Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Stakeholder Outreach Meeting on the NRC Staff's SECT-22-0076 Regarding Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems

Docket Number: (n/a)

Location: teleconference

Date: Thursday, October 20, 2022

Work Order No.: NRC-2126 Pages 1-83

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

STAKEHOLDER OUTREACH MEETING ON THE NRC STAFF'S SECY-22-0076 REGARDING EXPANSION OF CURRENT POLICY ON POTENTIAL COMMON-CAUSE FAILURES IN DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

+ + + + +

PUBLIC MEETING

+ + + + +

THURSDAY

OCTOBER 20, 2022

+ + + + +

The Public Meeting convened via Video-Teleconference, at 2:00 p.m. EDT, Bhagwat Jain, Moderator, presiding.

NRC STAFF PRESENT:

BHAGWAT JAIN, NRR

ERIC BENNER, NRR

NORBERT CARTE, NRR

SAMIR DARBALI, NRR

KHOI NGUYEN, NRR

RICHARD STATTEL, NRR

DINESH TANEJA, NRR

SHILP VASAVADA, NRR

ALSO PRESENT:

MOHAMMAD ALAVI

ALAN CAMPBELL, NEI

JERRY MAUCK, JLM Nuclear I&C

WARREN ODESS-GILLETT, Westinghouse

KEN SCAROLA, Nuclear Automation Engineering

CONTENTS

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

2:00 p.m.

MR. JAIN: Hello. Good afternoon. It's 2 o'clock. My name is Bhagwat Jain and I'm a senior project manager in NRR's Division of Operating Reactor Licensing. Along with Michael Marshall, we perform the project management function for all things digital in NRR.

For the background for this meeting, this is our third public outreach this year on the Staff's proposed expansion of the CCF policy on SECY-22-0076. That is now with the Commission for wording.

We have had two public meetings on CCF proposed policy earlier this year. One in mid-February and the other one in early June. We also briefed the ACRS Digital I&C Committee, once in May and then in late September. The ACRS provided very valuable feedback to the Staff.

During the last ACRS briefing in September, the industry had provided some feedback on some aspects of the proposed expanded CCF policy. Today we will continue with that dialogue with the stakeholders to hear their perspectives and feedback.

Today's meeting is scheduled for two hours. The staff encourages stakeholders to provide

comments and the feedback. You may submit your comments or feedback via email to myself or Michael Marshall. Our contact information is provided in the public meeting notice posted on the NRC public website and on the chat.

With that, I'm looking if some of the key part presenters are here. We will display the presentation. Those who did not have access to Team video portion, you can download the presentation using ADAMS ML number for the presentation. Okay, the ML Number for staff's presentation is ML22291A015. I will repeat again. It is ML22291A015.

As I said before, this information is also provided in the chat. And the public meeting notice posted on the website. If you have comments on feedback on any aspect of this meeting, please contact me or Michael Marshall and we'll provide you the necessary forms.

With that I'll go over a couple of point of etiquettes. Please allow the presenter to make the presentation. There will be an opportunity to ask questions or provide comments after the presentation. If you are not speaking, please keep your cell phone on mute and turn off your video please. When you speak, please identify yourself.

Now with that I will then start with some introductions. We have exactly from NRC in the meeting Eric Benner. The director of division of engineering and external hazard.

Today's presentation is led by Samir Darbali. Samir is the I&C tech staff in the Division of Engineering and External Hazards.

We have several other NRC staff on line. As they contribute to the meeting they will introduce themselves.

With that I will now request Eric Benner to make some opening remarks. Eric, please.

MR. BENNER: Thanks BP. And thanks everyone. Like BP said, this is the third of a series of meetings on this specific topic.

We're in an interesting space because we have provided the paper to the Commission now. So it's before the Commission for voting. But there has been ongoing dialogue about the contents of the paper. Both, like BP said, at the ACRS. And NEI provided a letter with some of their feedback.

So we do want to keep this dialogue open, so I'm going to steal some of BP's thunder and I'm going to look ahead to Slide 4 and say the purpose of this meeting is to summarize what's in SECY-22-0076.

We intend to do that pretty briefly because going into this I thought that most of the people who would be at this meeting were people who were at some of our previous meetings. But I know we're up to 76 participants. So I think we have some additional participants on this meeting.

So our summary will be pretty high level, but like BP said, we can go into a little more detail so that everyone understands what the paper proposes or doesn't propose.

We also want to share, because at the ACRS, the latest ACRS subcommittee meeting that we heard, the ACRS had some feedback and questions. And we have the answer to those questions, and we've provided that to the members. But we also just want to make sure all the stakeholders are aware of the answers to those questions.

We want to do a little deeper dive because it seems like some of the area of concern is on what we call Point 4 in the policy. And that deals with manual controls and displays. And what that part of the policy requires, or doesn't or, you know, how it influences, how we conduct our reviews. And then, like BP said, it's open dialogue.

It's going to be us certainly answering

any questions that people have on any of the things contained in the SECY or any of our other supplemental information we'll provide today. But also to hear the feedback from the stakeholders on any of those items.

And I know that the meeting today is being transcribed. Again, I might be stealing some of BP's thunder because we want to have everything on the record so that as we move forward, you know, either on potential implementation or on any supplemental communication we would want to have with the Commission, we want to make sure we're getting the record straight.

Because I will say there has been some ambiguity in some of the discussions we've had. And we really, we really do want to try and get it down to precisely what people's concerns are, what their requests are, that sort of thing. So we really know exactly where there might be just areas where we need to clarify things. Or are there areas where we truly have disagreements with differently stakeholders and why those differences exist.

So that's my preamble with that. I'll turn it back over to BP.

MR. JAIN: Well, with that I think Samir is going to make the presentation. Samir, would you

please?

MR. DARBALI: Thanks, BP. And thanks, Eric. Just for awareness -- you can see the slides, right?

MR. JAIN: Yes. We all can.

MR. DARBALI: Okay. Yes. And just for awareness, Jerry and Tom, you have your cameras on. I don't know if you intended to do so, but just so you know.

PARTICIPANT: Are we going to record this?

MR. JAIN: This is being transcribed. The meeting is being transcribed.

PARTICIPANT: Okay.

MR. DARBALI: Thanks, Tom. Jerry, your camera is on but it's all blank. It's a black screen. Just FYI.

So, good afternoon, everybody. Here is an outline of this afternoon's presentation. So we'll briefly go over the recent activities in the development of SECY-22-0076.

Eric already covered the purpose of the meeting. We'll provide a quick summary of the proposed expanded policy. Which I believe most here have now become familiarized with, but as BP and Eric said, if we need to look at some specifics we can do

that.

We'll address the staff's position on the questions we received during the ACRS Digital I&C Subcommittee meeting. We'll talk about the applicability of Point 4 and provide some clarifications. And we'll proceed with the open dialogue portion of the meeting.

The staff recently issued SECY-22-0076 on August 10th of this year. The SECY proposed an expansion to the digital I&C common cause failure policy. Which is contained in SRM SECY-93-087. Shortly after issuing the SECY, NEI provided a letter to the NRC with comments on the staff's position contained in Point 4, regarding diverse and independent main control room displays and manual controls.

The staff and NEI briefed the ACRS Digital I&C Subcommittee in September of this year. And the staff is scheduled to brief the full ACRS on November 1st.

The SECY is currently under Commission review. And the staff is waiting for Commission direction through a staff requirement memorandum, or SRM.

We already covered the purpose of the

meeting, so in Slide 5 we have the staff's key messages. That the proposed expanded policy in SECY-22-0076 encompasses the current four points of SRM SECY-93-087 with some clarifications. And expands the use of risk-informed approaches in Points 2 and 3.

Points 1 through 3, and Point 4 of the policy, address two facets needed to ensure the safe operation of the plant. Points 1 through 3 ensure Digital I&C systems are sufficiently robust to adequately cope with a CCF. And Point 4 ensures operators can manually control critical safety functions, even in the event of a Digital I&C CCF.

Point 4 already incorporates an implicit element of risk-informing, as it only focuses on those critical safety functions needed to ensure the safety of the facility.

The expanded policy is intended to be technology neutral and applies to any reactors licensed under 10 CFR Parts 50 and 52. And this includes non-light water reactor designs.

We acknowledge that the critical safety functions listed in SRM SECY-93-087, SECY-22-0076 and Branch Technical Decision 7-19 may not be the appropriate set for all reactor designs. However, the SECY does provide for the use of regulatory tools,

like exemptions and alternative, to accommodate for reactor designs with different critical safety functions.

And finally, if the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

Here is the figure that shows the single expanded policy that encompasses the current position in SRM SECY-93-087. And provides for risk-informed approaches in Points 2 and 3 to address Digital I&C CCFs.

The current path on the left in green allows for the use of best estimate analysis and diverse means to address a potential CCF. While the risk-informed path on the right allows for the use of risk-informed approaches. And out of the same technics for measures, other than diversity to address a potential CCF.

The ACRS Digital I&C Subcommittee provided some questions to the staff during the September meeting. The first question is, would the revised policy be applicable to advance reactors? And the response is, Yes. The policy would be applicable to advance reactors licensed under Parts 50 and 52.

The second question is, Do aspects of the policy for which the staff did not request a change carry forward unaltered? And this question was focused mostly on Point 4. Specifically the Commission stated in the SRM to SECY-93-087 that the requirements in the SECY-93-087 for the diverse displays of manual controls to be hardwired. That this requirement was highly prescriptive.

The ACRS noted that SECY-22-0076 was silent on this matter and wanted to know the expanded policy, maintain the Commission's direction for, from SRM SECY-93-087. And the answer is, Yes. The staff intended to maintain the Commission's direction regarding this matter.

The last question was, Might different reactor types warrant consideration of different critical safety functions? And the answer is yes. The expanded policy is intended to be policy neutral, but it relies on the staff's licensing experience and assumptions about the design of the facility. Such as the presence of a main control room.

We recognize that the critical safety functions listed in the SECY and BTP 7-19 might not be appropriate, an appropriate set for all reactor designs. Again, the staff has existing regulatory

tools, like acceptance and alternatives, to accommodate designs with different critical safety functions.

If the staff encounters a reactor design where the policy will not be applicable, the staff will engage the Commission as appropriate.

On Slide 8 right now. And this slide shows that Point 4 is already risk-informed because it requires diverse displays and manual controls only for those critical safety functions performed by the Digital I&C system.

This means that Point 4 does not apply to noncritical safety functions performed by the system. And it does not apply to critical safety functions that are not performed by the digital system. So you can see it's only that scope of critical safety functions performed by the system, which are applicable under Point 4.

Point 4 is further risk-informed because it does not require the display, the diverse displays and manual controls for critical safety functions to be safety grade.

Here is some background on the staff's position on diverse and independent main control room displays and controls. In the original SECY, 93-087,

the staff recommended that safety grade displays and controls located in the main control room are hardwired to the lowest level of the safety system architecture be provided for a manual system level actuation of critical safety functions and the monitoring parameters that support the safe functions. Those displays and controls should be independent and diverse from the safety computer system identified in Points 1 and 3 of the policy.

Now the staff made this recommendation because such controls and displays provide the plant operators with unambiguous information and control capabilities to enable the operators to quickly mitigate the effects of the postulated CCF.

The control room would be the center of activities to safely cope with the event. And the design of the plant should not require operators to leave the control room for such an event. Again, this is what the original SECY-93-087 proposed.

In its direction to the staff, the Commission's SRM to SECY-93-087 modified the policy to permit non-safety grade displays and controls, and more flexible architecture and implementation. Such as not needing the displays and controls to be hardwired.

But the Commission supported the staff's recommendation on diverse displays and controls for critical safety function. And the staff continues to believe this position remains appropriate to provide reasonable assurance of adequate protection.

Again, Point 4 already incorporates and implicit element of risk-informing as it focuses only on those critical safety functions needed to ensure the safety of the facility. And also because it allows displays and controls to not be safety grade and to not have to be hardwired.

Requests for exemptions or alternatives provide avenues for applicants to request a deviation from the regulations, based on risk information on a case-by-case basis. And again, if the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

And here on Slide 11, this slide shows that the points in SECY-22-0076, as well as the original SRM SECY-93-087, are intended to address two facets that are needed to ensure the safe operation of the facility.

Points 1 through 3 address the protection against Digital I&C CCFs to cope with the loss of a

safety function. Whereas Point 4 allows operators to take manual actions of critical safety functions when needed after a Digital I&C common cause failure.

If a Digital I&C CCF is not properly addressed, it can affect both a digital system as well as the manual controls and displays. The four points of the policy, when taken together, provide criteria for the assessment of diversity and defense-in-depth against CCF and ensure Digital I&C CCFs do not defeat safety functions and do not impede operators ability to take manual actions when needed.

And that concludes the staff's presentation. And we can open it up for questions and dialogue. Thank you.

MR. JAIN: So the floor is open for discussion on NRC's presentation, so --

MR. DARBALI: Go ahead, Alan.

MR. CAMPBELL: Hey, good afternoon. This is Alan Campbell with NEI. First, thank you all for hosting this meeting and having this open discussion. I think it will be very helpful in helping us to better see the different points of views that we both have.

When we review the presentation, I'm reflecting back on the June 8th stakeholder meeting

when we were talking through the initial, I believe it was the outline and initial presentation to the ACRS at the time. And we had a discussion regarding Point 4.

And at the time the industry provided a concern regarding a separate analysis that's needed for Point 4 and how that relates to the analysis in Points 1 through 3. At the time the NRC staff responded with the, with a statement that it's not intended to be a separate analysis, that they're meant to be, Point 4 is meant to be integrated in with Points 1 through 3.

It appears, you're showing Slide 11 here, and it appears that we're back to where the industry's initial concern was with this being a separate analysis that's different from Points 1 through 3 and Point 4.

MR. DARBALI: Right. So thanks for the comment, Alan. And I'll take a crack at it, and somebody else from the staff can also chime in.

So just because Point 4 is intended to address a separate safety aspect doesn't mean that it requires a completely different analysis. So when you do the analysis for, you know, Points 1 and 2 and then in Point 3 you identify how you're going to cope with

a potential CCF, in that aspect you can identify which are your critical safety functions and you can identify if those critical safety functions have a diverse manual control and display. It doesn't require an entirely different analysis.

And again, you're not looking at the entire facility's critical safety functions, only those that are modified by the digital upgrade.

MR. CAMPBELL: Okay. So --

MR. ODESS-GILLETT: Alan, this is --

MR. CAMPBELL: Go ahead, Warren.

MR. ODESS-GILLETT: Okay. So, as you know, the current way in which one performs the D3 analysis is to analyze each safety analysis event.

And then to determine what you have available in the plant to protect it using the criteria. The relaxed criteria. And so that analysis is a different, is a different set of inputs for the analysis and results in a different set of outputs for the analysis.

And then Point 4 doesn't even look really at your safety analysis, so much as looking at, okay, we have these critical safety functions we need to maintain. So it's a different set of inputs. And what manual controls we need to maintain those

critical safety functions.

And so in my opinion, it appears to be, it ends up being two separate analyses because you come up with two different sets of outputs.

MR. DARBALI: You're right. And thanks for the question, comment, Warren. You are coming up with two separate outputs or conclusions, but, and if you want to call Point 4 a separate analysis, okay, but it's not an analysis to the level of the analysis that you're performing for the first three points.

Of course, you know, I think the bulk of the experience, both in the licensee side and the staff side, when we're looking at these digital upgrades have been with operating plants. And so those plants already have those diverse manual controls because most of the mitigations we've seen, you're not replacing the actual controls in the control panels.

And in that sense, that point, how you're addressing Point 4, it doesn't require a lot of work. Because you can just say, look at our architecture. We're not ripping out controls from the control panel, therefore those controls still remain. And they're not part of the digital mod itself so they are diverse.

So there are different ways in which point, the information to justify Point 4 can be provided or extracted from the architecture.

MR. ODESS-GILLETT: I --

(Simultaneous speaking.)

MR. CAMPBELL: Go ahead, Warren.

MR. ODESS-GILLETT: Is it okay?

MR. CAMPBELL: Yes.

MR. ODESS-GILLETT: Okay. I don't want to monopolize.

MR. CAMPBELL: Go ahead.

MR. ODESS-GILLETT: But in fact, even if they're hardwired controls, they still, even to meet IEEE 603 they need to go down to a level of the architecture. As you even point out here, that is susceptible to a CCF and therefore you still need this other analysis to than determine what manual, diverse manuals and controls, displays and controls, I need in order to maintain the critical safety functions that will require a second interface to those same, let's say ESFAS components that your safe system has to interface with.

So, even if you have, so my point is, even if you have manual controls, I mean hardwired controls, they typically still go to a low-level

portion of your Digital I&C safety system.

MR. DARBALI: Understood. And I supposed that's, you know, dependent on the application.

MR. ODESS-GILLETT: Yes.

MR. DARBALI: Okay. I guess, you know, one clarification we've been wanting to make since, you know, Alan, you pointed to that, I believe the June meeting, is that we had, we thought some licensees were interpreting Point 4 as to say, hey, for Point 3 I'm crediting manual actions. Because I have those controls, those actions can be performing in a timely way so I'm crediting those.

And it seemed like some people were interpreting Point 4 to say, well, in addition to that manual control you have, you need a whole separate analysis and a whole separate manual control that's diverse from what you're crediting. So that's probably what we intended to say back then.

But, I mean, if you look at the language from the original SECY, on Point 4, all of the background information, it's really reinforcing the idea that your operators have to be able to take manual actions if needed.

MR. CAMPBELL: So I guess that brings me to my next question. You use the term, if needed.

Here on the slide it says when needed.

MR. DARBALI: Right.

MR. CAMPBELL: What would, is there a postulated scenario when, so we're looking at this in terms of layers of failure. So we've had a plant failure. A design basis event. Then we have an RPS/ESFAS failure with a common cause failure.

Are we now to assume that, you know, in Points 1 through 3 we're postulating and coming up with ways that we can maintain safety functions. Are we now assuming that that additionally fails?

A third failure here and now we have to have a fourth, this next layer down of manual actions to control the plant. Because Points 1 through 3 get you to a hot shutdown state --

MR. DARBALI: Right.

MR. CAMPBELL: -- which that's what's required for the policy.

MR. DARBALI: Right. And the way I'm interpreting your question, no. So point, like you said, Point 3 is going to provide for those. Whether it's going to be diverse meanings or mitigation measure or design technics or preventive measures, to address or cope with that CCF.

You lost your safety system, Point 3

measures are going to address that. Regardless of how that is addressed, you don't want your, under plants that have a control room and require, you know, have manual controls, you don't want to prevent your operators from even being able to take manual actions if they have to.

So, what you don't want to be is in a situation where your CCF took out your digital system, took out our manual controls and displays. And so yes, you have your Point 3 measures or designs technics addressing that CCF, but your operators are blind to plant, certain plant conditions or cannot perform any actions.

And again, for a reactor design that does rely on operators taking actions, we don't see a reasonable argument for having operators lose that ability. And maybe that's some insights that industry can provide to us. But we haven't encountered a scenario where we can say it's okay for operators to lose that ability.

MR. CARTE: Samir, can I propose we do a brief digression and let Jerry Mauck say something?

MR. DARBALI: Sure. Go ahead.

MR. CARTE: Jerry, you raised your hand?

MR. MAUCK: I was on mute. I have a hard

time with all the buttons on this thing.

I just wanted to point out that, you know, we're doing, pretty much have completed a D3 on Turkey Point. And you only really need Point 4 if you don't have success and you're pursued of Point 3.

But Point 4 is, I don't want to have anyone oversimplify it, it's rather complex because you not only have to have manual actions for the main system, you have to have manual actions for the systems that support the manual system. And it cascades down into quite a number of manual actions.

And also necessary diverse manual indications which can be quite large. And you can end up with pages of diverse indications that are reacquired. And also pages of manual actions that are required. It depends on what you're digitizing at the plant of what course. It can be rather complex or not so complex.

But the point I'm trying to make is, Point 4 is not a simple task. That was it.

MR. DARBALI: Understood. And, Jerry, if I can have you add to something you said. I think you said, Point 4 is needed if there is an issue with Point 3 or Point 3 cannot be fully addressed?

MR. MAUCK: Yes. That was our view that,

you know, if we have automatic diverse actions at Turkey Point, we didn't require any manual action. Any diverse manual action to be credited.

But if we got to the point that there was no way to get diverse automatic actions, whether from a safety system or a non-safety system, or the ATWS, or any control system, then we have to go to that Point 4. And then when we went to that, not only did we have to identify what the manual actions were and what the indications were that the operator had to have, we have to do the timing for it and make sure that the operator has the time to take this action. So it gets, it's not a simple task.

MR. DARBALI: So, and without getting to specifics of the particular Turkey Point licensing application, it seems, from what you describe as Point 4, really being part of Point 3.

MR. MAUCK: True.

MR. DARBALI: Right. And --

MR. MAUCK: Yes, true. True. Because, you know, that's a blend there. If you are, meet what you need to meet with your diverse manual actions, then it can be part of Point 3. Yes.

MR. DARBALI: Right. So with Point 3 if, you know, you mentioned either you have a diverse

system, ATWS or other system, or you can take --

MR. MAUCK: Right.

MR. DARBALI: -- timely manual action, then you meet Point 3.

MR. MAUCK: Right. Right. I see what you're saying now. It's kind of weird. We have to have for the critical, all critical safety functions we have to have diverse displays and diverse manual controls that aren't part of the software.

MR. DARBALI: Right.

MR. MAUCK: Which are, is a little bit different twist. It kind of goes hand-in-hand there. But it is a different twist on what you're trying to take manual action credit for over on Point 3. True.

MR. DARBALI: Right. Right.

MR. MAUCK: Yes.

MR. DARBALI: Yes, so, if you're crediting manual actions in Point 3, then you're already addressing Point 4. Because Point 4 doesn't --

MR. MAUCK: True.

MR. DARBALI: -- ask --

MR. MAUCK: Yes.

MR. DARBALI: Point 4 doesn't require timely actuation, it doesn't require safety grade.

MR. MAUCK: Right.

MR. DARBALI: Just that you have manual for critical safety functions.

MR. MAUCK: Right.

MR. DARBALI: If you're doing it in Point 3 for those functions, you're already doing it for Point 4.

MR. MAUCK: Right. Right. That's the same.

MR. DARBALI: Yes.

MR. MAUCK: True.

MR. JAIN: Dinesh, you have raised your hand. Do you want to say something? Dinesh Taneja.

MR. TANEJA: Yes. I was just trying to, you know, these analysis, you know, we looked at a number of analysis for new reactors. And the new reactor designs that we have looked at, you know, including API1000.

So the coping analysis, there were scenarios where they said, you know, hey, the plant, the CCF is bounded so no action needed. I can live with the potential CCF concern.

But really your analysis kind of said, hey, if it happens, so be it, I'm still bounded. You know, my AOOs and my scenarios that my analysis bounds it.

Now, the other thing that we've seen is that control systems have been used in those designs to provide the diverse means of actuation and indications. So they're taking credit for your plant control systems to be able to do certain, if your control system is available, to take the necessary actions. And those are diverse means. So that was your Point 3 manual actuation using control system capabilities.

Point 4 is used in some design to bring in the manual actuations in those, you know, new reactors now I'm talking about. They basically designed the manual actuations to meet the 603 requirement for system level manual actuation and they brought them into the, you know, the priorities modules as a hardwired input downstream of the digital.

So they actually were designing it such that you were actually meeting the 603 requirement, as well as the recipe requirement.

So there are some good design solutions there, but you really don't want to get caught up into just doing the analysis. I think we need to think about, in a good design from the get-go that meets the primary objective of being able to control the plant, manually as well as automatically.

I just want to bring that out, that we've seen those designs and we've never had any new reactors come back to having any issues with trying to meet the guidance or the policy statements of 93-087.

MR. JAIN: Thank you, Dinesh. Richard, you have comments?

MR. STATTEL: Yes. I just wanted to say that I fully agree with Jerry's interpretation that he just provided.

And that is completely consistent with previous applications and the evaluations we've performed of them. It wasn't until recently when we heard this new interpretation of addressing Point 4 as a separate issue outside of the D3 context.

The only thing I would also add to what Samir said was, is that Point 4, I agree. If you are crediting manual actions to address Points 1 through 3, really you have already addressed Point 4, other than the fact that Points 4 adds the requirement for diversity.

Which really ought to go without saying, because obviously if you're saying it in the presence of a common cause failure it has to function, it has to work. And the only way you can assure that that function is going to work is if it is in fact diverse

from the digital safety system.

But that's what it adds. That's what Point 4 brings to the table. It's basically, you can use manual actions and it's allowed by Point 3. But if you do that, you have to, it's almost like you also have to make sure that those functions are still going to work in the presence of the CCF.

And also, by the way, we did some research and we looked at what the source of Point 4 of that position is, and it was not drafted by the Commission, this was the staff's language. And this was what the staff put to the Commission in the SECY-93-087. And the Commission simply agreed with that portion of the SECY.

MR. JAIN: Thank you, Richard. Warren, you have your hand up.

MR. ODESS-GILLETT: Yes. But I'd like to defer to Alan, if he has any other points he wants to make.

MR. CAMPBELL: Yes. And so, Rich, just responding to what you said, I don't hear, I'm still hearing two different interpretations here that, you know, and please correct me if I'm wrong in understanding what you just said, but Point 3, if there are manual operator controls that are required

and Point 4 adds this diversity, you're saying it adds the diversity.

When I look at Point 3 in the SRM existing today, it has the diversity element in it. Point 4 adds in the term, critical safety functions, which broadens out the scope beyond what was identified in Points 1 through 3.

And so I think the concern is, now that we've broaden the scope in Point 4 to all critical safety functions, why are those needed?

MR. STATTEL: Well --

MR. CAMPBELL: Are we assuming that there is a failure of what happened in Point 1 through 3. We don't see it in an application where those are needed because we're already postulating the system fails and what do we need to do to get it into a safe state.

MR. STATTEL: Again, it's within the context of the D3 analysis. And of the scope of the safety system that's being evaluated. That's being analyzed.

So we talked at the last meeting, I think we had an agreement on this interpretation going forward. And we would be willing to provide clarification on that interpretation to avoid

alternate interpretations of this.

But really we have no indication that it was intended to be applied independently of a D3 analysis. It's one point of four points that were made in this SRM. And it's all within the context of the D3 analysis.

It was never, we have no indication, I mean, I wasn't around, I didn't, I wasn't around to draft it or anything, but we have no indication when we research the original SRM that it was intended to be applied independently as this interpretation.

And we don't have multiple interpretations. We're just trying to understand what you're saying. So we're really trying to be empathetic and to understand your position on these. On this.

And we get it. We understand how you're applying this. But we don't believe it's intended to be that way, and we would like to get that clarified.

MR. CAMPBELL: And so I think, you know, that's aligned with what we're asking for, Rich. I think the way that you're describing it is, unless I'm misunderstanding the way that we have proposed to intend it, or I'm sorry, implement it. But what I'm seeing on the screen and what we've seen in the SECY

paper brings us back into this, a different interpretation of what you just described.

MR. CARTE: So this is Norbert Carte. Let me jump in for a second. And then we also have another hand up that hasn't had the chance to speak yet.

So I guess there is, we got to look at this a different way because somehow we're talking past each other. So if we look at the requirements of 279 and 603, they both require that given an event or a condition in a facility that you determine whether automatic protective action is required. And that for every automatic protective action you have a manual means of initiating that same at the division or the system level.

So what they're saying is, you need manual for every automatic action. Well, one of the problems with the word safety, critical safety function, is that was sort of a reaction out of TMI.

And so, 603 and 279 don't talk about critical safety functions, and they talk about protective actions. And there is more protective actions then those that are needed for the critical safety functions.

So you might have a protective action that

protects the analysis. As you're analyzed for an event at a particular low steam generator level, and if the level goes below that, well, and that event occurred, you would be in an unbounded situation therefore you want to protect the analysis not necessarily protect against a particular event.

So there are more protective actions than are needed to protect the critical safety function. So the idea of critical safety functions wasn't to expand the scope of what's needed, it's to limit the scope of where you need diversity from every single protective action that's automatically initiated.

It's the important ones that really must have displays and controls. And they use a post-TMI wording to determine which ones are the important ones. So I see that as a little bit of a disconnect.

MR. CAMPBELL: All right.

MR. CARTE: We're not, Point 4 is not asking for new and different controls than anybody else is asking for. But that's my input. Can we go to Ken Scarola for a second?

MR. SCAROLA: Yes, Norbert, thank you. Can everybody hear me okay? I'm not sure I have this thing setup right.

MR. CARTE: Yes, we hear you.

MR. SCAROLA: Okay, thanks. I listened to Rich, and I listened to Norbert. And I think we are beginning to recognize that there is wisdom in IEEE 603 and 279.

And the wisdom is that we design the protection system for the events that we anticipate. But there is always the n+1 event that we did not anticipate.

And 603 and 279 say, we're going to address this n+1 event, the one that we did not anticipate, by giving the operators the ability for manual initiation of the safety functions. And Rich, I have to tell you, that was the intent of Point 4 in SECY-93-087.

It was not, you only need Point 4 if Point 3 says you need it, it was, you need Point 4 because you may not analyze everything that can possible happen in Point 3. There is always the event that you haven't thought of. And it's the same basis of why we have this capability for manual initiation in 603 and 279.

Now that manual initiation in 603 and 279 also gives the operators the ability to take preemptive actions. So there is really a twofold purpose here. Preemptive actions and manual actions

with the event for which the automated system does not actuate.

Now, I believe that we should not require Point 4 unconditionally. If you've done your homework and you've analyzed your Points 1 through 3, that you don't have a potential for a CCF, or it's risk-insignificant, then there is no reason to have Point 4. Point 4 should not be unconditionally required.

On the other hand, if you have identified that you do have the potential for a CCF and the CCF can affect the manual initiation capability required by 603 and 279, then Point 4 should be required. And I think that's an important distinction.

So I would recommend to the staff that the last phrase in the first sentence of Point 4 that ends, vulnerabilities to digital CCFs have been adequately identified and addressed, be clarified to add, including both automatic and manual control of critical safety functions. That's what we're trying to do here. Make sure that we can control critical safety functions both automatically, as intended by the protection system, and manually as we have given that capability to the operators.

So Point 1 needs to address the entire safety function, not just the automation.

Now in addition, when we get to Point 4, I would recommend that this be clarified with a preface that says, if Points 1 to 3 demonstrate inadequate manual control of critical safety functions, and then continue it as written, so the only time you would need Point 4 is if Point 1 through 3 demonstrate that you don't have adequate protection against CCF. Either through a deterministic method or a risk-informed method.

And then I would also make another very important clarification. 603 and 279 do not require manual control at the actuation level. Or at the component level. They require manual initiation of the same functions that the safety function automates. It's initiation, not actuation. And that's clarified again in Reg Guide 1.62.

So Point 4 should make the same distinction. We should be replacing the word "actuation" with "initiation." We need to give the operator the ability to "initiate" control of the safety functions.

Now how you deal with longer term needs is another issue. There are many ways that we can manage those control functions once they're initiated. But the timely problem is to initiate them.

I'll leave my comment at that. I have more comments that are not on the Point 4 issue, but I'll save them until after this discussion. Thank you.

MR. CARTE: Sorry, Ken, that was a little long but let me just try and shorten that a little bit. So what I heard you say was that if the CCF is not risk-significant, as determined by Step 3 or earlier, then Point 4 does not apply? That's one of the points you were making?

MR. SCAROLA: Well, what I'm trying to say, there can be two ways where Point 4 wouldn't apply. One is that you've concluded that you don't have a CCF.

MR. CARTE: Or it's risk --

MR. SCAROLA: Well then you already have manual controls through 603 and 279, therefore you don't need more manual controls. The second way, is as you said, is if you demonstrate that it's not risk-significant.

MR. CARTE: But the first way is no CCF. Well, yes, obviously.

MR. SCAROLA: Well no, not obviously because the way it's written right now Point 4 is unconditional.

MR. STATTEL: Yes, but you're reading it in isolation. If I could respond. So --

MR. SCAROLA: I'm not reading it in isolation, I'm reading it the way it's written. There is four points to the policy.

MR. STATTEL: It's one of four points.

MR. SCAROLA: Yes. But nothing in Point 4 says, if there is a CCF, then you need manual control. All it says is, you need manual controls.

MR. DARBALI: Well, unlikely to be subject to the same CCF assumes there is a CCF.

MR. STATTEL: But when do you apply these four points? You apply these four points in the conduct of a D3 analysis. So there is your condition.

So do you agree if, you know, what you just said, if you go through Points 1 through 3 and you conclude that you meet the criteria, right? You have adequate safety, then you basically have met Point 4. Even if you credit manual actions.

MR. SCAROLA: However, Rich, we commonly conduct the Point 1 analysis, and Point 1 through 3, with consideration of only the automated functions of the protection system.

MR. STATTEL: I have never seen a, I have never seen a D3 analysis that did not credit manual

actions. And I've been doing this for 30 years.

MR. SCAROLA: Oh. But those are only the manual actions that are in Chapter 15. That's not the only point of 603 and 279.

The manual actions that we credit in Chapter 15 are for the events we thought of. And what I'm trying to explain here, is that there are the events we have not thought of. But the guys who wrote 603 and 279 did think about those events.

But we used to call them the n+1 event. The one we didn't think of. And that is another intent, not just for the credited manual actions, but for the manual actions that you might have to take that you never anticipated you were going to have to take. Let's not forget defense-in-depth here.

MR. JAIN: Shilp, you raised your hand. Are you still there?

MR. VASAVADA: Yes, I'm still here, but I didn't want to stop the discussion. So if anybody else had something to discuss on --

MR. JAIN: Great.

MR. VASAVADA: -- like in the same vein of what was going on, I can wait. That's not too long. But yes.

MR. JAIN: Oh, okay. All right.

MR. CARTE: Warren?

MR. ODESS-GILLETT: Yes. So, let's give, let's come up with another situation here. So if you do Points 1 through 3, and my experience is that as much as possible the licensee tries to credit the manual actuation to cope with each event in the safety analysis concurrent with a CCF. But there are those cases where it's not fast enough and therefore then we need the automatic diverse actuation to make sure we meet the relaxed criteria.

Now, listening to Rich, if I also had a duplicate manual control for that automatic control, regardless of evaluating critical safety functions, would that meet Point 4?

MR. STATTEL: I don't understand where duplicate control comes in.

MR. ODESS-GILLETT: In other words, I need an automatic, a diverse automatic actuation in order to maintain the plant in the safe condition.

MR. STATTEL: Okay. So a non-safety related ATWS --

MR. ODESS-GILLETT: Yes.

MR. STATTEL: -- event.

MR. ODESS-GILLETT: Right. So, if for each one of those automatics that I had to add --

MR. STATTEL: Okay.

MR. ODESS-GILLETT: -- for the reverse actuation system --

MR. STATTEL: Okay, I'm following you.

MR. ODESS-GILLETT: -- could, if I added a manual control in addition to those limited automatic controls that we credit in the diverse actual system, that doesn't require any analysis, it's just we're giving the operator the manual control capability of what we've added in the diverse actuation system for the automatic.

MR. SCAROLA: Warren, I agree with you 100 percent. And that's exactly what was done in some licensing applications. There was no analysis related to Point 4, it was simply --

MR. STATTEL: That's right.

MR. SCAROLA: -- these are the diverse actuations that we need, so we're going to have manual initiation of those. And if we had other safety functions, critical safety functions that had no automated action, we simply added manual initiation for the equipment that was needed for those.

There was never an analysis to demonstrate that the manual controls for Point 4 were sufficient for anything. Because as I said, they're for the n+1

event. They're for the event you don't know you need. There was never an analysis.

MR. STATTEL: This has never really been a contentious issue during our evaluations though. Because, well, for one thing, the ability to initiate manual actuations for a diverse system, I don't think anyone, I have never seen anyone propose not having that ability and that it's always been there. Does it require an additional analysis, no. No, I wouldn't think so.

But if all, if you are directly crediting a manual actuation, then I don't think it's a lot to ask that it be diverse and that it, you know. I think when you read the original SRM, or the original SECY, actually going back before the SECY, I think there was an unwritten assumption that it was these critical safety functions that would always be necessary in order to bring the plant to the safe condition to meet the criteria. Actual site boundary criteria.

But I think --

MR. SCAROLA: So, Rich?

MR. STATTEL: -- it's kind of taken, it's taken on a life of its own in these different interpretations. But I don't think that that much thought went into those because it was assumed that if

your safety system is no longer functional, that you would somehow have a reliance on manual actions and those would, in turn, accomplish the critical safety functions that would be needed to meet your boundary conditions.

MR. SCAROLA: But, Rich, the analysis you're referring to is a Point 3 analysis.

MR. STATTEL: I know.

MR. SCAROLA: If in Point 3 you take credit for manual actions, then very clearly they have to be analyzed.

MR. STATTEL: And they have to be diverse.

MR. SCAROLA: Both from a hydraulic point of view and an HFE point of view.

MR. STATTEL: Right. And that goes down to the argument that Point 4 is within the context of the D3 analysis.

MR. DARBALI: Yes, but it's not --

MR. STATTEL: It's not beyond that.

MR. DARBALI: It's not clear.

MR. SCAROLA: Because let's assume that for Point 3 you only need one manual action. And let's say that's the initiation of emergency feedwater for some reason. No, that's not a good example. Let me give a good example here.

Now, let's say for Point 3 that you take credit for the manual closure of the main steam isolation valves. Well that's one safety function. You've got five or six more safety functions that you never credited manual actuation.

And that's the intent of Point 4. Is to have manual initiation capability for all the critical safety functions whether you credited those manual options or not.

MR. STATTEL: No, I don't agree. And we've never applied it that way. So, in other words, when we review a D3 analysis, and within the context of the D3 analysis, we look at what's being credited in the analysis, and we look at if those things are divers and they will function. We come to a reasonable assurance conclusion that they will function in the presence of the CCF.

We don't ask, right, I mean, I can point to dozens of analyses that we've evaluated, we don't ask for functions that are outside of that scope. We never have, right?

So if you want to do those analysis, if you want to show that functions that are not credited in the D3 analysis meet the Point 4 criteria, okay. But that's not in the scope of these four points.

MR. DARBALI: Well, Rich, I think --

MR. STATTEL: I mean, Point 4 is one of four points. And it's intended only to address the CCF. That's what it is.

MR. DARBALI: Well, Rich, I think the reason we haven't --

MR. STATTEL: Why would we?

MR. DARBALI: -- gone further on Point 4 for previous reviews, is because we can tell, based on the description of the modification and design modification architecture, that they're not ripping out those manual controls and displays. And they're not making those part of the digital modification.

So in turn we know they're meeting Point 4. And that's, I think, why we haven't really asked for a separate, tell us how you're meeting Point 4. We can abstract that information from the design.

MR. SCAROLA: Rich, you said something very important. I'm sorry, this is Ken Scarola again. You said something very important. Point 4 is intended to address the CCF.

The CCF that we're looking at is the CCF that adversely impacts the functions required by 603 or 279. One of those functions is manual initiation. So if the CCF adversely affects manual initiation,

it's got to be addressed in Point 4.

MR. STATTEL: I agree. Yes, I agree.

MR. SCAROLA: Whether you credit that manual --

MR. STATTEL: That puts it within scope.

MR. SCAROLA: -- initiation or not, because all the manual initiations that are in there for 603 are not necessarily credited in the accident analysis. Or your D3 analysis.

MR. STATTEL: That's true.

MR. SCAROLA: Well, then you got to make them all work in the presence of a CCF. That's my point, that the Point 1 analysis needs to address all the functions of 603 and 279. And that includes both automated and manual actions. Manual initiation actions.

I think where we run into trouble is when people try to extend Point 4 to include manual actuation. That's a much bigger problem.

MR. TANEJA: Hey, Ken, this is Dinesh. 603 requirements for manual actuation, you know, they can be implemented in your safety related digital, in a protection system, right?

MR. SCAROLA: They can or can't? Did you say can or can't?

MR. TANEJA: Can be, right?

MR. SCAROLA: Can be, yes.

MR. TANEJA: And typically are.

MR. SCAROLA: Yes.

MR. TANEJA: So those manual capabilities are susceptible to potential CCF.

MR. SCAROLA: Certainly.

MR. TANEJA: Okay. So, all what we are saying is that the CCF considerations, potential software common cause, you know, the whole four points are based on the predicament that this failure mechanism is beyond design basis.

By design, your safety system should not fail, right? You're building them to the highest possible quality, and they're supposed to be available under all potential hazards that you recognize.

Now, you n+1 argument is applied here. You know, your potential CCF is an n+1 argument. Now, how do you deal with it, I don't think you need to do a timing analysis or anything like that for the Point 4.

If you do need to rely on a manual actuation to cope with a CCF, I don't think you need to worry about the timing consideration for the four points.

MR. SCAROLA: I agree.

MR. TANEJA: Because that timing consideration is only for Chapter 15 events where you take credit for a manual action.

MR. SCAROLA: I agree with you 100 percent. No analysis --

MR. TANEJA: So I think we are getting --

MR. SCAROLA: -- is needed for Point 4.

MR. TANEJA: So we are getting this argument kind of, you know, we need to basically separate these items out.

MR. SCAROLA: Yes, Dinesh, I agree with you. I don't know why we're talking about any analyses for Point 4, the analyses is Point 3.

If you need manual actions for complying with Point 3, then you do need a timing and an HFE analysis. And a thermal hydraulic analysis.

Point 4 needs nothing, other than you got to have the control and it's an I&C design review. It's not an analytical review at all.

MR. ODESS-GILLETT: But, Ken, you're proposing that Point 4 is just a matter of replicating all of your, if they are susceptible to a CCF, your point is just to replicate all of your manual controls again for Point 4?

MR. SCAROLA: No. That's an overstatement, Warren. And that's what's so important here. You only have to replicate the manual initiation controls, not all the manual controls. You don't have to replicate manual controls at the actuation or the, at component level.

MR. ODESS-GILLETT: Well certainly not at the component level, but maybe you can help me, again, understand the differentiation between initiation and actuation system, system level initiation versus system level actuation.

MR. SCAROLA: Well, the initiation typically refers to what would happen if a bistable were to trip.

MR. ODESS-GILLETT: Okay.

MR. SCAROLA: That's initiation.

MR. ODESS-GILLETT: Okay.

MR. SCAROLA: The actuation typically refers to everything downstream of the voting logic.

MR. ODESS-GILLETT: Okay.

MR. SCAROLA: That's actuation.

MR. ODESS-GILLETT: Okay. So you're proposing --

MR. SCAROLA: And I can tell you that this --

MR. ODESS-GILLETT: Go ahead.

MR. SCAROLA: -- idea of meeting Point 4 at the level of initiation was licensed for System 80+, for US-APWR, for APR-1400. That's all they had for Point 4.

And it was, again, because you wanted to give the operators the ability to take preemptive actions in the presence of a CCF, or to take actions for the n+1 event. That the system didn't actuate automatically for.

MR. DARBALI: But, Ken, you're saying at the initiation level that's diverse. But certainly you're not saying that anything downstream would be subject to the same CCF, right?

MR. SCAROLA: You have to address the CCF at all levels. Absolutely, you have to address CCF at all levels.

You may have a CCF at the component level and no CCFs at the initiation or the actuation level. Well that CCF at the component level is as debilitating to the plant as a CCF at the initiation level. In fact, even more debilitating to the plant. So yes, you do have to address the CCF at all levels.

MR. DARBALI: Okay.

MR. CARTE: Sorry, a quick point. Somehow

I get this notice that this meeting is locked. Did someone lock the meeting, no one else can join, or did we just run out of slots?

MR. JAIN: I don't think it's been locked. Not from my end.

MR. CARTE: Okay, so --

MR. DARBALI: I do want to go back to something that Warren had mentioned when we were talking about DAS. I just want to clarify.

I think, Warren, you had said, or you had asked, if the DAS has a manual pushbutton. And of course, the DAS is diverse from your system so it's not subject to the same CCF. So if the DAS has a manual pushbutton, that meets Point 4.

MR. ODESS-GILLETT: Understood.

MR. DARBALI: Okay.

MR. ODESS-GILLETT: My question is, how many of those do you need if you can claim that I have, let's say I've been able to cope with a CCF using 1 through 3, and I only need, I was able to do it all with manual actuations, except maybe three automatic functions. And does that mean, does Point 4 say then, okay, I only need manual controls for three of those, those three automatic functions?

MR. DARBALI: Point 4 says you need a

diverse manual means for all critical safety functions.

MR. ODESS-GILLETT: Yes, that's what I thought. So it seems to me it's like, you've already demonstrated you've coped with both automatic and manual and we'll even throw in the manual to back up the automatic, but that's still not good enough, we still have to have diverse manual controls for all critical safety functions after you've addressed the coping mechanism using non-safety control systems, anything else that exists and so on.

MR. DARBALI: Right. So you would only need those manuals, right. Those manual controls you credited at Point 3, they need Point 4 for critical safety functions.

MR. ODESS-GILLETT: I got you.

MR. DARBALI: Any DAS you credit or any diverse means that you credit in Point 3, that also has an option for a manual pushbutton. Whether that diverse system is digital or analog, that's going to meet Point 4.

It would be a case where you have no ability to manually perform that critical safety function that you need to do something extra for Point 4. Which for an operating plant that you're not

ripping out controls, wouldn't be the case.

MR. ODESS-GILLETT: Yes. But, Samir, we do have to take into consideration, we want to move into the future and --

MR. DARBALI: Right.

MR. ODESS-GILLETT: -- have glass control rooms.

MR. DARBALI: Yes.

MR. ODESS-GILLETT: But I think we're, I understand what you can credit in Point 4, as part of credit, doing in Parts 1 through 3. I'm just seeing that, and this is also my, I don't know what the word is, my concern about Ken's proposal that you basically, regardless of what you have done to cope, you need to add these manual controls in addition to being able to demonstrate that you've been able to cope with a minimum set of manual controls and a minimum set of automatic controls.

MR. CARTE: So, Warren, let me just jump in here a little bit. So I understand your concern, but I think there is two parts of Ken's issue. And let me try and summarize the other part.

So let's visualize the architecture as a three-layered architecture with a bistable function layer, a voting logic layer and say an implementation

layer. And I think what Ken is saying is that, so the question is, those manual inputs, are those separate inputs into the logic layer, because obviously they're not separate inputs into the bistable layer, but are they separate inputs into the logic layer where the voting is done or are they separate inputs to the implementation layer?

So your reactor trip system says trip, and in parallel you have a manual system that says trip. Or your ESF says containment isolation, and in parallel your manual system says containment and isolation. And then the implementation portion received both inputs and performs all of the actuation functions. Right?

So first I'd like a little clarification on, Ken, where you're saying those manual control inputs going into, do they go into the logic or they go into the implementation?

MR. ODESS-GILLETT: The assumption is that those would go into the logic.

MR. SCAROLA: There is no requirement for that. They have to go into the place where you bypass the CCF.

MR. ODESS-GILLETT: Okay, we're talking two different things, Ken. He's asking me about the

603 controls for your primary protection system.

MR. SCAROLA: They typically go into the initiation level or the actuation level. But depending upon the vendor.

MR. ODESS-GILLETT: Yes.

MR. CARTE: So I guess I'm hearing both Warren and Ken agree that the logic, the manual inputs go in, are inputs into the logic layer, and sometimes into the implementation layer. And so the question is, if you have a CCF in the logic layer, if that's part of your system, then your CCF would disable the manual function, but, and therefore you would need a diverse function to do that?

MR. ODESS-GILLETT: The question is, what do you need in a beyond design basis event of a CCF concurrent with your safety analysis evaluation?

And if you're saying that in addition to successfully coping, I also need to have these diverse manual system controls to maintain 603, I think it is, with today's technology and reliability I don't think it's necessary.

MR. CARTE: Right. But my interpretation is not that the, that SECY or the SRM is requiring additional displays and controls above and beyond what you have, it's putting criteria on the set that you

have. Now, if the set that you have doesn't satisfy the SECY, then you may want to put in, it may be easier to build diverse displays and control than to make the existing ones satisfy the SECY. Right?

But in general I don't, and Samir's point earlier was that what we've seen to date on the existing power plants is they're not changing, significantly, the operating interface in the control room. And therefore Point 4 is not such a big deal.

MR. SCAROLA: Right.

MR. CARTE: But, Warren, your point is that the new facilities want glass control rooms, but the problem with a glass control room is, how do you do a safety related manual control on a glass control room. So that's a different set of issues than they're diverse.

But, Rich, I see you have your hand up.

MR. STATTELL: Well, I just wanted to respond. So in such a system that you describe, Warren, I would expect the analysis itself to identify the loss of those manual functions. But I would also expect the analysis to identify other diverse functions.

They could be manual, they could be a diverse automatic actuation system that would

accomplish the necessary critical safety functions to maintain safety for the plant. Plant safety.

So, you know, I don't rule that out, the possibility. And I've actually seen some designs that don't even make an attempt to have diverse manual initiation at the system level. On the safety system.

But in every one of those cases I also see some diverse system, and it may be performing a completely different safety function. But it's maintaining the critical safety functions. They're all still maintained. Even if I don't have an alternate means of manually actuating the primary safety function itself.

MR. DARBALI: I want to give a chance to Khoi and Mohammad who have been waiting. Khoi, go ahead.

MR. NGUYEN: Hi. I just want to --

MR. ALAVI: Hi. Oh, okay.

MR. NGUYEN: I'm sorry.

MR. ALAVI: Oh, sorry. Go ahead, Khoi, he didn't call me yet.

MR. NGUYEN: Yes, I just wanted to clarify the point that we have been back and forth on. Whether it's initiation or actuation.

So, Reg Guide 1.62, manual initiation of

the protective action, even though the title of the reg guide is initiation. But the start of six and seven make the statement that the point at which the manual control are connected to the safety equipment should be downstream of the Digital I&C safety system output.

To me that's a actuation. You shouldn't initiate the control and send the signal through either bistable, processor or any voting logic, you should actuate the A&D device, like pump and valve, whatever. So I just wanted to clarify one thing that we keep talking whether it's initiated or actuated. Thank you.

MR. JAIN: Thank you, Khoi. Now Mohammad.

MR. ALAVI: Yes. Actually, so the topics right now we're talking, I mean, that's -- I mean, two subjects. The one is the manual, the capability of the manual control by the operator, and the other one, the CCF.

So there is an overlap between these two. And maybe it's not exactly the same in all the situations. So, having the manual control input to the logic, that can address that event n+1 that Ken was elaborating, which is the common design, loss of the design I&C.

But if we have a CCF in the software of the safety instrument, that system, obviously that manual input to the logic doesn't make sense. So that has to go to the actuation.

So in my opinion, maybe these two points have to be separated and each one, each objective evaluated separately. So having the manual, capability of manual control ability for the operator is a total different thing. And cope with the CCF, that's different things that we can address in the Point 3 if we go with the system, I think, assessment. Going with the, all assessment, for the D3.

So that's what I get from this discussion I wanted to point out.

MR. DARBALI: Thank you.

MR. JAIN: Thank you, Mohammad. I see Ken's hand is still raised. Ken, do you have any more questions or comments?

MR. SCAROLA: Yes, I raised it again. I think we have to avoid trying to design in this meeting. You know, all these architectures can be very different.

In an operating plant you may have a digital upgrade for one layer of the architecture or two layers or three layers. In new plants, all three

layers are always going to be digital.

You know, we have to stop designing and recognize the intent here. The intent is that your manual control be able to initiate control of the safety functions in the presence of a CCF that you can't get rid of. It's that simple.

Regardless of where the CCF is in the architecture, you have to design your manual control so it's not adversely impacted by that CCF. And I don't think we should be trying to design in any more detail than that in this meeting.

MR. JAIN: Thank you, Ken. Are there other questions or comments of the feedback on staff's presentation?

MR. CARTE: Yes. My only comment would be on Ken's issue. I don't think we're trying to design but we're trying, I feel the need for concrete examples to clarify the meaning of some of the, because I think there is this impression that we're talking, I get this impression we're talking past each other a little bit. And it's strictly abstract you may never solve the problem, as philosophers never solve anything, right?

But if we can get the concrete real-world examples, then maybe. And that's the point. I'm not

trying to design, I'm trying to concretize. Give a couple examples of what would work. But I see that raised a couple of issues.

MR. SCAROLA: Well, Norbert, the problem is, regardless of what's digital, does not mean that that digital thing has a CCF potential. We have many examples where the digital is of sufficient simplicity where we were able to preclude a CCF.

And that has very often occurred at the lowest level in the architecture. Where the implementation, or what we call component control, is utilized by both the primary actuation system and the backup diverse actuation system. Therefore we don't postulate a CCF in that because it's sufficiently simple.

So, you know, it's very hard to discuss this on a generic basis other than to say, the CCF cannot adversely affect the manual control, now go design it.

MR. ODESS-GILLETT: And that's kind of where I disagree because in a lot of aspects the manual controls are a backup to the automatic controls. And in your D3 analysis you have analyzed how you can cope with your CCF of both your automatic and your manual controls.

And if there is a concern that we're relying on an automatic control and it feels like the need that you need to have also a manual along with the automatic, that I think would be sufficient versus replicating your backup manual controls. Not replicating your manual controls in a backup system.

MR. SCAROLA: If you go that way, Warren, then you're throwing out the wisdom of 603 and 279. Those documents recognize that we haven't analyzed everything and there could be events that the operators need to take action on that we have not considered.

And you need to think about the same things when you postulate a CCF in those safety systems that we're relying on that had hat manual capability. And that's what Point 4 is all about. It always has been from the very beginning.

MR. JAIN: Alan.

MR. CAMPBELL: Yeah, I just wanted to -- I think Warren summarized our points pretty well. He said most of what I wanted to say. But, you know, I think we're still in a position now where there's confusion around this, from what I'm hearing.

And if we need to pull up some examples, we had an example that we provided as part of the ACRS

meeting package that I can share. Or we also provided a diagram to the NRC staff showing some different concepts, if it's helpful to facilitate more conversation around this to be a little bit more exacting in the way we're speaking.

MR. STATTEL: Hey, Ken, this is Rich. Nothing we do here is going to impact anything that's in IEEE 603 or those regulatory requirements. So I don't see there being any risk at undermining any of the existing protections that 603 provides.

MR. SCAROLA: Yes, I agree. You are not going to undermine anything that's required by 603 through this SECY or anything the staff is doing. It's the CCF that undermines the functions of 603. So now the question is do you still need those functions of 603 in the presence of a CCF. And I believe you do. The functions of 603 are not only the automatic functions but the manual functions as well.

MR. ODESS-GILLETT: And I guess where I'm coming from is that 603 defines your design bases of the plant and then, if you go into beyond design basis with relaxed criteria, you don't necessarily need to maintain 603 to do that.

MR. SCAROLA: Yeah, I guess it comes down to what do you define as outside the design bases. I

believe the anticipation of the n+1 event is within the design bases of 603. That's why 603 requires manual action, the capability for manual actions, because within the design basis you anticipate the unanticipated event.

MS. DONAHUE: But are we not in a n+1+1 event now, n+2? We have the IEEE, we're saying the design basis event, now a CCF. So Points 1 through 3 have your coping mechanisms for that, but now we're adding this extra layer of manual controls and displays for an extra layer. It just -- we're stacking -- how many layers are sufficient here?

MR. SCAROLA: Well, Alan, you're not adding anything. You're maintaining what was there in the presence of a digital CCF. You're not adding, you're maintaining.

(Simultaneous speaking.)

MS. DONAHUE: Is it okay if I share my screen?

MR. CARTE: Yes, no objection. So I don't think it's our adding, maintaining, or you're designing such that. So whether you say adding or maintaining, your design is such that you maintain.

MS. DONAHUE: So this is a slide that we had as background material for the ACRS meeting in

September. This is the US-APWR, all the protection system functions. So this is slightly modified. We re-labeled the columns here.

This first or second column, rather, is the automatic -- this is your IEEE 603 automatic function. This is the, this third column is the IEEE 603 required manual function. Then we get into DAS system.

So points one through 3 drive us into these three different DAS automatic functions. And then this last column are the diverse manual functions. Sorry, that was the second to the last column. The last column is, are those manual functions actually credited in the D3 analysis?

So I think what Warren, the question that at least I heard from Warren and, Warren, correct me if I'm misstating you, is in the scenario of ECCS and EFW actuation, the vendor here determined that an automatic function was needed.

We still, the vendor still had to include a diverse manual function to satisfy Point 4, but it's not credited in any of the D3 analysis.

Warren, your question was are these switches needed, right? Did I summarize that correctly?

MR. ODESS-GILLETT: That's right.

MR. DARBALI: So I want to make one point clear, so this is based on the APWR which the review for this design has not been completed. So the design has not been approved. So we can't say here that those two additional switches that you're showing intended to meet Point 4.

If that was a decision made by the Applicant, we can't say that that was in response to an NRC review of the application or that the NRC had determined that it met or didn't meet Point 4. So let's be clear that this has not been proved.

MR. CAMPBELL: Yeah, understood. I think, you know, the point that we're trying to -- this is indicative, through my review of the different D3 analyses that are publicly docketed and things, this is indicative of a common, I won't say the interpretation but a common interpretation of how Point 4 has been implemented where, regardless of whether it's being credited in a D3 analysis, it's still being added.

So the concern here, and I want to bring this back to safety, the concern here is the complexity at the operator, right. So now we're getting into a scenario where we have three different

initiation sources for the same, I'm sorry, four different initiation sources for the same function and the complexity that that introduces to an operator.

MR. SCAROLA: Alan, this is Ken. There's something important on this chart that you're missing. You're pointing out that the switches for ECCS and emergency feed water actuation are not credited in the D3 Point 3 analysis. I agree 100 percent. They're not.

But what you're failing to mention is, in the second column where you have those same switches, they are not credited in the Chapter 15 analysis. But yet we still have them. And why do we have them? We have them because 603 gave us the wisdom to recognize that there may be another event where we need them. And therefore we should give operators that capability.

MR. CAMPBELL: And I would say that we did give them that capability through the set of -- in the IEEE required. And then we also gave them that ability, we also gave them protection during a CCF through an automatic function.

MR. DARBALI: But I think what Ken is saying is, and correct me, Ken, if I'm wrong, that you're giving the ability in that second column by

providing the switch to the digital system. So you're giving the manual ability.

The CCF is taking away that ability, so that switch on the fourth column is maintaining that ability. Because the DAS, and I'm assuming the DAS you're highlighting doesn't have a push-button. So by adding the switch on the fourth column, you are maintaining that ability. Is that correct, Ken?

MR. SCAROLA: Not quite. Yes, you are maintaining the capability, but the way that switch worked on US-APWR is it simply initiated the DAS. But the initiation of the DAS was sufficient because the DAS intercepted into the architecture at a very low level where there was no longer a CCF concern. So it was okay to initiate the DAS.

If the DAS didn't penetrate low enough into the architecture, then you would have to do something else to meet Point 4. Because then that same thing would be subject to a CCF. So the DAS, in this case the switch simply initiated the DAS.

MR. ODESS-GILLETT: So I guess our point is that it seems that we're imposing 603 not only on the protection system design basis, but we're imposing 603 on our DAS system.

MR. SCAROLA: Warren, functionally yes,

but it can be non-safety --

MR. ODESS-GILLETT: Oh, yeah.

MR. SCAROLA: It doesn't require any qualification, I mean, so don't say you're imposing 603.

MR. JAIN: Ken, this B.P. Jain. We have very limited time left. And I don't think we are converging at this point. So we need to get back to the purpose of the meeting.

I think we have discussed, got a lot of feedback from different stakeholders. And we'd like to hear from other participants if they have other thoughts or other points of view. I see a hand from Shilp. Shilp?

MR. VASAVADA: Yeah, this is Shilp. So I guess I won't take too much time, but I just -- this is from maybe a different perspective and see if there are any thoughts on that.

And looking forward, I mean, at the expanded policy, the Points 1 through 3 provide, like, a risk-informed alternative in terms of diverse design or (audio interference). And a part of it is, like, using a bounding approach and PRAs to determine the risk significance, and go forward with decision-making based on that.

There was discussion about risk significance, there was discussion about different inputs and outputs. So please bear with me as I kind of lay the context.

PRAs, old manual operator actions for several sequences, the purpose over there is obviously to have an integrated look if systems, safety-related, non-safety related, both don't work with a certain failure probability. Sorry.

COURT REPORTER: This is the Court Reporter. Sorry to intrude. I would encourage anyone not currently speaking to mute their microphones.

MR. VASAVADA: Thanks. The PRAs would have safety related, non-safety related, and then manual actions. Those manual actions go through a process called human reliability analysis (audio interference) does the operator even understand they need to take an action.

The cognition piece has cues, some cues that are -- C-U-E-S, cues -- that the operator needs to mean that an action needs to be taken. Those need displays, those need, for performing the action, controls or at least switches, et cetera.

So then when that (audio interference) made to the sequence that would be included, the

determination would include that manual action. And if, quote, credit, end quote, is being (audio interference) determining the risk impact, then that operator action would have to have the three displays and controls to make sure that it is feasible and valid, and that the inputs, the PRA continues to remain valid.

So I just wanted to understand, like, I mean, where does that fall in all this? Wouldn't that already need something which would not be impacted by the CCF, because otherwise there is no credit could be taken for that action?

I open it up to anybody who has thoughts on that. Thanks.

MR. DARBALI: Go ahead, Warren. You're muted, Warren.

MR. ODESS-GILLETT: Thank you. Sorry about that. And is it Shilp, is that how you pronounce --

MR. VASAVADA: It's Shilp.

MR. ODESS-GILLETT: Okay, Shilp. Okay, thank you. I think what -- I'm not sure if I understood completely, Shilp, what you were saying. But are you asking how, what Position 4 is risk-informed or can be risk-informed, or is it --

MR. VASAVADA: I'm trying to understand, like, in the actual (audio interference) in risk assessment or PRA for digital CCF analysis, one would not achieve Point 4 if the manual action in the PRA is being credited to determine the risk significance. Does that make sense?

MR. ODESS-GILLETT: Well, yes. So I'm not sure if it makes sense to me, but the way Point 4 is written now, even with the risk informed expansion, doesn't seem to take into account risk significance of the manual action at all.

MR. VASAVADA: Okay. So the other way I'm looking at it, and it may be because I'm not an expert in the design aspect of it. But Point 3 has information about a risk informed approach. It also talks about that manual actions can be considered as a form of diversity.

And then Point 4 says, if I'm not mistaken, that anything you consider in Point 3 can be used for Point 4, right. So, I mean, yeah. So again, even if it doesn't explicitly talk about the significance, what I'm trying to get at is while you're doing Point 3, and you're using that sequence from PRA in your actions, it's implicitly considering the risk significance of the reaction.

And then I think it is important, the ability to perform the action. And then for that last line, Point 4, why would you need anything else? I'm unable to understand that.

MR. ODESS-GILLETT: Well, I have a difficulty understanding why we would need -- your statement about why do we need anything else. Can you clarify that?

MR. VASAVADA: So, okay, let me back track and hopefully I'm not taking too much time from next steps, otherwise let's cut it short. (Audio interference) have an action in it, which would need cues and the ability to perform the action. So it would need a display or some control to tell the operator that an action needs to be taken and the way to perform the action, a switch, a push button, what have you.

And that will be included in the risk significance determination. And it would have to be, obviously, not impacted by the -- otherwise the operator action could not occur. So, be a diverse operator action which is un-impacted by the CCF, which can offer a critical safety function. Because the events -- the PRA would include events which would require critical safety functions to be present,

inventory control, decay heat removal, et cetera.

So, then, if that manual action is already being imbedded and not impacted by the CCF, and this last point in Point 4 says these main control room displays and controls may be used to (audio interference) lay together to address the concern that has been raised (audio interference).

MR. ODESS-GILLETT: Shilp, you're cutting out. But I think, from industry's point of view, I think it's fairly -- there's consensus that there's no issue with crediting what you have in remaining controls and Points 1 through 3, that you can apply those to Point 4.

MR. DARBALI: Okay. I think we can move on. Shilp, that was your comment?

MR. VASAVADA: Yeah, I didn't have anything, maybe --

MR. JAIN: Yeah, this is B.P. Jain, you know, we are at that point that if there are other questions, or comments, or feedback on the staff's presentation, you can provide your feedback in writing after the meeting, or by email to me or Mike Marshall.

With that, I would ask Samir to recap the feedback if he could. Samir?

MR. DARBALI: Yeah, just before that, so

I don't forget, Alan, could you send B.P. the slide that you shared. I believe it's the same one you provided at the ACRS meeting, but just so that we can make that part of the record.

MR. CAMPBELL: Yes, will do.

MR. DARBALI: Thank you. And I'll add the additional slides that we showed on the four points and 603 and 279.

So, you know, I think we were able to provide clarity on the applicability of the SECY 22-0076 and the intention with the original Point 4 and how we're carrying that intention to the expanded policy.

I think we clarified the distinction that Point 4 has when compared to the previous, or the first three points. I understand that some of this information or how we're explaining our interpretation might be new to some of the audience, so I recognize that not everybody is 100 percent in alignment. But hopefully we did get closer to that.

And I think we were able to understand a little bit better industry's concerns. One thing to note, and we appreciate all of the feedback and suggestions we've had on ways that the language in the four points could be different. Because it helps us,

you know, think of things that maybe we have not considered or look at the points in a different way.

But the process for developing SECY paper doesn't really have a public comment portion to it. So the SECY is with the Commission and, you know, they'll review it and they'll provide direction to the staff in an SRM which we're waiting on.

A lot of what we heard today, I think, is very good discussion for when we move into the implementing or developing implementing guidance. You know, how do we apply the policy to advance reactors that have a completely different design?

Maybe they have different critical safety functions. They don't have the same types of manual controls or, you know, they don't have a control room as we're used to or we're talking about a completely digital flat panel display control room.

So a lot of that can be addressed through implementing guidance. I think the policy, as we've said before, you know, we allow for alternatives and exemptions that allows us to look at those different reactor designs. So hopefully a lot of the concerns can be addressed properly in implementing guidance. And for those we will obviously have public engagement. Anything that I am missing, B.P.?

MR. JAIN: No. I think you covered it all. Thank you very much, Samir. And I would like Eric to make closing remarks before we close out the meeting. Eric?

MR. BENNER: Yeah, I would -- another good dialogue, we've had several good dialogues on this topic. I will say what has been most helpful to me today is we've heard some different views. We've heard some more specifics. I think that gives us a lot of information to chew on.

I agree with Samir's point that there could be lot done in implementation guidance. I acknowledge that we do, as the staff, have decisions to make whether we would do any additional communications with the Commission, you know, to supplement the paper or other things.

So I don't want to close the door on the idea that, you know, we're just waiting for the Commission, because I think the Commission may also be waiting for us, because we've said we're continuing the dialogue on this topic.

So I don't quite know what the right answer is. I will say I appreciate everyone. Everyone came to the meeting today ready to discuss, at good detail, what the concerns are in either

direction, particularly on Point 4. I think we really focused on Point 4. We knew that was going to be the focus of the discussion.

So I'm not sure what our next step is. We definitely have to digest what we heard today and caucus internally as to what the next step is. Whatever that next step is, we commit to be transparent about it, you know, regarding letting stakeholders know what we're doing.

You know, obviously the Commission gets to do what the Commission wants to do. But we want to keep making sure we understand what the concerns from stakeholders are here. Because, you know, we've done a lot of internal dialogue and felt we were at the right place from a safety standpoint.

But we want to continue to be open to hearing stakeholder views to see if there's any things that we can learn from that. So I will also just turn it over to say if NEI wants to make any closing remarks.

And I see Ken's hand is still up. So, Ken, given that he provided significant input, I'd also be open to hearing to see if he had any closing remarks he wanted to make.

MR. JAIN: Ken or -- Ken is mute.

MR. DARBALI: You're muted, Ken. Alan?

MR. CAMPBELL: Great. And thank you, I appreciate the opportunity to provide some remarks here at the end. Again, thank you guys again for hosting this. I do believe that the discussion was beneficial in helping to understand your perspectives a little bit more. And then hopefully we were able to communicate the industry perspectives as well.

I think that we're still, as Eric, I believe, you acknowledged, I think we still have some work to do on Point 4 regarding the language. You know, some of what I heard there is some alignment in the interpretation, but the language itself isn't leading to that interpretation from our perspective. And so we look forward to continue to be able to work with you guys and engage with you on this in the future.

MR. JAIN: Thank you, Alan. Ken, you have a statement to make, closing remarks?

MR. SCAROLA: Yeah, thank you. We've been focusing exclusively on Point 4 here. But I want to raise the point that there is really a bigger issue here. Industry and NRC need to recognize that the cost of nuclear power is our enemy.

If nuclear power is going to remain

viable, there's a need for significant O&M cost reduction. And the biggest part of that is operator staffing. We need to reduce operator staff. And the only way we're going to do that is with more complex, non-safety and safety digital systems.

We need more automation, we need better human system interfaces, and unfortunately that complexity leads to a higher likelihood of a design defect and therefore a higher likelihood of a CCF.

And I'm very concerned that our need for increased complexity is going to outpace our ability to prevent design defects or manage them through risk-informed methods. It's just not going to happen. We need the complexity. And that complexity is going to be very, very difficult to overcome.

Therefore, diversity may be our only viable solution. So I would really like to see the staff and industry focusing on ways to achieve cost effective diversity. You know, the diversity can be very simple.

A diverse actuation system can be non-safety, it doesn't have to have all the same functions as the primary protection system. It has to be adequate. It's not the enemy. Diverse protection systems facilitate more complex primary systems that

are absolutely necessary to achieve cost effective nuclear power.

So while we're focusing here on ways to eliminate the need for diversity through risk-informed methods, I think we're kidding ourselves. I really do. I think we have to recognize that the complexity of our primary systems has to grow if we're going to be cost effective. And with that growth, we're not going to be able to manage the potential for design defects to risk-informed methods.

MR. JAIN: Thank you very much, Ken, appreciate it. With that, I'd like to thank all the participants for this meeting and providing the feedback. With that, I would like the meeting adjourned.

(Whereupon, the above-entitled matter went off the record at 4:01 p.m.)

U.S.NRC

United States Nuclear Regulatory Commission

Protecting People and the Environment

SECY-22-0076
"Expansion of Current Policy on Potential Common-Cause Failures in Digital Instrumentation and Control Systems"

Public Meeting
October 20, 2022

Presentation Outline

- Recent Activities and Current Status
- Purpose of Today's Meeting
- Staff Key Messages
- Summary of Proposed Expanded Policy
- Staff Position on ACRS Questions
- Point 4 Applicability and Clarifications
- Open Dialogue with Stakeholders

Recent Activities and Current Status

- The staff issued SECY-22-0076 on August 10, 2022, proposing an expansion to the digital instrumentation and control (DI&C) common cause failure (CCF) policy contained in the Staff Requirements Memorandum (SRM) to SECY-93-087
- The Nuclear Energy Institute (NEI) provided a letter to the NRC on August 26, 2022, providing comments on the staff's position contained in the SECY on diverse and independent main control room displays and manual controls
- The staff and NEI briefed the Advisory Committee on Reactor Safeguards (ACRS) DI&C Subcommittee on September 23, 2022, and the staff is scheduled to brief the full ACRS on November 1, 2022
- The SECY is currently under Commission review and the Commission will provide its direction to the staff through a Staff Requirements Memorandum

Purpose of Today's Meeting

The staff will use today's meeting to:

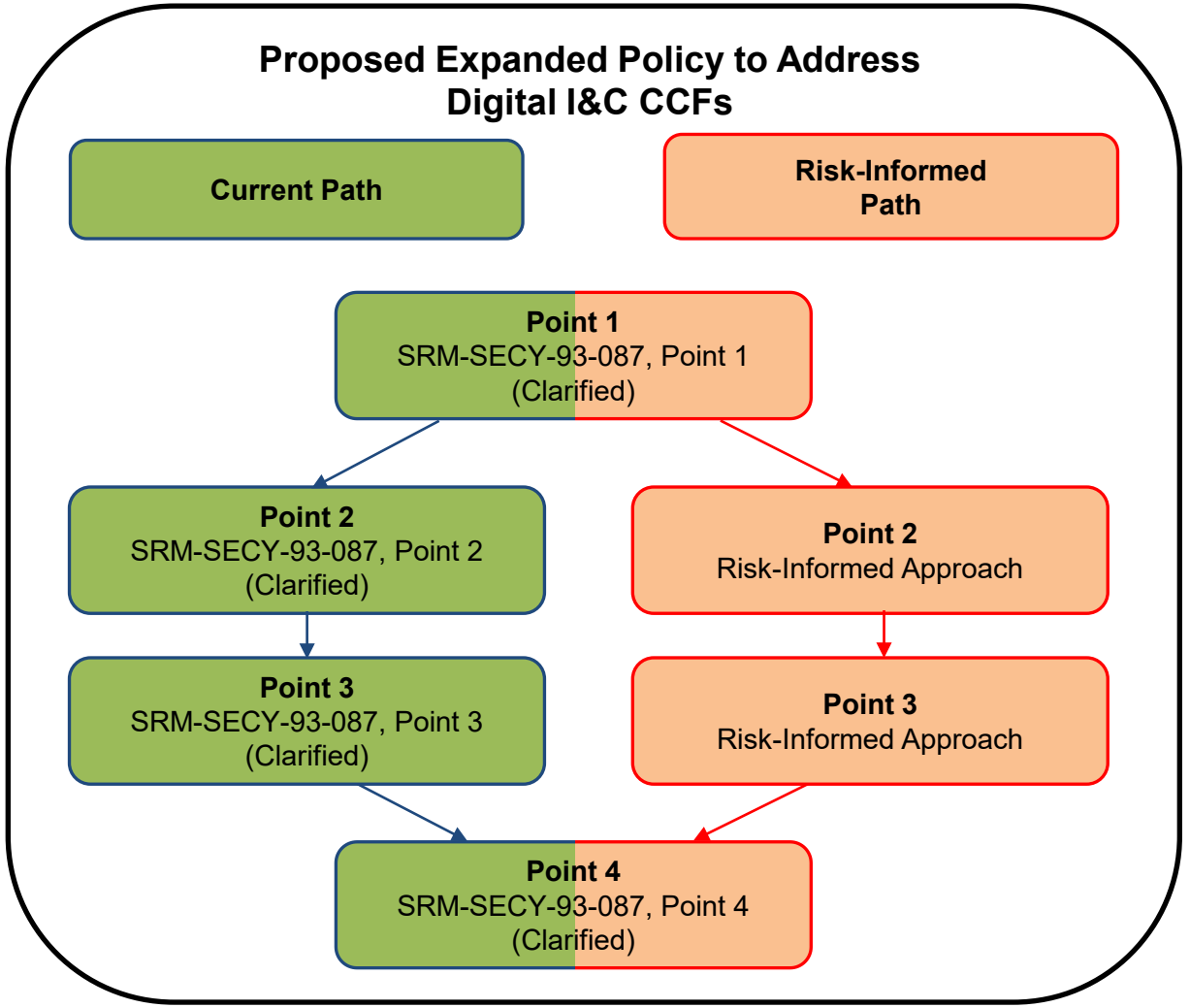
1) Summarize the expanded policy contained in SECY-22-0076
2) Share the staff's position on questions received from the ACRS
3) Share the staff's position on diverse and independent main control room displays and manual controls, i.e., "Point 4"
4) Conduct an open dialogue with stakeholders to hear their perspectives

Staff Key Messages

- The proposed expanded policy in SECY-22-0076 encompasses the current four points of SRM-SECY-93-087 (with clarifications) and expands the use of risk-informed approaches in points 2 and 3.
- Points 1-3 and Point 4 of the policy address two facets needed to ensure safe operation of the plant:
  - Points 1-3 ensure DI&C systems are sufficiently robust to adequately cope with CCF
  - Point 4 ensures operators can manually control critical safety functions even in the event of a DI&C CCF
- Point 4 incorporates an implicit element of risk-informing as it focuses only on those critical safety functions needed to ensure the safety of the facility.
- The expanded policy is intended to be technology neutral and applies to any reactors (including non-light-water reactors) licensed under 10 CFR Parts 50 and 52.
- The staff acknowledges that the critical safety functions listed in SRM-SECY-93-087, SECY-22-0076 and Branch Technical Position (BTP) 7-19 (i.e., reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity) may not be the appropriate set for all reactor designs
- The SECY provides for existing regulatory tools (exemptions and alternatives), if necessary, to accommodate for reactor designs with different critical safety functions
- If the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

Summary of Proposed Expanded Policy

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

Staff Positions on ACRS Questions

ACRS Question 1: *Would the revised policy be applicable to advanced reactors?*
Answer: The proposed expanded policy would apply to requests all nuclear power plant types licensed under 10 CFR Part 50 and 10 CFR Part 52, including advanced reactors.

ACRS Question 2: *Do aspects of the policy for which the staff did not request a change carry forward unaltered?*
Answer: Yes

ACRS Question 3: *Might different reactor types warrant consideration of different critical safety functions?*
Answer: While the expansion of the policy is intended to be technology neutral it relies on the staff's licensing experience to date and assumptions about the design of the facility, such as the presence of a main control room. The staff acknowledges that the critical safety functions listed in the SECY and BTP 7-19 (reactivity control, core heat removal, reactor coolant inventory, containment isolation, and containment integrity) may not be the appropriate set for all reactor designs. The staff has existing regulatory tools (exemptions and alternatives), if necessary, to accommodate designs with different critical safety functions and, if the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

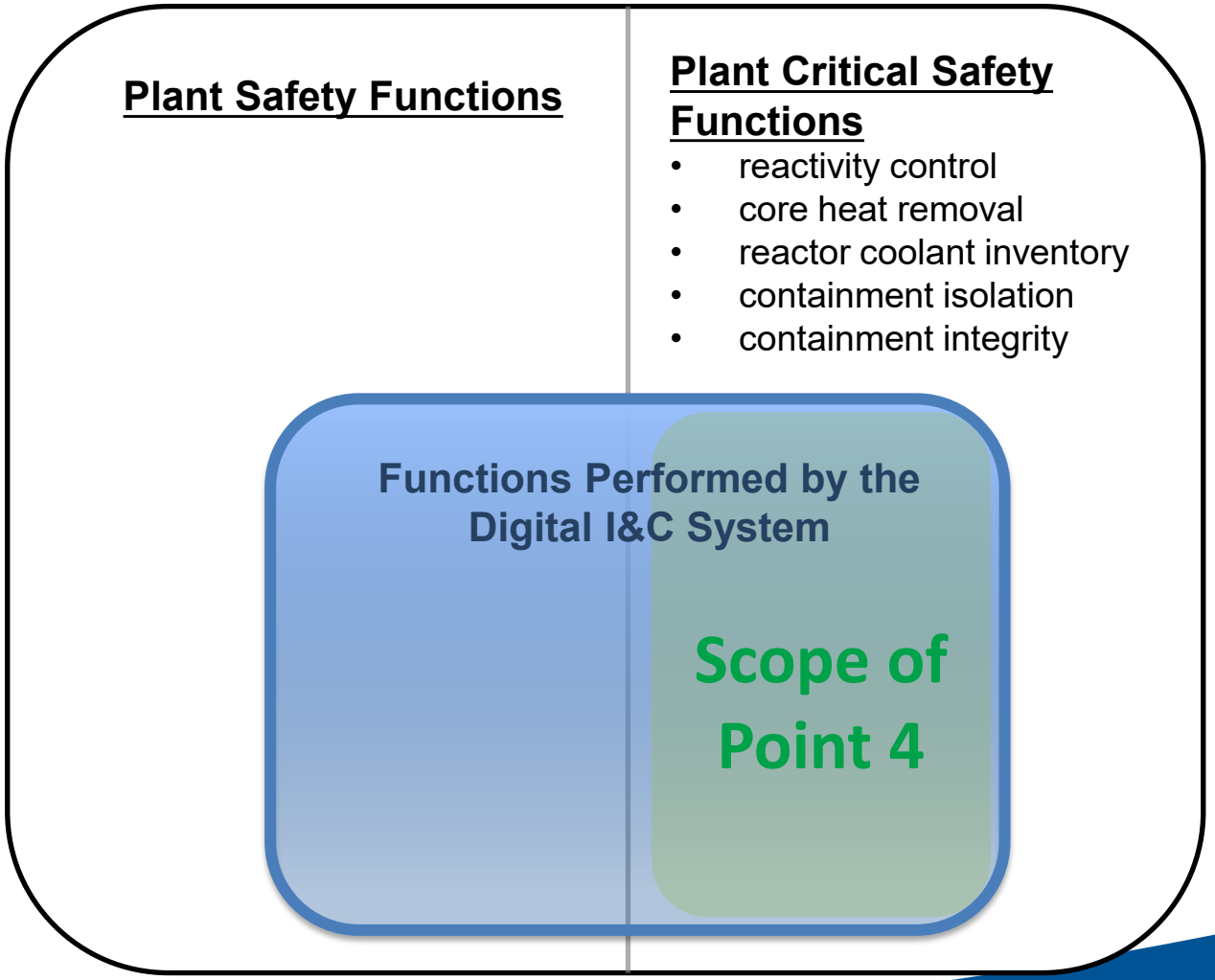
Applicability of Point 4

Point 4 only applies to:

- The critical safety functions performed by the digital I&C system.

Point 4 does not apply to:

- All safety functions performed by the digital I&C system.
- Critical safety functions not performed by the digital I&C system.



The diverse manual controls and displays for critical safety functions ensure the safety of the facility.

Staff's Position on Diverse and Independent Main Control Room Displays and Manual Controls

- In SECY-93-087, the staff recommended that safety-grade displays and controls located in the main control room and hardwired to the lowest level of the safety computer system architecture, be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions and that the displays and controls should be independent and diverse from the safety computer system identified in Points 1 and 3 of the policy.
- The staff recommended this because such controls and displays provide the plant operators with unambiguous information and control capabilities to enable the operators to expeditiously mitigate the effects of the postulated common-cause software failure of the digital safety I&C system. The control room would be the center of activities to safely cope with the event, which could also involve the initiation and implementation of the plant emergency plan. The design of the plant should not require operators to leave the control room for such an event.

Staff's Position on Diverse and Independent Main Control Room Displays and Manual Controls (contd.)

- While the Commission's Staff Requirements Memorandum to SECY-93-087 modified the policy to permit non-safety grade displays and controls and more flexible architectural implementation, the Commission supported the staff's recommendation on diverse displays and controls, and the staff continues to believe this position remains appropriate for critical safety functions to provide reasonable assurance of adequate protection.
- Point 4 incorporates an implicit element of risk-informing as it focuses only on those critical safety functions needed to ensure the safety of the facility.
- Requests for exemptions (under 10 CFR 50.12 or 52.7) or alternatives (under 10 CFR 50.55a(z)) provide avenues for applicants to request a deviation from the regulations based on risk information on a case-by-case basis.
- If the staff encounters a reactor design where the policy would not be applicable, the staff will engage the Commission as appropriate.

SECY-22-0076: Addressing DI&C CCFs & Ensuring the Ability to Perform Manual Actions

Points 1-3 and Point 4 address two facets needed to ensure the safe operation of the plant

Protection against DI&C CCFs
to cope with the loss of a safety function

- Point 1 – Perform a D3 Assessment
- Point 2 – Ways of performing the assessment
- Point 3 – Ways of addressing a postulated DI&C CCF

Allow operators to take manual actions
when needed, after a DI&C CCF

- Point 4 – Diverse displays and manual controls for critical safety functions

- If not addressed, a DI&C CCF can affect both the DI&C system and manual controls and displays

- The four points when taken together provide criteria for the assessment of diversity and defense in depth against CCF, and ensure DI&C CCFs do not:
  - Defeat safety functions (Points 1-3)
  - Impede operators' ability to take manual actions when needed (Point 4)

Open Dialogue with Stakeholders

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
I&C	Instrumentation and control
NEI	Nuclear Energy Institute
NRC	Nuclear Regulatory Commission
PRA	Probabilistic Risk Assessment
RG	Regulatory Guide
RPS	Reactor Protection System
SAR	Safety Analysis Report
SECY	Commission Paper
SRM	Staff Requirements Memorandum

Backup Slides

SECY-22-0076: Point 1

The applicant shall assess the defense in depth and diversity of the facility incorporating the proposed digital I&C system to demonstrate that vulnerabilities to digital CCFs have been adequately identified and addressed.

The defense-in-depth and diversity assessment shall be commensurate with the risk significance of the proposed digital I&C system.

SECY-22-0076: Point 2

In performing the defense-in-depth and diversity assessment, the applicant shall analyze each postulated CCF. This assessment may use either best-estimate methods or a risk informed approach.

When using best-estimate methods, the applicant shall demonstrate adequate defense in depth and diversity within the facility's design for each event evaluated in the accident analysis section of the safety analysis report.

When using a risk-informed approach, the applicant shall include an evaluation of the approach against the Commission's policy and guidance, including any applicable regulations, for risk-informed decision-making. The NRC staff will review applications that use risk-informed approaches for consistency with established NRC policy and guidance on risk-informed decision making (e.g., Regulatory Guide (RG) 1.174, "An Approach for Using Probabilistic Risk Assessment in Risk Informed Decisions on Plant Specific Changes to the Licensing Basis").

SECY-22-0076: Point 3

The defense-in-depth and diversity assessment may demonstrate that a postulated CCF can be reasonably prevented or mitigated or is not risk significant. The applicant shall demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures, other than diversity, that are credited in the assessment. The level of technical justification demonstrating the adequacy of these techniques or measures, other than diversity, to address potential CCFs shall be commensurate with the risk significance of each postulated CCF.

A diverse means that performs either the same function or a different function is acceptable to address a CCF, provided that the assessment includes a documented basis showing that the diverse means is unlikely to be subject to the same CCF. The diverse means may be performed by a system that is not safety-related if the system is of sufficient quality to reliably perform the necessary function under the associated event conditions. Either automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation.

If a postulated CCF is risk significant and the assessment does not demonstrate the adequacy of other design techniques, prevention measures, or mitigation measures, then a diverse means shall be provided.

SECY-22-0076: Point 4

Main control room displays and controls that are independent and diverse from the proposed digital I&C system (i.e., unlikely to be subject to the same CCF) shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. These main control room displays and controls may be used to address point 3, above.

IEEE Std 279

- "**4.17 Manual Initiation.** The protection system shall include means for manual initiation of each protective action at the system level (for example, reactor trip, containment isolation, safety injection, core spray, etc). No single failure, as defined by the note following Section 4.2, within the manual, automatic, or common portions of the protection system shall prevent initiation of protective action by manual or automatic means. Manual initiation should depend upon the operation of a minimum of equipment." [emphasis added]
- "**4.20 Information Read-Out.** The protection system shall be designed to provide the operator with accurate, complete, and timely information pertinent to its own status and to generating station safety. The design shall minimize the development of conditions which would cause meters, annunciators, recorders, alarms, etc, to give anomalous indications confusing to the operator."

IEEE Std 603-1991

- "**6.2 Manual Control**
- **6.2.1** Means shall be provided in the control room to implement manual initiation at the division level of the automatically initiated protective actions. The means provided shall minimize the number of discrete operator manipulations and shall depend on the operation of a minimum of equipment consistent with the constraints of 5.6.1." [emphasis added]

Gen IV Light Water Reactor Example

Protection System Function	IEEE Req'd Automatic Function	IEEE Req'd Manual Function	SECY Points 1-3 (D3 Analysis) Diverse Automatic Function	SECY Point 4 Diverse Manual Function	SECY Point 4 Manual Action Credited in D3 Analysis?
Reactor Trip	RPS	1 switch/train	DAS (Note 3)	1 switch	Yes (Note 4)
Containment Isolation Phase A	ESF	2 switches	-	1 switch	Yes
Containment Isolation Phase B	ESF	Note 1	-	-	-
Containment Purge Isolation	ESF	Note 2	-	-	-
Containment Spray Actuation	ESF	2 switches/train	-	-	-
CVCS Isolation	ESF	2 switches	-	-	-
Emergency Core Cooling System (ECCS)	ESF	1 switch/train	DAS	1 switch	-
Emergency Feedwater (EFW) Actuation	ESF	1 switch/train	DAS	1 switch	-
Emergency Feedwater (EFW) Isolation	ESF	2 switches/train	-	1 switch/SG	Yes
Main Feedwater Isolation	ESF	2 switches	-	-	-
Main Steam Line Isolation	ESF	2 switches	-	1 switch/SG	Yes
MCR Isolation	ESF	1 switch/train	-	-	-
Main Steam Depressurization Valve	-	-	-	1 switch/SG	Yes
Safety Depressurization Valve	-	-	-	1 switch	Yes

Note 1: Initiated upon Manual Core Spray actuation
Note 2: Initiated upon Manual Core Spray or Manual Containment Isolation Phase A actuation
Note 3: Also includes Turbine Trip and Main Feedwater Isolation
Note 4: Manual trip required for Steam Generator Tube Rupture. Other scenarios credit DAS automatic signal.