committee had. If the Committee wants to have some influence on the Commission's decision on this SECY, writing a letter now would do that. Writing a letter a month or two months after the SECY goes up might be too late. They might have already acted. On the other hand, sometimes they sit up there for a couple of years before they get acted on.

(Laughter.)

CHAIRMAN BROWN: Yes, that is the other approach. Because, I mean, if in this letter we just point these other things out, but we say we agree with the staff approach, that at least lets the Commission know that we're onboard with it.

The problem is we haven't seen the actual language. So, the argument for not writing a letter now would be that we haven't seen the -- do we want to commit ourselves when we haven't seen the actual

language?

MEMBER REMPE: Is there any way that this plan to send it up to the Commission in July is going to get delayed? Because I've heard things before and things often get delayed.

MR. BENNER: I mean, I wouldn't want to assess a probability for that.

(Laughter.)

MEMBER REMPE: Well, by the full Committee meeting in a couple of weeks, will you have more insights about that? Or you think, no, there's not going to be any change in the next couple of weeks?

MR. BENNER: I mean, the staff is responding to our interactions with our senior management on the Commission expectations for when they would like to see this paper.

I would say that the staff has done a lot of heavy lifting, and I feel comfortable saying that, you know, the paper we would write, right, that we would provide to the Commission, will reflect exactly what we presented to you today. Now any such paper has to go through concurrences, but, on this paper, we have been, you know, sharing this information, the key messages, up our management chain.

We have, like I said, a diverse set of

people on the working group, including legal representation, to ensure that the direction we're going, it fits within these constraints we've outlined for ourselves; i.e., the PRA policy statement, safety goal policy statement, existing regulations, whatnot.

And like I said, we were going to have these three interactions -- today, the full Committee meeting on June 1st, and a public meeting on June 8th -- mainly, to tell people where we were going. And the only course correction we were going to do is, all of a sudden, if there was like a fatal flaw that we believe we have missed.

And I can tell you that, from what I've heard today, we have not heard anything that we think is a fatal flaw. We've heard definitely some things we want to consider, and we want to look more closely at all the work that's been done on the Licensing Modernization Project to see if there's some synergies there we should leverage.

But that's where we're at. I mean, our marching order today is we've done what we think is the heavy lifting and the heavy thinking. And now, we're just marching towards making a recommendation to the Commission that aligns with the messaging we've given you today.

MEMBER REMPE: So, wouldn't it be better, from a staff perspective, to have this simple letter, which I hope it's simple, saying we think the staff's going the right way, but we want to make -- I always want to cover my options, and leave an option in from an ACRS member, and say, "By the way, we haven't seen the text and they may change things, and we'll let you know if that happens," or something like that. Because it's kind of a wishy-washy letter in some respects, but I think it's better for you to have that letter than to just be silent, and then, come in late, don't you think?

MR. BENNER: Uh-hum. What you've just verbalized is clearly factual. So, given -- and I don't want to put words in the Committee's mouth -- but, given what you've heard today, you think the approach is the right direction for the staff to be going in, but you haven't seen the paper. So, the views you're expressing are not based on a complete paper. And you could even weave in what I just said, that, ultimately, any implementing guidance we would expect to be offered to the Committee for review.

MEMBER REMPE: And then, P.S., it would be nice if the staff would have us a little earlier in the process in a more orderly fashion. Now, well, the

Committee will decide what goes in there, but, I mean, that's where I've kind of been --

MR. BENNER: I mean, I will say we have been challenged to try to make sure we're having the right, all of the right stakeholder touchpoints, to make sure that whatever we're sending to the Commission, we're fully aware of all the stakeholder views.

I mean, the staff's been working hard because we've had to do a lot of homework, right? I think Christina told me that it was something like 20 documents we provided you in preparation for this meeting. And I can assure you the staff has done a lot of homework into the looking at the history on this particular subject, the policy as encapsulated in 93-087. But, obviously, a lot of looking at all the other risk-informed guidance that has propagated since 1993, to leverage that in how we think we should change this policy. So, the staff's been very busy on this --

MEMBER REMPE: I know.

MR. BENNER: -- and we appreciate --

MEMBER REMPE: It's just that the process is a little different.

Anyway, I'm still with my position,

Charlie.

CHAIRMAN BROWN: Yes, the only downside to us writing a letter right now, a simple letter which I think I could -- I'm not quite sure how I'd do that. How much time do I have? I've only got about 10 days to do that, but I can give it a shot.

The only downside is we end up saying we agree with the staff's approach it's trying to take on this issue. And then, if it comes out they do something different in their actual paper than what is here, because of the interactions with some of the concurees, then we have egg on our face.

MEMBER REMPE: No, not really, because I want a caveat in that letter, or I'll do added comments saying that, you know, I think the members should have acknowledged that we haven't seen this; all we saw were slides. We knew there was going to be a subsequent stakeholder meeting, and staff changed their mind. And I will promise you I'll do added comments if you write a letter that doesn't have such a hook in it that says --

CHAIRMAN BROWN: No, I would put a hook in it.

MEMBER REMPE: Yes.

CHAIRMAN BROWN: Don't worry about that.

I'm not that old. I'm not that dumb.

MEMBER REMPE: But, anyway, so I don't think there's any risk to us. It just makes it very clear that this thing was kind of out of process and we're putting in something to support the approach, even though we haven't seen the document.

CHAIRMAN BROWN: Other members? We've only got two people voting here.

Vesna? Open your mic. Are you still there? I didn't look. Did I lose Vesna?

MEMBER REMPE: I don't see her there.

MEMBER DIMITRIJEVIC: Sorry. I'm here. I'm here. I tended to some delivery and I was just in the door, but I heard all the discussion.

Okay. So, tell me, what did you ask me? What did --

CHAIRMAN BROWN: We've got seven members here. We've got you, Ron, Dave, Vicki, Walt, Joy, and me. Okay? So, we've got seven -- I think that's seven.

MEMBER SUNSERI: And Matt.

CHAIRMAN BROWN: And Matt. I'm sorry, I missed you, Matt. You were up on the next line.

So, we've got enough. I could write a letter. I know Joy has great angst at me writing a

simple letter that's other than 452 lines long and 10 pages. But Dennis will help me out, I'm sure, on a consultant basis.

So, I will make that effort to write a simple letter that just says we agree that they're going in the right direction, and then, try to figure out the right -- but we have not seen the actual language of the SECY at this time, something of that nature.

MEMBER DIMITRIJEVIC: Well, I have no problem with you writing that letter. But if you don't think we need to write the letter, I also don't have a problem with that, either. So, I'm good on both of those things.

Now my mind thinks it was interesting they will not be part of this letter. They connected to this NEI approach.

CHAIRMAN BROWN: Yes.

MEMBER DIMITRIJEVIC: So, I am good with whatever you feel like should be done.

CHAIRMAN BROWN: Okay. Ron? Are you there?

(No response.)

Dave?

MEMBER REMPE: Dave I know is gone.

CHAIRMAN BROWN: Oh, okay.

Vicki, you didn't see the need for a letter, right?

MEMBER BIER: Correct. I don't object to writing one, but I don't think it's necessary at this time.

CHAIRMAN BROWN: Okay. Matt?

MEMBER SUNSERI: I have the same opinion as Vicki.

CHAIRMAN BROWN: Okay. Vicki's a no. Matt's a no. Vesna is --

MEMBER DIMITRIJEVIC: Whatever you, as Subcommittee Chairman, feel like, I'm with you.

CHAIRMAN BROWN: So, either?

Ron hasn't answered yet.

Who am I missing? Walt?

MEMBER KIRCHNER: I align with Vicki and Matt, but I'm neutral.

CHAIRMAN BROWN: You align with no?

MEMBER KIRCHNER: Yes, "no."

CHAIRMAN BROWN: So, there's three and a half noes.

And where's Ron? Is he there yet? Ron?

(No response.)

Ron's always getting -- his internet

connection blows out on him frequently.

So, we've got three and a half to one, plus me. So, it's three and a half to two noes and two, one and a half yeses.

So, if we don't write a letter, we don't need the full Committee meeting presentation. Isn't that right, Joy?

MEMBER REMPE: That's true. I wouldn't see a reason for the staff to be presenting to us.

CHAIRMAN BROWN: Yes, I agree with that.

Now, the only thing I'm dealing with is that you are the Chairman. If you demand a letter, we will do a letter.

MEMBER REMPE: I don't think the Chairman has that right. I'll go back and look at the Bylaws, but I can't do that.

CHAIRMAN BROWN: I don't know. I mean, I just -- then, I would suggest we go ahead and wait to see.

I have confidence that the staff has put out what they're going to be representing. And I hope, Eric, if something deviates from that, you all would let us know.

MEMBER REMPE: No, because this has gone back and forth so much -- you know, Jose did just a

little paragraph and came at P&P and said, "Hey, the Subcommittee said no letter was needed."

We heard this, and it's just your opinion. Don't make it five pages or even two or three, more than two or three paragraphs. But say we heard about this; the approach sounds good, but the Subcommittee recommended that we not provide a letter until we actually see it.

You see what I'm saying? I think that's a nice way to close the fact that the staff did come and that you, the member, thought their approach sounded good. Would you be willing to do a paragraph, Charlie?

CHAIRMAN BROWN: Who do I send the letter to? Who do I send the letter to? To myself?

MEMBER REMPE: No, it's not even a memo. It's a paragraph. It's presented at P&P, like Jose did last month. I'm sure that Christina can help you by looking at what was done last month with Jose's thing. Or maybe it's two months ago. Sometimes I'm a month off.

But I think it's a nice way to just document that this occurred.

CHAIRMAN BROWN: Is it one of the numbered items in the schedule?

MEMBER REMPE: It's in the P&P, like the handout that it has.

CHAIRMAN BROWN: Yes.

MEMBER REMPE: But, you know, we can talk about that offline. But I think that would be a nice way to close this discussion that acknowledges that the staff came, and that you supported it; that the Subcommittee supported the approach. We thought, though, a letter wasn't needed at this time because we haven't seen the final language.

CHAIRMAN BROWN: Okay. I'll do a --

MEMBER REMPE: And, yes, if you have any questions, give me a call.

CHAIRMAN BROWN: It will be three or four sentences.

MEMBER REMPE: Yes, just a few sentences. Yes, and you can send it to me, and I can look at it. But, again, it's similar to what Jose did.

CHAIRMAN BROWN: Hold on. Hold on.

MEMBER REMPE: Uh-hum.

CHAIRMAN BROWN: You're overworking me here.

(Laughter.)

MEMBER REMPE: Okay.

CHAIRMAN BROWN: I'm 80 years old. How do

you expect me to absorb all this?

(Laughter.)

MEMBER REMPE: We can talk offline.

CHAIRMAN BROWN: I will put together three or four sentences along your suggested line.

MEMBER REMPE: Okay, and send it to me, and I can tweak it, if you want to take my comments, but it's just a nice way to end the whole situation.

CHAIRMAN BROWN: I'll send it to Christina, and she can make sure Larry has it for the P&P preparation, or whoever does that. And you can look at it in whatever process, and I'll send a copy to you.

MEMBER REMPE: Wonderful.

CHAIRMAN BROWN: Dennis, do you have any other observations?

DR. BLEY: No, it's a committee thing.

CHAIRMAN BROWN: Yes, okay. Good.

DR. BLEY: It's up to you guys.

CHAIRMAN BROWN: I know you're a consultant, but you're an important consultant.

So, that's good. Okay.

Eric, are you still there?

MR. BENNER: I am.

MEMBER REMPE: I see hands up from Myron

and Vicki. Are they old hands or are they new questions or comments?

CHAIRMAN BROWN: I don't know.

We've made a decision. There will be no letter and there will be no full Committee meeting.

MR. BENNER: With what you said, we will commit to, you know, after that stakeholder meeting, to find a way -- maybe it would be as simple as in the meeting. So, we'll find a way to provide a communication to the Committee as to any changes we've made.

MEMBER REMPE: That would be good, just to make sure. Because you may get a letter in September or October that you didn't want.

MR. BENNER: You'll get the paper when it's done. But we'll look for a way, after we're having those stakeholder interactions, to overtly describe any changes that we made. Any -- I mean changes that are from what we presented today.

Even today, we clearly have heard things today that we want to polish our messaging and our language and our presentation for that, that stakeholder meeting. But we haven't heard anything today that changes the philosophy of the paper and the key messages of the paper.

CHAIRMAN BROWN: Yes, the only other things I would have put in a simple letter were the idea that they've taken an approach similar to ISG-06, where you had an alternate review and you made it separate. Okay?

MR. BENNER: Yes.

CHAIRMAN BROWN: And whatever we do -- but that will be a BTP 7-19 review.

MR. BENNER: That's an implementation piece.

CHAIRMAN BROWN: Yes.

MR. BENNER: And we've heard that, and we talk about it offline. I mean, obviously, when we go putting pen to paper, we'll have to see how it best works out, but when we talked internally, we certainly don't have any objection to that. Because, just like we did on the ISG, right, it's an alternate pathway. So, clarity in the implementing guidance as to how people do the different pathways, we certainly support that philosophically.

CHAIRMAN BROWN: The other thing to bear in mind -- and this is a separate subject. Okay? Do you remember when we did 7-19, Rev. 8, we had a recommendation to include something relative to unidirectional communications?

MR. BENNER: Uh-hum.

CHAIRMAN BROWN: Which you ended up not -- not "you" personally, okay? -- but the staff did not incorporate because it was in the cyber world.

MR. BENNER: Uh-hum.

CHAIRMAN BROWN: 5.71 now says you can use methods for design purposes. It's in the first couple of page now, the preamble.

If we do another revision, again, that's a subject. Just bear in mind you will be hearing from me that we ought to --

MR. BENNER: Okay. We made the commitment that the next version of BTP 7-19 would definitively come to the Committee.

CHAIRMAN BROWN: Yes.

MR. BENNER: So, solely expect, as part of our closeout to the EDO for EDO's recommendations.

CHAIRMAN BROWN: That's good. All right.

MR. BENNER: No surprises.

CHAIRMAN BROWN: And I didn't want you to be surprised because you know I will be on that one like -- I hate to use the term --

MR. BENNER: I would be surprised if you weren't.

(Laughter.)

CHAIRMAN BROWN: Okay.

Any other comments from anybody?

(No response.)

Okay, I don't hear any. That's the five-second rule again.

MS. ANTONESCU: But, Member Brown, the public also might like to have --

CHAIRMAN BROWN: Oh, I forgot. Thank you very much, Christina.

I take it the lines are open and all that.

We're at the end now. Is there any public comment?

I think, some circumstances, you may need to hit *6 in order to make yourself heard. But, other than that, unmute yourself and identify yourself and who you're with, if you're with anybody, and make your comment.

(Pause.)

That's the 10-second rule.

I'll pass on that.

And I'm going to go on to my final comments.

I do want to thank the staff and NEI for two very, very good presentations.

I thought the discussions that we got into

were informative. And personally, I think a lot of the information you presented now is better understood by the overall Committee. We had seven of the full Committee here. So, I think that was beneficial to hear this a little bit down in the weeds.

So, I thought you all, you presenters, did a good job, and I much appreciate your efforts on a nice, crisp presentation, both on the staff's side and on the NEI side.

With that, I will adjourn the meeting. Thank you all completely.

(Whereupon, at 5:14 p.m., the Subcommittee was adjourned.)

NEI Common Cause Failure Policy Input

Alan Campbell
Technical Advisor

NUCLEAR ENERGY INSTITUTE

State of Digital I&C

- The Digital I&C Integrated Action Plan (IAP) has improved regulatory guidance clarity and consistency
  - RIS 2002-22 Supplement 1 provided criteria for qualitative assessments of Common Cause Failure (CCF) in low safety significant safety-related systems.
  - BTP 7-19 Revision 8 incorporated graded approach assessments into staff review guidance
  - NEI 96-07, Appendix D and Reg. Guide 1.187 Rev. 3 provided enhanced guidance for digital systems under 50.59
  - DI&C-ISG-06 Rev. 2 provided an Alternate Review Process to improve regulatory confidence for digital safety systems upgrades.

Why Digital Safety Systems?

- Existing systems are reaching (or have already reached) obsolescence
- Enhances safety via system diagnostic capabilities to identify and respond to issues
- Improves plant performance via improved accuracy, processing time, and automated capabilities
- Provides more data available to Operations, Maintenance and Engineering resulting in better real-time knowledge
- Reduces hardware inventory compared to existing systems

Supports long-term, safe operation of our plants

Today's Digital Landscape

- Digital I&C technology has design features that provide for deterministic behaviors through the use modern standards
- International standards, such as IEC/IEEE, are widely accepted and have stable processes to reflect current understanding
- Hazard analysis techniques have matured and are used extensively in non-nuclear safety industries (such as aviation/aerospace, defense, automotive, and chemical industries)

NRC needs a modernized digital CCF policy that reflects today's technology, experience, and understanding

Applicable Regulation

- 10 CFR 50.55a(h) – Codes and Standards, Protection and safety systems
  - Requires compliance with either IEEE 603-1991 or IEEE 279-1971
- IEEE requirements
  - Both IEEE standards require means to implement manual initiation of protection actions
  - Neither IEEE standard requires diversity
- RG 1.62 – Manual Initiation of Protective Actions
  - Provides guidance for manual initiation/control to meet IEEE requirements
  - Provides a staff position that diversity is required to meet BTP 7-19.

Required codes and standards specify a means for manual initiation of protection actions, BUT do not specify diversity as a requirement.

Applicable Regulation

- 10 CFR 50.62 – Anticipated Transient Without SCRAM (ATWS)
  - PWRs
    1) Must have diverse means of automatic Auxiliary (or Emergency) Feedwater Initiation and Turbine Trip
    2) Must have diverse SCRAM system (CE and B&W only)
  - BWRs
    3) Must have diverse Alternate Rod Injection system
    4) Must have standby liquid control system (no diversity requirement)
    5) Must have reactor coolant recirculation pump trip (no diversity requirement)

ATWS requirements for diversity are limited to specific functions and do NOT require manual, system-level actuation.

Applicable Regulation

- 10 CFR 50 Appendix A, General Design Criteria 22 – Protection System Independence
  - *The protection system shall be designed to assure that the effects of natural phenomena, and of normal operating, maintenance, testing, and postulated accident conditions on redundant channels do not result in loss of the protection function, or shall be demonstrated to be acceptable on some other defined basis.* ***Design techniques,*** *such as functional diversity or diversity in component design and principles of operation****, shall be used to the extent practical to prevent loss of the protection function.*** [emphasis added]

Design techniques **are required to prevent loss of the protection function.**

How Are We Addressing CCF Today?

- Branch Technical Position 7-19, Rev. 8
  - Eliminate
    - Diversity within system or component
    - Testing
    - Alternative Methods
  - Mitigate
    - Existing System
    - Manual Operator Action
    - New Diverse System
  - Acceptance
    - Bounding acceptance criteria

How Are We Addressing CCF Today?

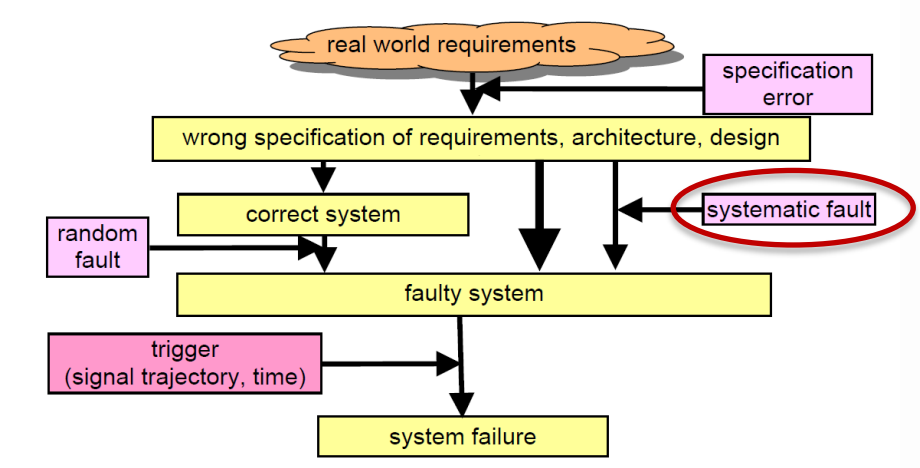
- Branch Technical Position 7-19, Rev. 8
  - Eliminate
    - Diversity within system or component
    - ~~Testing~~
    - ~~Alternative Methods~~
  - Mitigate
    - Existing System – Requires “sufficient diversity”
    - Manual Operator Action – “SSCs used to support the manual operator action are diverse”
    - New Diverse System – Requires “sufficient diversity”
  - Acceptance
    - Bounding acceptance criteria

How Are We Addressing CCF Today?

- Branch Technical Position 7-19, Rev. 8
  - Eliminate
    - Diversity within system or component
  - Mitigate
    - Diversity using Existing System
    - Diversity using Manual Operator Action
    - Diversity using New Diverse System
  - Acceptance
    - Bounding acceptance criteria

How Are We Addressing CCF Today?

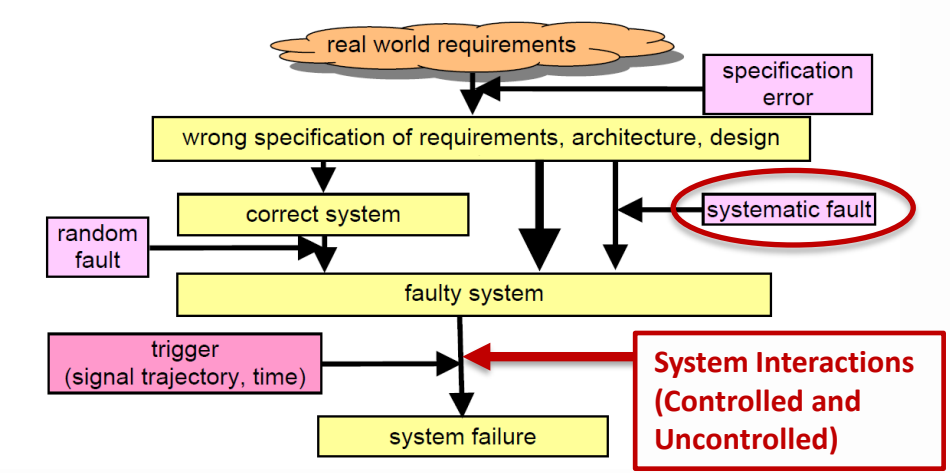
Primary System #1



NRC Digital Instrumentation & Control Training, Module 3.0
Regulatory Concerns, Figure 3-22

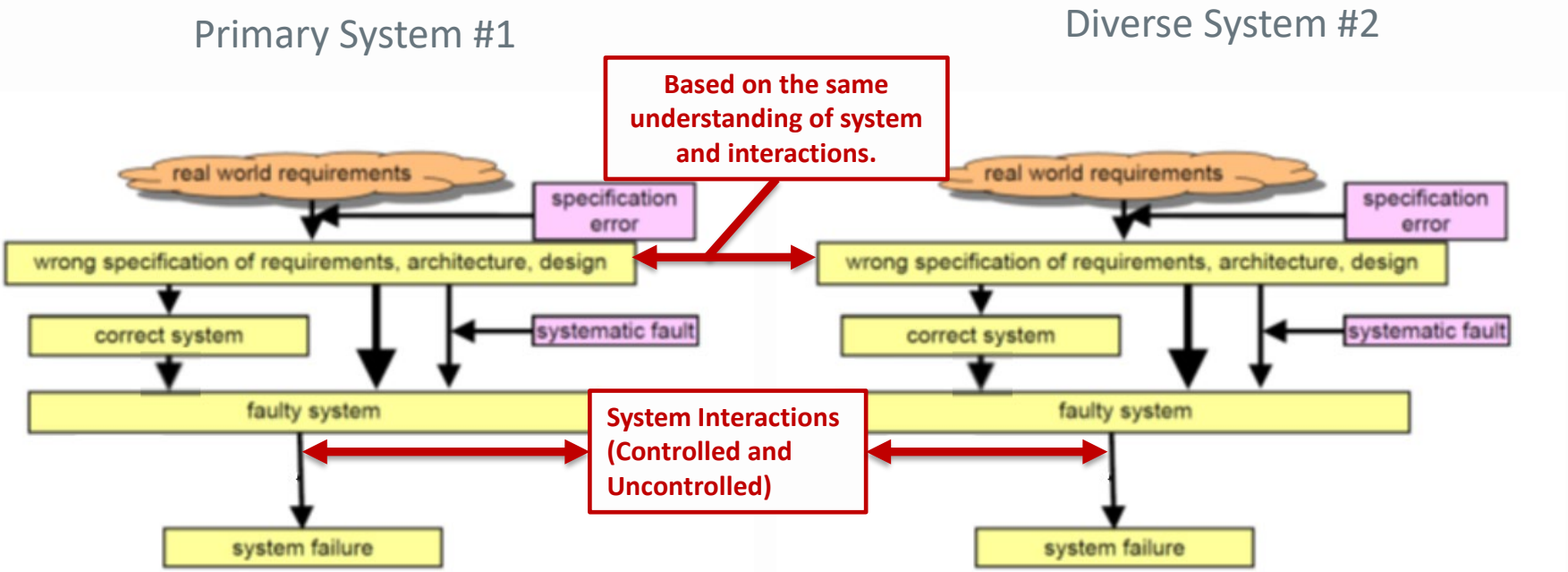
How Are We Addressing CCF Today?

Primary System #1



NRC Digital Instrumentation & Control Training, Module 3.0
Regulatory Concerns, Figure 3-22

How Are We Addressing CCF Today?



How Are We Addressing CCF Today?

- I&C OE (nuclear and non-nuclear) indicates that most systematic failures are a result of:
  - Latent design defects due to inadequate requirements
  - Uncontrolled system interactions
- An EPRI study on nuclear events[1] indicate that the primary contributing factor is requirements errors

Diversity MAY be useful in addressing hazards (e.g., CCF), BUT:

1. **Diversity CAN increase plant complexity and errors.**
2. **Diversity MAY NOT address all sources of systematic failures.**

1. EPRI 3002005385

How Are We Addressing CCF Today?

- I&C OE (nuclear and non-nuclear) indicates that most systematic failures are a result of:
  - Latent design defects due to inadequate requirements
  - Uncontrolled system interactions
- An EPRI study on nuclear events[1] indicate that the primary contributing factor is requirements errors

Industry solution to CCF is a diagnostic approach to addressing systematic failures proven effective in other industries and research.

1. EPRI 3002005385

Proposed Implementation Guidance

- NEI 20-07 Rev. D
  - Leverages EPRI Hazards and Consequence Analysis for Digital Systems[2] and Digital Reliability Analysis Methodology[3]
  - Provides a diagnostic approach to addressing systematic failure beginning during early stages of design process
    - Identifies missing, inadequate, or incorrect requirements
  - Diagnoses system architecture for unsafe control actions
  - Uses risk-insights to address hazards commensurate with plant risk

2. EPRI 3002016698
3. EPRI 3002018387

Research Basis

- EPRI investigated strengths and limitations of various hazard and failure analysis techniques[4]
- EPRI HAZCADS and DRAM combines Fault Tree Analysis (FTA) and Systems Theoretic Process Analysis (STPA)
  - Complementary strengths
  - Reduces limitations of each method used on its own

4. EPRI 3002000509

Proposed Implementation Guidance

- The applicant will:
  - apply Systems Theoretic Process Analysis (STPA) to diagnose the system architecture and determine specific loss scenarios leading to hazards
  - perform a Fault Tree Analysis (FTA) to determine the risk impact of loss scenarios
  - map results of FTA to RG 1.174 Figures 4 and 5 regions (graded approach)
  - apply control methods to address each loss scenario of STPA commensurate with results from FTA mapping

Systems Theoretic Process Analysis

- Diagnostic tool that iteratively analyzes requirements, design and system interactions

5. STPA Handbook, https://psas.scripts.mit.edu/home/get_file.php?name=STPA_handbook.pdf

Systems Theoretic Process Analysis

- Efficacy proven through blind studies
- Example blind study[6]
  - Real incident caused by digital I&C system analyzed
  - Participants were familiar with STPA and blind to the selected OE
  - Participants provided general description of the system as it existed prior to the incident
  - STPA results compared to actual flaws that led to OE

STPA anticipated exact flaw that led to OE.
STPA also identified ~9 other scenarios unaccounted for in the design.

6. EPRI 3002000509

Systems Theoretic Process Analysis

- Utilized in non-nuclear industries (automotive, aviation, chemical, defense, etc.)
  - Automotive Standards:
    - ISO/PAS 21448, SOTIF: Safety of the Intended Functionality
    - SAE J3187, Recommended Practice for STPA in Automotive Safety Critical Systems
  - Aviation Standards:
    - RTCA DO-356, Airworthiness Security Methods and Considerations
  - Cyber Security Standards:
    - NIST SP800-160 Vol 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach
  - Standards in Progress:
    - ASTM WK60748, Standard Guide for Application of STPA to Aircraft
    - SAE AIR6913, Using STPA during Development and Safety Assessment of Civil Aircraft
    - IEC 63187, Functional Safety – Framework for safety critical E/E/PE systems for defence industry applications
    - IET 978-1-83953-318-1, Code of Practice: Cyber Security and Safety

Systems Theoretic Process Analysis

- NuScale used STPA to perform a hazards analysis of I&C systems
  - DCA[7] describes how STPA was used to analyze I&C systems
  - SER[8] provides NRC acceptance of hazards analysis

SER, Chapter 7 Section 7.1.8.6
The NRC staff concludes that the application provides information sufficient to demonstrate that ***the proposed HA has identified the hazards of concern, as well as the system requirements and constraints to eliminate, prevent, or control the hazards****. The NRC staff also concludes that* ***the HA information includes the necessary controls for the various contributory hazards, including design and implementation constraints, and the associated commitments****. The QA measures applicable to HA for developing the I&C system design conform to the QA guidance in RG 1.28 and RG 1.152. […] On this basis, the NRC staff concludes that the application provides information sufficient to demonstrate that* ***the QA measures applied to the HA for I&C system and software life cycle meet the applicable QA requirements*** *of GDC 1 of Appendix A to 10 CFR Part 50; Appendix B to 10 CFR Part 50; and Section 5.3 of IEEE Std. 603-1991. [Emphasis added]*

7. https://www.nrc.gov/docs/ML2022/ML20224A495.pdf
8. https://www.nrc.gov/docs/ML2020/ML20204B028.pdf

Benefits of Risk

- “Risk-Informed” v. “Risk-Insights”
- Better system function allocation between components
- Better understanding of the impacts of system architectural decisions
- Inform the use of measures to address a potential common cause failure based upon risk significance
- Understand risk impact to specific loss scenarios

Proposed Risk Guiding Principles

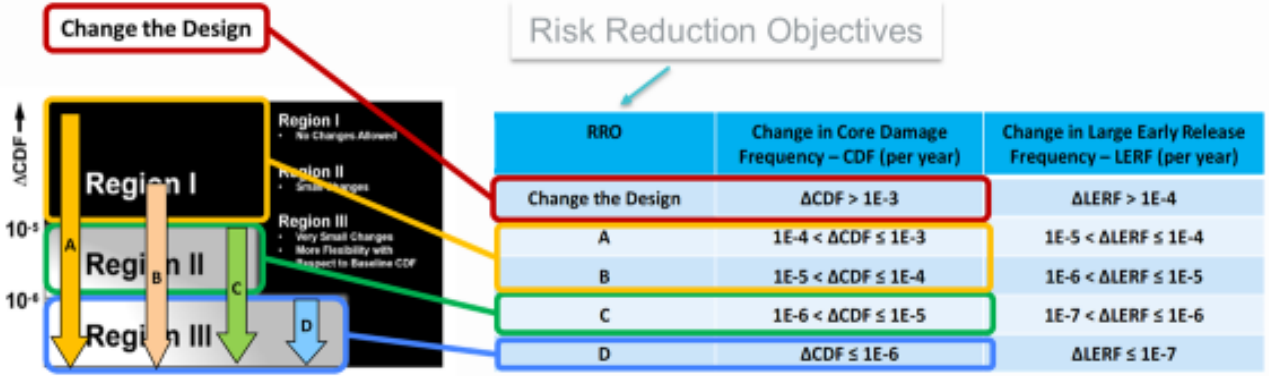
- Common-Cause Failure (CCF) SECY Paper Outline, “Guiding Principles”
  - All five principles of risk-informed decision making, as listed in RG 1.174, need to be addressed satisfactorily.
  - The PRA used for risk-informed approaches needs to be technically adequate (e.g., meets the guidance in RG 1.200) and include an effective PRA configuration control and feedback mechanism.
  - The expanded policy needs to ensure that the introduction of digital I&C does not significantly increase the risk of operating the facility.

Proposed Risk Guiding Principles

- Due to challenges modeling Digital I&C software reliability in PRA:
  - The absolute risk impact of software reliability cannot be quantitatively measured without substantial uncertainties
  - The effectiveness of applied design techniques cannot be quantitively measured without substantial uncertainties
  - There are no means of comparing design techniques to using diversity without substantial uncertainties
- NEI 20-07 Rev. D leverages concepts from RG 1.174; however, it is not completely applicable
  - This RG is used in the context of licensing basis changes, not design decisions

How Can We Use Risk Insights?

- NEI 20-07 utilizes Fault Tree Analysis to assess the risk sensitivity of each loss scenario
- The result of the sensitivity analysis is mapped to the CDF/LERF regions and used in a graded approach to apply control measures



RRO	Change in Core Damage Frequency – CDF (per year)	Change in Large Early Release Frequency – LERF (per year)
Change the Design	ΔCDF > 1E-3	ΔLERF > 1E-4
A	1E-4 < ΔCDF ≤ 1E-3	1E-5 < ΔLERF ≤ 1E-4
B	1E-5 < ΔCDF ≤ 1E-4	1E-6 < ΔLERF ≤ 1E-5
C	1E-6 < ΔCDF ≤ 1E-5	1E-7 < ΔLERF ≤ 1E-6
D	ΔCDF ≤ 1E-6	ΔLERF ≤ 1E-7

Policy Considerations

- Allow for graded approaches based upon plant risk-insights to ensure applicants focus on the most risk-significant functions and to provide flexibility in meeting established system performance criteria.
- Consider the full plant defense-in-depth strategy to prevent (to the degree practicable), mitigate, or respond to a digital common cause failure.
- Allow for the use of modern hazards and/or reliability analysis techniques to examine the system for adverse conditions and identify appropriate system requirements to prevent systematic failures.
- Expand the ability to use design techniques, including diversity when applicable, to prevent (to the degree practicable), or mitigate a digital common cause failure in accordance with GDC 22.

Example Policy

1. The applicant shall assess the impact of the proposed digital instrumentation and control Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) on the plant's defense-in-depth systems and procedures to demonstrate that vulnerabilities to digital common cause failures have been adequately addressed.
2. The applicant shall identify each digital common cause failure that could adversely impact a safety function using risk-insights, and hazards and/or reliability analysis techniques.

Example Policy

3. The applicant shall demonstrate commensurate with the risk significance of each identified digital common cause failure adequate measures to address the identified digital common cause failure that could adversely impact a safety function. The measures may include non-safety systems or components if they are of sufficient quality to reliably perform the necessary functions and with a documented basis that the measures are unlikely to be subject to the same common cause failure. The measures may also include monitoring and manual operator action to complete a function.

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

Expansion of Current Policy Regarding Potential Common-Cause Failures in Digital Instrumentation and Control Systems

Advisory Committee on Reactor Safeguards
Digital Instrumentation & Controls Subcommittee Briefing
May 20, 2022

Technical Staff Presenters

- **Samir Darbali** – Electronics Engineer, NRR/DEX
- **Norbert Carte** – Senior Electronics Engineer, NRR/DEX
- **Steven Alferink** – Reliability and Risk Analyst, NRR/DRA

Digital I&C Project Managers

- **Bhagwat Jain** – Senior Project Manager, NRR/DORL
- **Michael Marshall** – Senior Project Manager, NRR/DORL

Working Group Members

- **NRR/DEX**
  - Norbert Carte
  - Samir Darbali
- **NRR/DRA**
  - Steven Alferink
  - Shilp Vasavada
  - Sunil Weerakkody
- **NRR/DSS**
  - Charley Peabody
- **NRR/DORL**
  - Bhagwat Jain
- **OGC**
  - Sheldon Clark
- **RES/DE**
  - Sergiu Basturescu
- **Additional NRR/DEX and DORL Support**
  - Wendell Morton
  - Ming Li
  - Michael Marshall
  - Khoi Nguyen
  - David Rahn
  - Richard Stattel
  - Michael Waters
  - Steve Wyman

Presentation Outline

- Introduction and Key Messages
- Background
- Subject and Purpose
- Proposed Expanded Policy
  - Current Path
  - Risk-Informed Path
- Status of Draft SECY Paper and Next Steps

Introduction

- Nuclear power plants continue to install digital I&C technology
  - Increased reliability and safety benefits
  - Can introduce new types of types of potential systematic, nonrandom, concurrent failures of redundant elements (i.e., CCFs)
- SRM-SECY-93-087 directs that, if the D3 assessment shows that a postulated CCF could disable a safety function, then a diverse means be provided to perform that safety function or a different function
  - Diverse means may include manual actions
  - The current policy does not allow for the use of a risk-informed approach to determine specific circumstances that would not require a diverse means for addressing DI&C CCFs
- The staff is developing a SECY paper that will provide recommended language for an expanded policy, which allows greater use of risk-informed approaches to address DI&C CCFs

Key Messages

- The expanded policy will encompass the current points of SRM-SECY-93-087 (with clarifications) and expand the use of risk-informed approaches
- Any use of risk-informed approaches will be expected to be consistent with the Safety Goal Policy Statement, PRA Policy Statement, and SRM-SECY-98-0144
- The current DI&C CCF policy will continue to remain a valid option for licensees and applicants

Background – Early Concerns with CCFs

- Early concerns with CCFs
  - CCFs have been an NRC concern since the mid-1960s
  - In the early 1990s, the introduction of DI&C became a concern as a new source for introducing CCFs, as explained in SECY-91-292
- Current DI&C CCF policy
  - The NRC's current DI&C CCF policy is expressed in various documents, including SRM-SECY-93-087; SECY-18-0090; and BTP 7-19, Revision 8
- Current state of DI&C in the nuclear power industry
  - Design development practices and quality assurance tools have evolved
  - DI&C CCFs remains a serious area of concern

Background – Use of Risk-Information

- Increased use of risk-informed decision making
  - The staff is following the PRA Policy Statement and SRM-SECY-98-144 to expand risk-informed decision making
- Modernizing the DI&C regulatory infrastructure
  - SRM-SECY-16-0070 approved implementation of the staff's integrated action plan to modernize the NRC's DI&C regulatory infrastructure
  - The staff issued guidance on risk-informed, graded approaches to address DI&C CCFs for low safety significant systems (e.g., BTP 7-19 and RIS 2002-22, Supplement 1)
  - The staff believes this is an appropriate time to expand the current policy on DI&C CCFs to include the use of risk-informed approaches

SECY Paper Subject and Purpose

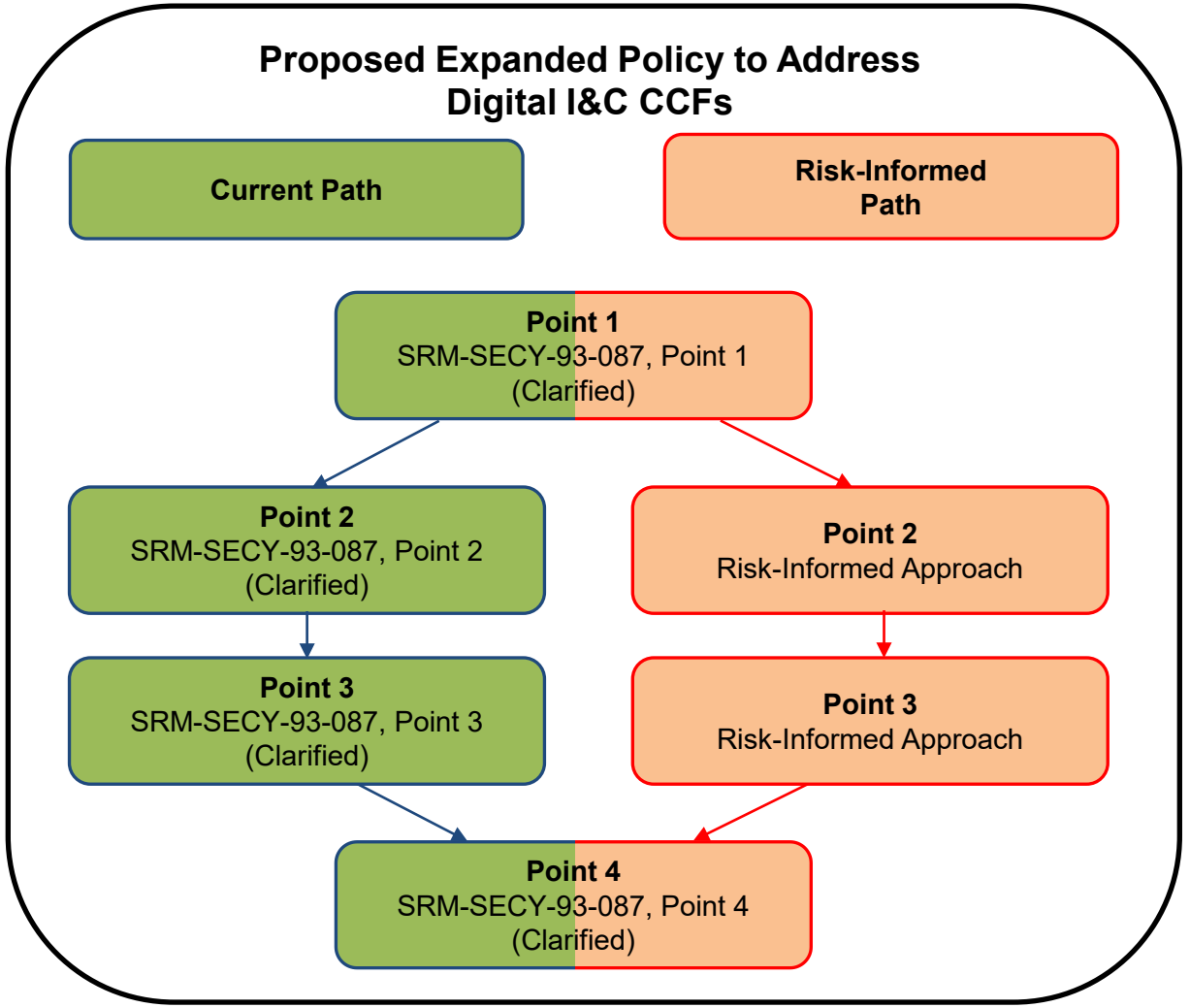
- **SUBJECT**
  - Expansion of Current Policy Regarding Potential CCFs in DI&C Systems
- **PURPOSE**
  - Provide the Commission a recommendation on expanding the current policy to include the use of risk-informed approaches for addressing DI&C CCFs
  - The recommended expanded policy will encompass the current positions in SRM-SECY-93-087 and the use of risk-informed approaches to determine the appropriate level of defense-in-depth and diversity to address DI&C CCFs

Proposed Expanded Policy to Address DI&C CCFs

- A **single expanded policy** that encompasses the current position in SRM-SECY-93-087 and provides for risk-informed approaches to address DI&C CCFs
- The expanded policy includes:
  1) Position in points 1, 2, and 3 of SRM-SECY-93-087 with appropriate clarifications and corrections from SECY-18-0090
  2) Position in point 4 of SRM-SECY-93-087 with appropriate clarifications
  3) The addition of risk-informed approaches to points 2 and 3 of SRM-SECY-93-087
- The expanded policy provides for:
  1) The deterministic demonstration of adequate diversity
  2) Risk-informed approaches

Proposed Expanded Policy to Address DI&C CCFs

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

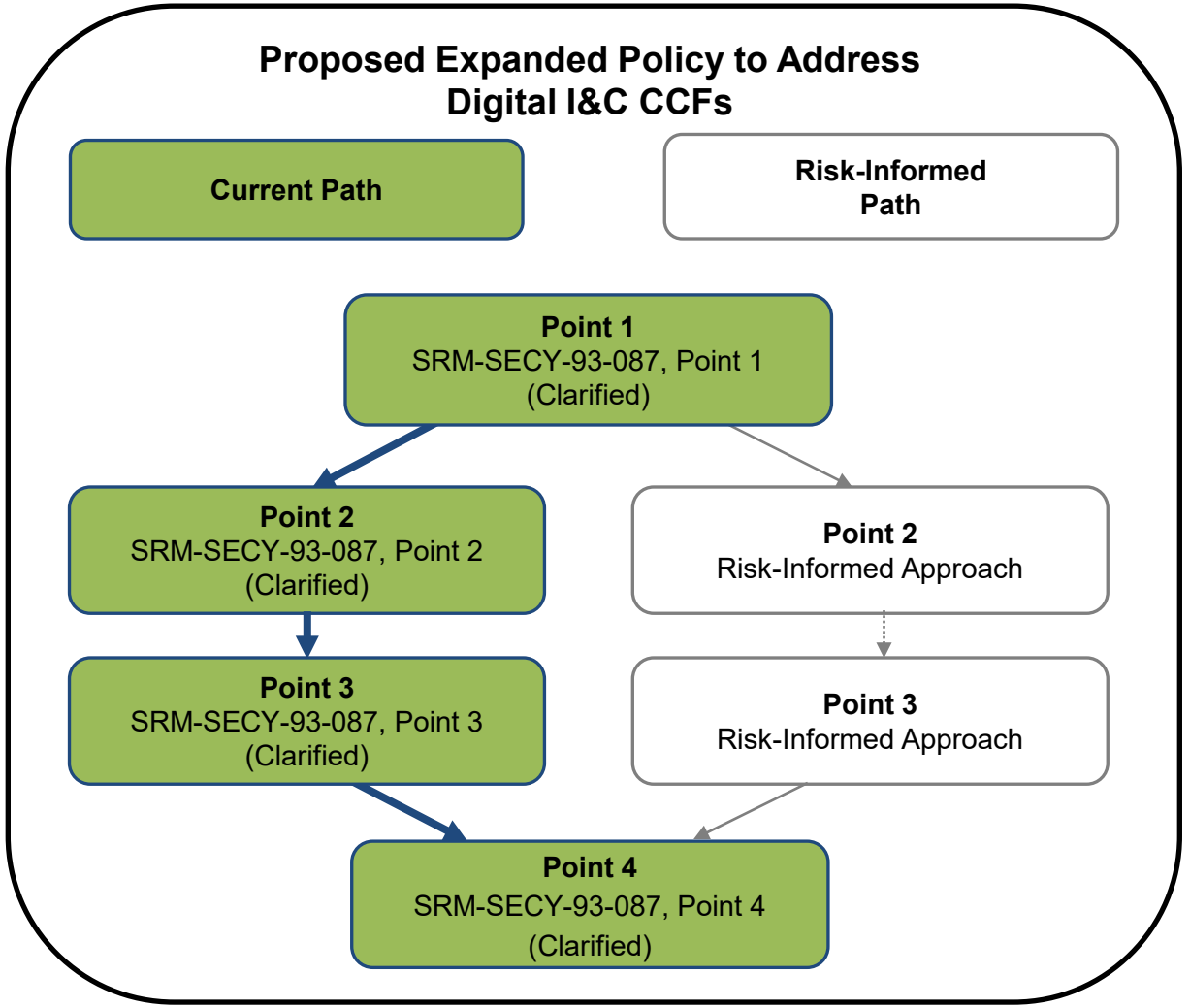
Current Path

Current Path

- The current policy continues to be a viable option to address DI&C CCFs
- The current four points in SRM-SECY-93-087 will remain as a viable path to licensees and applicants:
  - **Point 1** – "… assess the defense-in-depth and diversity of the proposed I&C system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed."
  - **Point 2** – "… 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… demonstrate adequate diversity within the design for each of these events."
  - **Point 3** – "If a postulated common-mode failure could disable a safety function, then a diverse means… shall be required to perform either the same function or a different function."
  - **Point 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…"
- SECY-18-0090 provides guiding principles for the application of policy, which were used in the development of BTP 7-19, Revision 8

Proposed Expanded Policy – Current Path

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF

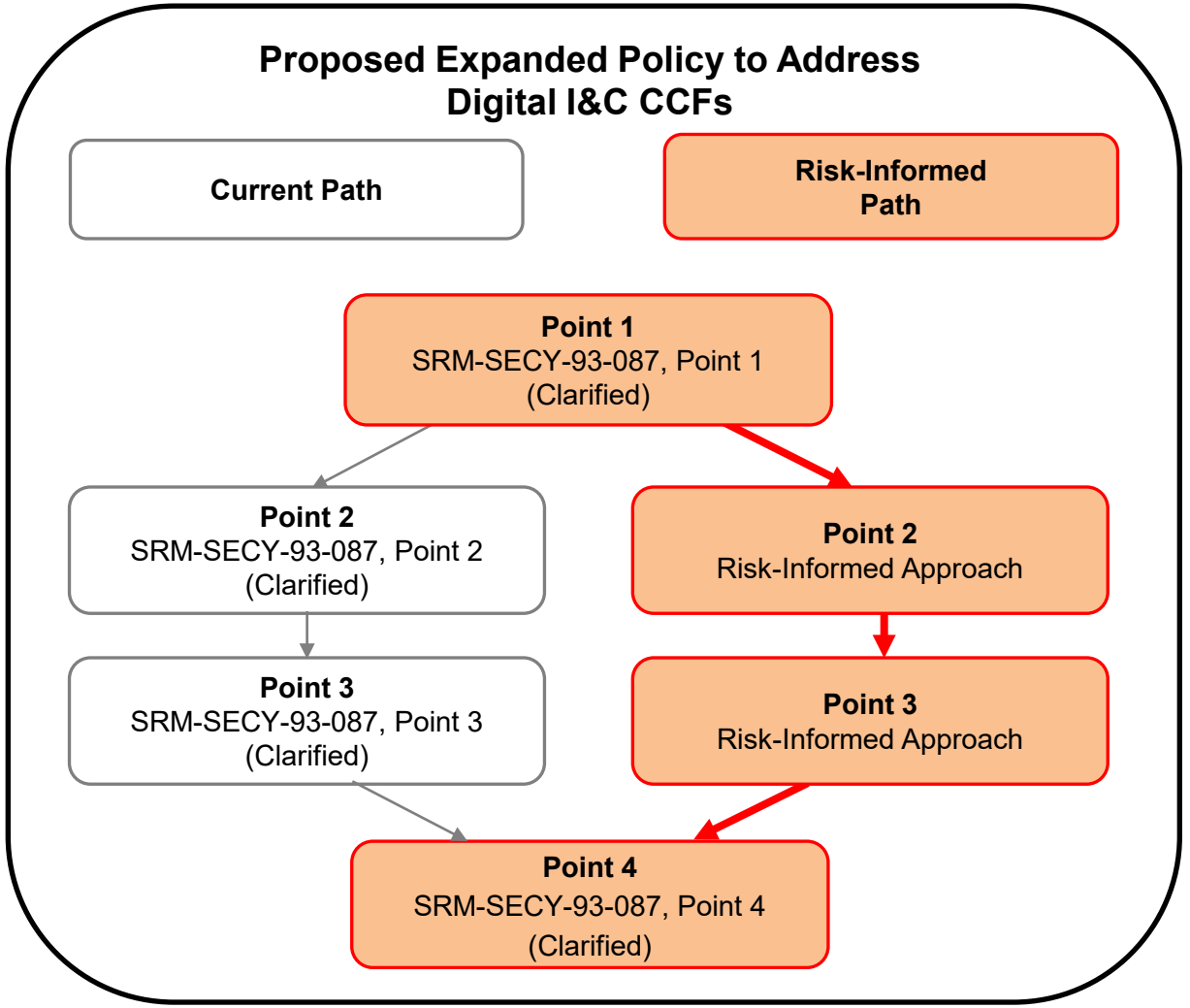


Clarifying the Current Policy Language

- Replacing “common-mode failure” with “common-cause failure”
  - The current language in SRM-SECY-93-087 points 1, 2, and 3 uses the term “common-mode failure” when the intent and implementation is “common-cause failure”
- Adding “facility” where appropriate
  - The current language in SRM-SECY-93-087 points 1 and 2 focuses on the proposed I&C system, when the NRC’s concern is on the defense-in-depth and diversity of the facility incorporating the DI&C system
- Adding “defense-in-depth” where appropriate
  - The current language in SRM-SECY-93-087 point 2 focuses on demonstrating adequate diversity, when the intent and implementation includes defense-in-depth

Risk-Informed Path

Proposed Expanded Policy – Risk-Informed Path



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

SRM-SECY-93-087, Point 1 in the Risk-Informed Path

- Point 1 does not preclude the use of risk-informed approaches for the D3 assessment

- Existing policy and guidance support a graded approach and applying a level of rigor for the D3 assessment commensurate with the safety significance of the proposed DI&C system or component

SRM-SECY-93-087, Point 4 in the Risk-Informed Path

- Point 4 is consistent with current regulations that effectively require diverse and independent displays and controls
  - 10 CFR 50.55a(h) incorporates by reference IEEE Std 279 and IEEE Std 603-1991, which are mandatory for nuclear power plants licensed since 1971
  - IEEE Std 279, clauses 4.1, 4.17, and 4.20, and IEEE Std 603-1991, clauses 4.10, 5.6.1, 6.2.1, 6.2.2, and 6.2.3 contain requirements related to automatically-initiated protective actions, manual controls, and information displays
  - 10 CFR Part 50, Appendix A, General Design Criterion 22 states, "… [d]esign techniques, such as functional diversity or diversity in component design and principles of operation, shall be used to the extent practical to prevent loss of the protection function."
- Risk-informed approach to point 4 would not provide appreciable benefits

SRM-SECY-93-087, Point 2 in the Risk-Informed Path

- Current approach focuses on consequences
- The staff considers this an appropriate area for risk-informing the evaluation of postulated DI&C CCFs
- The staff's goal is that risk-informed approaches will be consistent with all five principles of risk-informed decision making, as listed in RG 1.174

SRM-SECY-93-087, Point 3 in the Risk-Informed Path

- Current approach only provides one way of addressing undesirable outcomes (i.e., diverse means)
- The staff considers this an appropriate area for evaluating design measures other than diversity to reduce the risk from a DI&C CCF
- The staff's goal is to apply a graded approach for the level of justification needed for design techniques or measures other than diversity
- Diverse means will continue to be acceptable

Benefits of Risk-Informed Approaches

- Risk-informed approaches can provide flexibility to address DI&C CCFs and are consistent with the PRA Policy Statement
- Risk-informed approaches can have different levels of PRA use
- Risk-informed approaches could support a graded approach for addressing DI&C CCFs in high safety significant systems
- PRA models could be used to systematically assess the need to reduce the risk introduced by the DI&C system
- Risk-informed approaches can identify initiators or scenarios where lack of DI&C diversity does not compromise safety

Guiding Principles for Implementation

- The expanded policy will not conflict with existing regulatory requirements
  - A rule change or exemption will not be required to implement it

- The expanded DI&C CCF policy will be implemented consistent with the Commission's 1995 PRA Policy Statement, SRM-SECY-98-0144, and the current agency focus on expanding risk-informed decision making

- Implementation of the expanded DI&C CCF policy will continue to provide reasonable assurance of adequate protection of public health and safety

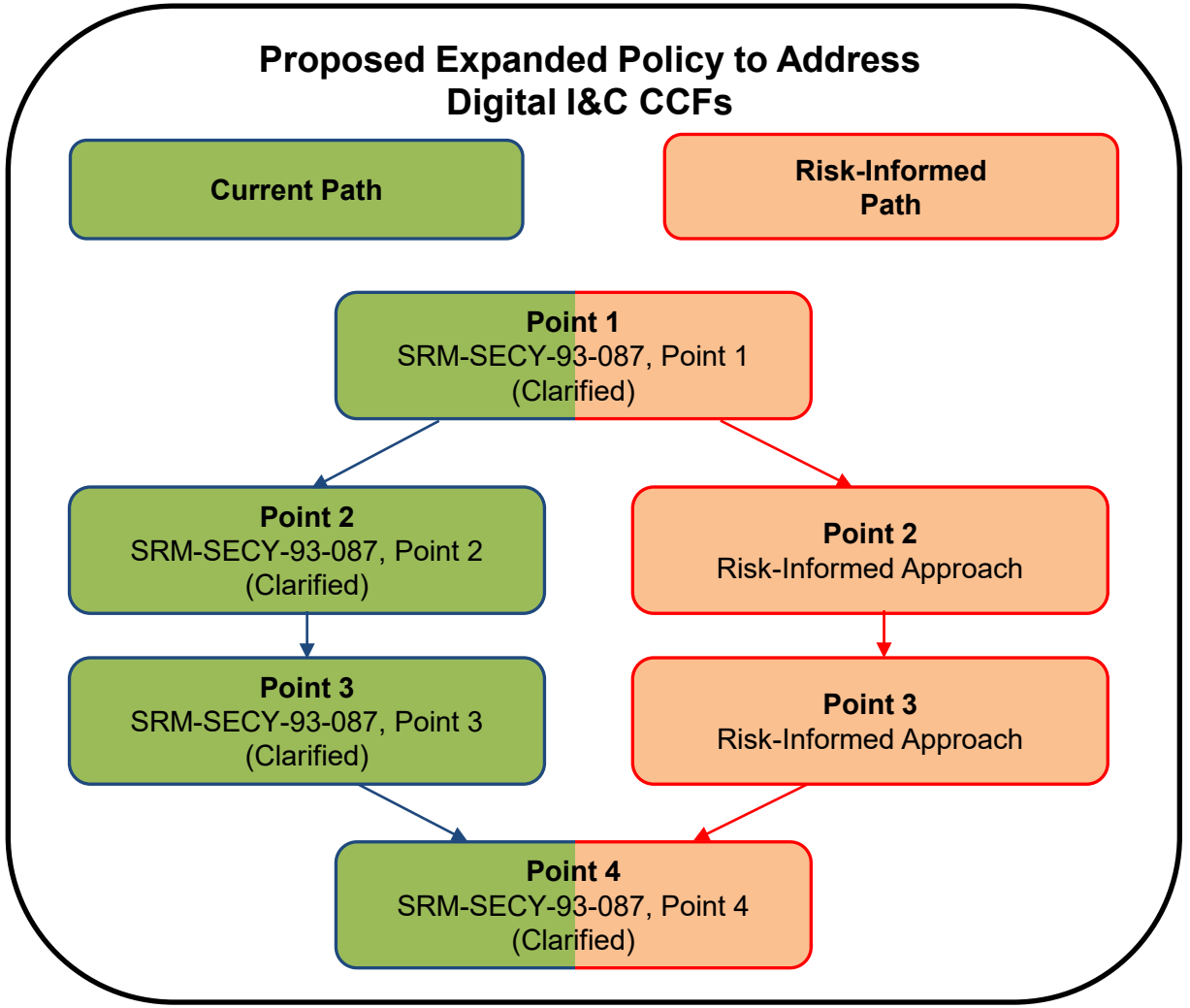
Guiding Principles for Implementation (contd.)

- The use of risk-informed approaches will be consistent with all five principles of risk-informed decision making, as listed in RG 1.174

- PRAs used for risk-informed approaches will be technically acceptable (e.g., meet the guidance in RG 1.200) and include an effective PRA configuration control and feedback mechanism

Proposed Expanded Policy to Address DI&C CCFs

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

Key Messages

- The expanded policy will encompass the current points of SRM-SECY-93-087 (with clarifications) and expand the use of risk-informed approaches

- Any use of risk-informed approaches will be expected to be consistent with the Safety Goal Policy Statement, PRA Policy Statement, and SRM-SECY-98-0144

- The current DI&C CCF policy will continue to remain a valid option for licensees and applicants

Status of Draft SECY Paper and Next Steps

- The draft SECY is currently being developed
- A public outreach meeting is planned for June 2022
- The staff plans to send the SECY paper to the Commission in 2022
- Upon approval of an expanded policy, the staff will proceed to update the implementation guidance in BTP 7-19

Questions?

Acronyms

BTP	Branch Technical Position
CCF	Common Cause Failure
D3	Defense-in-Depth and Diversity
DI&C	Digital Instrumentation and Control
ESFAS	Engineered Safety Features Actuation System
GDC	General Design Criteria
IAP	Integrated Action Plan
I&C	Instrumentation and control
MP	Modernization Plan
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
OEDO	Office of the Executive Director for Operations
PRA	Probabilistic Risk Assessment
RG	Regulatory Guide
RIS	Regulatory Issue Summary
RPS	Reactor Protection System
SAR	Safety Analysis Report
SECY	Commission Paper
SRM	Staff Requirements Memorandum