Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Advisory Committee on Reactor Safeguards

Docket Number: (n/a)

Location: teleconference

Date: Tuesday, November 1, 2022

Work Order No.: NRC-2149 Pages 1-98

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

DISCLAIMER

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

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

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

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

700TH MEETING

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

TUESDAY

NOVEMBER 1, 2022

+ + + + +

The Advisory Committee met via teleconference at 1:00 p.m., Joy L. Rempe, Chairman, presiding.

COMMITTEE MEMBERS:

JOY L. REMPE, Chairman

WALTER L. KIRCHNER, Vice Chairman

DAVID A. PETTI, Member-at-Large

RONALD G. BALLINGER, Member

VICKI M. BIER, Member

CHARLES H. BROWN, JR., Member

VESNA B. DIMITRIJEVIC, Member

GREGORY H. HALNON, Member

JOSE A. MARCH-LEUBA, Member

MATTHEW W. SUNSERI, Member

ACRS CONSULTANT:

STEPHEN SCHULTZ

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

C-O-N-T-E-N-T-S

P R O C E E D I N G S

(1:00 p.m.)

CHAIRMAN REMPE: Good afternoon. This meeting will now come to order. This is the first day of the 700th meeting of the Advisory Committee on reactive safeguards.

I'm Joy Rempe, Chairman of the ACRS. Other Members in attendance are Ron Ballinger, Charles Brown, Vesna Dimitrijevic, Greg Halnon, Walt Kirchner, Jose March-Leuba, Dave Petti, Matt Sunseri and I believe we're going to be joined soon by Vicki Bier.

I note we do have a quorum and today the Committee is meeting in person and virtually. The ACRS was established by the Atomic Energy Act and is governed by the Federal Advisory Committee Act.

The ACRS section of the U.S. NRC Public website provides information about the history of this Committee and documents such as our charter, bylaws, Federal Register Notices for meetings, letter reports and transcripts of all full and subcommittee meetings including all slides presented at the open meetings.

The Committee provides its advice on safety matters to the Commission through its publicly available letter reports. The Federal Register notice announcing this meeting was published on October 14th,

2022.

This announcement provided a meeting agenda as well as instructions for interested parties to submit written documents or request opportunities to address the Committee.

The Designated Federal Officer for today's meeting is Ms. Christina Antonescu. A communications channel has been opened to allow members of the public to monitor the open portions of the meeting.

Members of the public may use an MS Teams link to these slides and other discussion materials during these open sessions. MS Teams link information was placed in the Federal Register Notice and Agenda on the ACR's public website.

We received no written comments or requests to make oral statements from members of the public regarding today's sessions. Periodically the meeting will be open to accept comments from participants listening to our meetings.

Written comments may be forwarded to Ms. Christina Antonescu. During today's meeting, the Committee will consider two topics. The SECY on Potential Expansion of Current NRC Policy on Common Cost Failures and Regulatory Guide 1.82, Rev 5, Water Sources for Long-term Recirculation Cooling following

a Loss-of-Coolant Accident.

A transcript of the open portions of the meeting is being kept and it is requested the speakers identify themselves and speak with sufficient clarity and volume so they can be readily heard.

Additionally, participants should mute themselves when not speaking. So at this time, I'd like to ask other members if they have any opening remarks.

PARTICIPANT: Thank you, Madame Chair.

MEMBER BIER: Joy, I have no opening remarks, but I just wanted to let you know I'm in attendance. I joined a couple of minutes late.

CHAIRMAN REMPE: Thank you, Vicki. Member Kirchner, would you like to --

MEMBER KIRCHNER: Yes, thank you, Madame Chair.

CHAIRMAN REMPE: Yes.

MEMBER KIRCHNER: So today is the 700th meeting of the Advisory Committee on reactor safeguards. And I thought it might be of use and historical value to share some information with you.

In 1947, the U.S. Atomic Energy Commission recognized the need for an independent technical group to review and provide advice on reactor safety matters.

And thus, a Reactor Safeguard Committee was formed chaired by Dr. Edward Teller.

In 1950, the AEC established a second committee called the Industrial Committee on Reactor Location Problems which was chaired by C. Rogers McCullough.

And it was charged with the responsibility of advising on what we would today consider siding issues including seismic and hydrological characteristics of proposed sites.

In 1953, the Reactor Safeguard Committee and the Industrial Committee on Reactor Location Problems were combined by the AEC and the ACRS was formally established.

There were 13 Members on that original Committee. Mr. McCullough continued as the Chair, four from academies, seven from industry, interestingly enough, one from an insurance company and one from the U.S. Weather Bureau.

And they were assisted by a secretary which would be our Executive Director today. And in noting this, I would like to look forward approximately five years from today will be the 750th meeting and I'd like to put a marker down.

I think it would be appropriate at that

point under some new Chair to host a conference that would mark ACRS contributions to reactors safety. And hopefully they would invite past members as well to attend.

And I would note such a conference was held evidently in concert with the 500th meeting of this Committee. With that, I thank you, Madame Chairman.

CHAIRMAN REMPE: Thank you for the historical reminder of the history of this Committee. Any other members have any other opening remarks? So if not, I'd like to ask the Member Charles Brown to lead us in our first topic for today's meeting.

MEMBER BROWN: Might be nice if I turned my microphone on. Okay, this is just as, we're going to run through fundamentally what we ran through during the subcommittee meeting. It's whose, NRC, Samir, are you going to be doing the presentation for this?

MR. BENNER: Samir will be leading the --

MR. BROWN: I can't hear you.

MR. BENNER: -- presentation, Member Brown. This is Eric Benner, I'll do the kickoff from our side.

MR. BROWN: We've got a -- yes, we can't hear you right now. I guess we've got a technical problem.

CHAIRMAN REMPE: Oh, could you speak again? Let's see, I've increased the volume and I hope that helps.

MR. BENNER: Okay. One, two, --

MEMBER BROWN: No.

MR. BENNER: -- three, four.

CHAIRMAN REMPE: Can you also increase your volume.

MR. BENNER: My microphone volume? I will, yes.

MEMBER BROWN: Yes, you're very faint, Eric.

CHAIRMAN REMPE: Yes, that helps. Other people I can hear. And so it's just you, Eric.

MR. BENNER: Okay, is that any better?

CHAIRMAN REMPE: Maybe just get real close to your mic and I think we'll manage.

MR. BENNER: Okay. I, my piece is fairly short so I will speak loudly and then turn it over to people who can better manipulate this equipment. Again, so as Member Brown said, this will largely replicate what we discussed at the subcommittee meeting.

I will say in respect for the Committee's time, we have abbreviated some of what I would call

the background and have focused it more on the issues that were raised at the subcommittee meeting both by the subcommittee and in the industry presentation.

But we will, we certainly will go anywhere in the discussion where the Committee wants to go. We thank you for your time and with that, I will turn it over to Samir.

MEMBER KIRCHNER: Yes, before we continue, Charlie, can you just introduce the topic so it's on the record and transcript?

MEMBER BROWN: Oh, okay. This is an expansion of the SECY, get the right date, what's the old one? '83, no, '93-087 on Common Cause Failure and the SRM that the Commission provided providing their additional comments and observations on.

And they will go through those as part of this overall presentation point by point through the SECY and the Commission's comments on it. Did I get that correct, Samir?

MR. DARBALI: Yes.

MEMBER BROWN: Okay, and one observation I would make and I don't, we didn't beat on this as much as we maybe should have, but one of the key points for, if I can find down and see where the right answer is of this expansion of the policy is to address the

diversity, allow risk assessments to address diversity of the design in terms of multiple software, different processors, whatever diversity sort of means that comes into play.

While you're going through this and others who are there, just one of the things I like to talk about after you finish the presentation just explores, when you talk about not providing any diverse automatic actuation of safety functions, how do you envision that?

What is the thought process as opposed to just the magic words of saying with the risk-informed approach we would be addressing whether you would need diverse automatic actuation of safety functions as has been done for the last 30 years or more.

So just keep that in mind until we get to the end. We go through the presentation and other than that, I'll turn it over to you, Samir.

MR. DARBALI: Okay. Thank you, Member Brown and thank you, Eric. Oh, alongside me presenting this afternoon will be Steven Alferink and Norbert Carte.

And our project managers for this project are BP Jain and Michael Marshall. And we've also had a diverse membership in our working group and a lot of support from NRR and research staff.

Here's the outline for our presentation today. We'll go over the background and key messages from our effort to expand the Digital I&C Common Cause Failure Policy.

We'll cover the purpose of the proposed expanded policy described in SECY 22-076. We'll present the Staff's position on the questions the ACRS Digital I&C subcommittee asked the Staff back in the September meeting.

We'll go over the new points in SECY 22-076 and we'll finish by discussing the next steps. As we know, nuclear power plants continue to install Digital I&C technology which results in increased reliability and safety benefits.

However, this use of digital technology can also introduce digital common cause failures. The current policy on Digital I&C CCFs is in Staff Requirements Memorandum to SECY 93-087 which requires a diverse means of a postulated common cause failure could disable a safety function.

The diverse means may be an automatic or an action or include manual actions. The Staff has been expanding the use of risk Informed approach as much as is allowed by these SRI.

However, the current policy does not allow

for the use of risk informed approaches to determine when a diverse means would not be required. Because of this, the Staff developed SECY 22-076 to allow for greater use of risk-informed approaches to address Digital I&C CCFs for high safety significant systems.

The key messages from our presentation are that the proposed expanded policy in SECY-22-076 encompasses the current points of SRM-SECY-93-087 and expands the use of risk-informed approaches in Points 2 and 3.

When taken together, the four points provide criteria for the assessment of diversity and defense and depth against CCFs. Use of risk-informed approaches will be consistent with the Safety Goal Policy Statement, the PRA Policy Statement and SRM-SECY-98-144.

The current policy will continue to remain a valid option for applicants and licensees and Point 4 regarding dependent and diversity's place in manual controls ensures the health and safety of the public.

And it is already risk informed as it focuses only on those critical safety functions needed to ensure the safety of the facility. The purpose of the SECY is to request the Commission, expand the current policy to allow the use of risk-informed

approaches to demonstrate the appropriate level of defense and depth including not providing any diverse automatic actuation of safety functions.

This expanded policy would be applicable to new or amended licenses and design approvals for all nuclear power plants, power plant types under Parts 50 and 52.

The Staff sent the SECY to the Commission in August of this year and we are currently waiting for direction from the Commission on how to move forward. I'm on slide 8 now.

The ACRS Digital I&C subcommittee provided some question to the Staff during the September meeting. The first question was if the revised policy would be applicable to advanced reactors.

And the answer to this question is yes. The policy would apply to advanced reactors, licensed under Parts 50 and 52. When we get to the third question below, we'll explain how reactor designs that may or may not seem to fit within the policy would be addressed.

The second question was related to whether those aspects of the current policy for which the Staff did not request a change carry forward unaltered.

This question was focused on Point 4 and the Commission's statement in SRM-SECY-93-087 that

certain requirements in the original SECY were highly prescriptive.

One of these requirements being that the diversities placed a manner of controls had to be hardwired. The ACR CRL subcommittee noted that the SECY-22-076 was silent on this matter and wanted to know if expanded policy maintain the Commission's direction from the original SRM.

The answer to his question is yes, the Staff intended to maintain the Commission's direction regarding this matter.

MEMBER BROWN: I guess, this is Charlie, I guess the point being is there is nothing that says that in the 0076 as presently written. At least I didn't find it. Is that correct?

MR. DARBALI: Correct. It is --

MEMBER BROWN: Okay.

MR. DARBALI: It is 22-076 did not mention anything specifically from 93-087, then we're carrying that forward.

MEMBER BROWN: Okay, go ahead.

MR. DARBALI: Okay. And the last question was if different reactor types warrant consideration of different critical safety functions. And the answer is yes.

The expanded policy is intended to be technology neutral, but it does rely on the Staff's licensing experience and assumptions about the design of the facility such as the process of a main control room.

We recognize that the critical safety functions listed in the original SECY in SECY-22-076, and in BTP-7-019, may not be the appropriate set for all reactor designs.

But the expanded policy provides for the use of existing regulatory tools like extensions and alternatives that, if necessary, can be used to accommodate 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. Any questions before I continue?

All right, here on Slide 9, it's a figure that shows the proposed expanded policy that encompasses the current position in SRM-SECY-93-087 with clarifications and provides for risk-informed approaches in Points 2 and 3 to address Digital I&C Common Cause Failures.

The current path shown on the left in green

allows for the use of best estimate analysis and diverse means to address a potential CCF. Whereas the risk-informed path on the right allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential CCF.

And I know we'll get these towards the end, but we're talking about consideration of whether the CCF can be properly prevented or mitigated. And in the next slides, we'll show each of the four points of the expanded policy.

This Slide shows Point 1 of SECY-22-076 which calls for a defense in diversity assessment of the facility incorporating the proposed Digital I&C system.

This assessment is to be, is to demonstrate that vulnerabilities to Digital I&C CCFs have been adequately identified and addressed. Point 1 does not preclude the use of risk-informed approaches for the D-3 assessment.

And the level of rigor of the assessment is to be commensurate with the risk significance of the Digital I&C system. The current guidance in branch technical positions 7-019, Revision 8 supports a greater approach in applying a level of rigor for the

D3 assessment.

And we'll continue to refine this guidance if needed. I will now turn it over to Steve Alferink who will go over Points 2 and 3.

MR. ALFERINK: Thank you, sir. This is Steven Alferink. As Samir said, I'll discuss Points 2 and 3 of the proposed policy. Point 2 contains the requirements for evaluating postulated Digital I&C CCFs.

As you can see on the slide, Point 2 consists of three paragraphs. The first paragraph requires that Applicants analyze each postulated CCF in the D3 assessment and it allows Applicants to use either best estimate methods or a risk-informed approach.

The second paragraph describes the evaluation when using best estimate methods. This paragraph meets the intent of the current Point 2 with some minor wording changes.

This paragraph requires that Applicants consider each event evaluated in the accident analysis section of the Safety Analysis report when analyzing each postulated CCF.

The third paragraph describes the evaluation when using a risk-informed approach. This

paragraph is in addition to the current Point 2. This paragraph requires the Applicants evaluate the risk-informed approach against the Commission's policy and guidance of risk-informed decision making.

This paragraph also specifies that the Staff will review Applications that use risk-informed approaches or consistency with established policy and guidance and risk-informed decision making.

In contrast to the evaluation using best estimate methods, the Staff expects the Applicants using a risk-informed approach will consider a broad spectrum of initiating events not limited to only those evaluated in the accident analysis section of the Safety Analysis Report.

Next slide please. With respect to Point 2, the Staff's goal is that the acceptance criteria for risk-informed approaches for Digital I&C CCFs will be consistent with the NRC's broader practices and guidance for risk-informed decision making and not specific to Digital I&C.

As an example, the Staff intends to review license amendment requests that use risk-informed approaches for conformance to the guidance in Reg Guide 1.174. The Staff does not envision approaches that are radical departures from existing practices. Next

slide please.

MEMBER BROWN: Oh, don't go. Don't leave yet. This is Charlie. How are you going to make a decision that you're not going to accept their approach using a risk-informed decision?

MR. ALFERINK: Well I --

MEMBER BROWN: You haven't laid out any guidelines for that yet.

MR. ALFERINK: That's correct. We still have to develop the implementing guidance. I would say at this point, we're just envisioning that it will not be a radical departure.

MEMBER BROWN: Where would you put this implementing guidance? Radical departure and stuff like that, those are critical words. And you mentioned this in the last meeting.

MR. ALFERINK: I think the intent is we would like to keep it within the current paradigm. We're not intending to do something that's completely different.

MEMBER BROWN: But well, if you don't have a diverse, that's completely different. Isn't it?

MR. ALFERINK: I'm talking about the regulatory process for evaluating it.

MEMBER BROWN: Okay, my question then is

how do you determine whether you're going to accept the risk-informed approach or not? That you don't have any implementing guidance for?

MR. ALFERINK: That's correct. We still have to develop the implementing guidance for that.

MEMBER BROWN: So you don't know how you're going to say no?

MR. ALFERINK: At this point, the guidance has not been developed so you're correct.

MEMBER BROWN: And if --

MR. DARBALI: And I believe what Steven is saying is that risk-informed approaches have been used in other disciplines outside of Digital I&C and so we want to maintain consistency with those.

MEMBER BROWN: Okay, that's kind of amorphous. All right, I'm making the point just so that Members will, Committee Members will understand that this is a, we have an objective to approach to taking this approach.

We didn't say that obviously you're all intending to try to go in that direction. The key issue here is how do you know, how do you make a decision to say no and because you're not saying, you're not requiring them to do something?

Everything is now based on the

risk-informed approach. Even Point 1 says has added the word about risk-informed decision making even though there were no real details for that. Two and three were where the meat and potatoes were.

So okay that's just something that we need to think about. Go ahead.

MR. ALFERINK: Okay so now we should be on Slide 14. So now we'll discuss Point 3 as the proposed policy. Point 3 contains the requirements for addressing postulated Digital I&C CCFs.

When discussing Point 3 it is helpful to keep in mind that the current policy requires a diverse means to address postulated CCFs that can disable a safety function.

Point 3 also consists of three paragraphs. The first paragraph describes the outcome of the D3 assessment. This paragraph requires that applicants demonstrate the adequacy of any design techniques, prevention measures, or mitigation measures other than diversity.

This paragraph also requires that the level of technical justification for demonstrating the adequacy of these measures or techniques other than diversity be commensurate with the risk significance of each postulated CCF.

The second paragraph meets the intent of the current Point 3. This paragraph specifies that a diverse means is acceptable to address the postulated CCF.

This paragraph also specifies that automatic or manual actuation within an acceptable timeframe is an acceptable means of diverse actuation. I would note that BTP-7-019 Revision 8 provides the Staff guidance for determining if automatic and manual actuations can be performed within an acceptable timeframe.

MEMBER BROWN: Okay, I've got a question. Have you accepted other circumstances in the older plans where automatic, where manual actuation is an acceptable diverse actuation method, explicitly accepted it?

MR. ALFERINK: I would defer to Samir or Norbert on that one.

MR. CARTE: Norbert Carte, I&C. Even in newer plants we've done that so on the digital upgrade for Oconee, basically only two of the functions had a diverse actuation systems high pressure, low pressure safety injection.

The other functions were deemed to have enough time to do it manually. Oconee actually

believed they had enough time to do all but one. There was a disagreement about that and we sort of forced them to put in two rather than just one.

But they concluded they only need diverse actuation for one. We concluded they needed it for two and we, and they put in for two, but not all safety functions.

MEMBER BROWN: What were the two again?

MR. ALFERINK: High pressure and low pressure safety injection.

MEMBER BROWN: Okay, what about reactor trip?

MR. CARTE: So they already have an ATWS system or they already met the ATWS requirements so we didn't impose anything additional for reactive trip. And I see Dinesh has his hand up.

MR. TANEJA: Yes, Member Brown. The ABWR design certification that we certified back in mid-90s, the SECY-93-087's origination is really, you know, connected to the review of that design cert application from GE at that time.

And when we look at the certified design, this concern was raised, the CCF concern and the solution where we accepted was the worse manual actuation of high pressure injection and low pressure

injection and the analog display indications of level reactor vessel level for initiating those two functions manually as diverse means.

The reactor trip scram function was already available in a manual scram. So those manual actions, you know, as diverse means were what we accepted to satisfy the CCF concern for the ABWR design.

And, you know, the SECY paper was really written too in connection with our review of the ABWR design cert application because it was all digital at that time.

MEMBER BROWN: You mentioned the Oconee application. You all approved that just as I arrived in 2008 so early '09. We never reviewed that that I know of. I'm not aware of the Committee reviewing that design approach.

Go ahead, that one was a little puzzling to me. It just appeared. When I first got here all of a sudden it was approved. So that detail is lost on us somewhat so the memory bank is pretty well drained on that one. All right.

MEMBER HALNON: Charlie, I had a question.

MEMBER BROWN: Oh, go ahead, Greg.

MEMBER HALNON: Yes, this is Greg Halnon. Just to kind of explore this manual a little bit

further. To be acceptable, what is the pedigree behind a manual actuation?

There's five parts to a manual actuation when there's a failure detection diagnosis procedure that procedure determination actions and then verification the action taken is, was supposed.

So I guess the question is with the training, the knowledge and abilities procedural perspective, what are you looking for to make sure that would be an acceptable --

MR. CARTE: Well --

MEMBER HALNON: -- means?

MR. CARTE: -- so first of all, 603 and 279 basically require that for every automatic actuation there's a manual means to do it. Initiate at the system or division level and that needs to be safety related.

There are also associated requirements for the display of information association with manual actions. So in terms of equipment design, the I&C review is to ensure the equipment has the capability.

The human factors folks review implementation operator training and that sort of thing and I'm less familiar with that.

MEMBER HALNON: Okay. All right, the

reason I ask is acceptable timeframe is certainly part of it. But there's also that first part which the pre-emptive should be able to diagnose and detect and determine what you're going to be doing both procedure out, make sure you're doing it by procedure then verify.

So I was wondering if there was anything in your thought process behind this allowing a manual actuation beyond just the acceptable timeframe.

MR. CARTE: Well so, we generally use the human factors people to evaluate operator responses associated with the D3 analysis. So in terms of the regulatory requirements and that says the means shall be there, whether the, there's sufficient time to do it, to meet the diversity in defense and depth analysis, is a D3 criteria and generally we involve the human factors people to do that review.

MEMBER HALNON: Okay. And that would probably be expected to be a deep dive into the training and the abilities of the operator and so forth, so forth. Is that what you're saying?

MR. CARTE: Yes, I can't speak much to what they do.

MEMBER HALNON: Okay.

MR. DARBALI: Yes, this is Samir. And I believe that for the Oconee example, it was determined

in the D3 assessment that those two functions would not be performed in a timely manner. And thus, a diverse actuation system was needed.

MEMBER HALNON: Okay. So that just shows that there is a deeper dive somewhere else in the review process.

MR. CARTE: Right and in Oconee, it wasn't strictly analysis. They did do some tests with operators in the simulator to support that they could perform the actions.

MEMBER HALNON: Okay. That's what I was looking for to see, you know, make sure we were just outside of these words and to some other assessment or inspection or whatever the case may be to ensure that the human factors piece was still there. Thank you. That's it.

MEMBER BROWN: I've got a note. Norbert, you quoted 603, 19-091, about the requirements, but if you look at the new rule making that's disappeared. So that stuff is not in there explicitly anymore. It's all off in guidance if it's there anywhere.

MR. CARTE: New rule, you mean Part --

MEMBER BROWN: Part 53.

MR. CARTE: Part 53. Okay, I'm less familiar with Part 53 maybe someone can chime in if

I'm wrong, but my understanding is mostly the difference between Part 50, 52 and 53 is that there are different processes and the technical criteria are predominantly in Part 50.

So I'm not sure to how much extent Part 53 invokes Part 50 technical criteria. But that's the --

MEMBER BROWN: It just --

MR. CARTE: -- my general idea.

MEMBER BROWN: -- it depends on which framework you're in if I'm not mistaken. Dave, isn't that correct? Or if the, you got the Part Frame B, Frame A and Framework A and B? Framework A is, is that the risk-informed one?

CHAIRMAN REMPE: No, it's --

MEMBER BROWN: And B is the more traditional.

MR. CARTE: Well okay, the other part is. One, this doesn't apply to 53 and two, 53 isn't done so it's a little bit, three, I'm not involved in it so I, it's a little hard to speculate on that.

MEMBER BROWN: Yes. One of the next questions is when we talk about manual means, to me manual means are very explicit. I turn a switch, there's a wire going somewhere, operates a circuit

breaker or relay starts a motor, closes a valve, does whatever.

In other words, there is no intermediate computer-based system like somebody's touching a touch screen that's says close. And you're depending on another computer system to then process that data and then get it down in trip something else or the same thing that would have been tripped otherwise.

It pretty much when you get to the new technology approaches to doing that in terms of what is an acceptable manual means? Does that mean totally divorced from computers or software? Is that clear anywhere or is that you're envisioning it, but it's not stated?

MR. CARTE: I think there's some flexibility there. And --

MEMBER BROWN: That's what I was afraid of.

MR. CARTE: We have a Reg Guide 1.62 that discusses that, but I believe that manual means could use safety related display systems to implement the manual actuation.

If you look at the current plant designs, there's various levels of independence that the, that a manual switches have. So I believe on combustion

engineering designs the manual switches are just equivalent to a bi-stable input to the voting logic, but then it's relay voting.

So when you replace the relay voting system with a digital system, you put your switches into that digital system. That hasn't been decided yet because no one has upgraded a combustion engineering protection system yet.

Other facilities, the switches bypass some of the voting logic and go directly to implementation of the function. So it's a little bit design and function specific how much independence the manual switches have.

MEMBER BROWN: If I wanted to scram the plant, I certainly wouldn't want to go through the voting units. That doesn't make any sense. You ought to go trip the scram breakers. Period.

Or if you wanted to start a pump, a fuel pump if you need fuel systems or if you need some other system, you ought to start the pump. It ought not be voted on. Manual is manual.

You don't wait to see if you have two or three or four of them in there. But that's subject to another discussion. I'm just --

MR. CARTE: Well right. What gets into

that discussion is how complicated the function you're implementing. So when you're implementing a reactor trip, in effect, you're just moving two breakers.

If you're trying to do containment isolation or diesel load sequences, you've got this shed the bus, load the bus and how much independent logic you have associated with the manual push button as opposed to the automatic system.

Or they just both provided an input to the diesel load sequencer. And then that diesel load sequencer does what it does. So part of that, it gets complicated depending on the complexity of the implementation function. That's part of the problem.

MEMBER BROWN: You know, that's a little bit more back in the other parts of the plant would typically we have focused on the reactor protection side and the engineered safety actuation feature side.

Not necessarily diesel generator sequencing. All right, so --

MR. CARTE: All right.

MEMBER BROWN: -- as much as going to be even more amorphous now. All right. I guess anybody else have any other questions or -- okay, go ahead.

MR. ALFERINK: Thank you. So I'll pick up with the third paragraph. The third paragraph

requires that a diverse means be provided if a postulated CCF is risk significant and the D3 assessment is unable to demonstrate that measures other than diversity are adequate.

So this paragraph acts as a fallback position. To summarize this Point 63, Point 3 allows measures other than diverse means to be used with appropriate justification.

If appropriate justification cannot be provided, then diverse means must be used. Next slide please. With respect to Point 3, the Staff has the following expectations for a license member request.

First, the risk significance of postulated CCFs will be determined by any increase in risk to the facility using the traditional measures of increase and core damage frequency or large early release records.

Second, this increase in risk would be determined using a quantitative bounding assessment. Current experience is insufficient to establish confidence and quantifying the probability of occurrence of Digital I&C CCFs.

However, current experience may be sufficient to establish founding values that can be used in a quantitative bounding assessment. The Staff

expects the applicants may have flexibility in selecting a bounding value.

The choice of a bounding value may vary from system to system depending on the design and it could be less than 1.0 with justification. The Staff has confidence that a bounding assessment can account for the uncertainties in quantifying the probability of occurrence of Digital I&C CCFs. Because --

MEMBER BROWN: Just a second.

MR. DARBALI: -- of the lack of --

MEMBER BROWN: Go ahead. I'll ask after you're finished.

MR. DARBALI: Thank you. Because of the lack of confidence and quantifying the probability of occurrence of Digital I&C CCFs, the Staff will not be able to approve risk-informed quantitative approaches based on reducing the probability of occurrence of Digital I&C CCFs through design techniques or for high safety significance SSEs.

MEMBER BROWN: All this, all this commentary that you make about your ability to assess, trying to phrase this correctly, that really requires at the design stage if it's a new plant, new application, or a replacement even for back fit that you have a pretty detailed architecture structure from which to make

these judgments.

Without that architecture, it's just nothing that people say and what they're going to do without one-line diagram showing the architecture and why they can justify it seems to me somewhere you've got to be expressing that.

I know right now it's been introduced in 7-019. It's also in the design and review design specific review standards, the last two that have been used. It's not in the SRP yet.

But it is in I think ISG-06, the licensing approach that you do pre-licensing submittal. You could argue that with the requirements you had before, but once you go to the risk-informed approach, that you need a more comprehensive architecture from which to make these judgments as to whether they're approached as okay or not. Am I misstating that or do you all disagree?

MR. ALFERINK: I have a different way to envision it from my perspective it would be a little bit simpler approach. You don't need all the detail drawings.

You just need to have an understanding for what the system will do and how it can interact and then choose a suitably large bounding value for your

risk assessment.

MEMBER BROWN: I didn't say detailed drawings, but an architecture can be shown on a single sheet of paper as we have done in all the last three or four design certifications we've run.

That's -- those have been detailed enough that you could make that judgment or it would enable you to make that judgment.

MR. DARBALI: Though we would still expect to see that level of detailing the architecture. When we may not get to see or an alternate review process application is the software side.

MEMBER BROWN: I got that. The architectural protection from the software side if you do it right partially protects you anyway. All right, you can go ahead.

MEMBER MARCH-LEUBA: No, no.

MR. DARBALI: Yes --

MEMBER MARCH-LEUBA: Hold it. I was just going say how --

MEMBER BROWN: Please go ahead.

MEMBER MARCH-LEUBA: Just to entertain you. Explain to me, I'm having problem understanding this slide. You, you're saying that we have to evaluate the risk to the facility.

And typically risk to the facility is determined as the CDF or the LERF or frequency of something bad happening. And then on the last part you say, but this time doesn't really believe the probability of occurrence of CCF that you calculate anyway.

So if we don't have any confidence on the probability of this hidden factor, how do we have confidence on the risk which is the product of that and something?

MR. ALFERINK: The intent here is that we will be able to pick a value that's large enough it should encompass all the uncertainty. For example, let's just pick a value, you know, 0.1 for the probability of occurrence of the CCF.

I think everyone would likely agree that would be a bounding number. Then we would not have to go into the details to determine is it really 20 negative two, negative three, negative four.

If we agree that there's a suitably large value then we can perform the risk assessment with that and then not worry about the uncertainty in determining the actual value.

MEMBER MARCH-LEUBA: So you can correlate the increase in say callosity assuming a resolutely

high probability of occurrence of the CCF and then you don't --

MR. CARTE: Issue the -- I wouldn't use the phrase ridiculously high probability of occurrence. So I would --

MEMBER MARCH-LEUBA: You said this in Point 1.

MR. CARTE: Well no --

MEMBER BROWN: Zero point one is definitely --

MEMBER MARCH-LEUBA: A 10 percent chance of, is a really critically high probability. I mean, or you have a really bad design.

MR. CARTE: Well no, I was just looking at a report out of the oil and gas industry yesterday, today. And they were looking at CCFs of transmitters and things like that.

And they came up with a range, their estimate for realistic estimate of CCFs for their redundant components was between .1 and .2. If .11 was the lowest CCF probability they had and Point 2 was the highest.

So their CCF range for 61-511, 61-508 compliant facilities was between .1. That was the realistic estimate. It was between .1 and .2. Now

that didn't include logic solvents.

That was just things like the damper, the dampers we'll point to, but values, sensors, and things like that. So between .1 and .2, was the basically oil and gas industry standard for CCF.

Based on over 1,400 components analyzed or failures analyzed.

MEMBER BROWN: This is a nuclear plant not an oil and gas.

MR. CARTE: Right, but --

MEMBER BROWN: There's a big difference. I mean you, we had one problem in the country. One problem shut down the entire industry.

MR. CARTE: No, I get that, but we've also just approved the commercial grade dedication process where we use 61-508-03 certified components. So it's the same components used in the oil and gas.

MEMBER BROWN: Yes, but if they're using an architecture that's well defined, then you can certainly get yourself better than .1.

MR. CARTE: Well, yes. Well okay --

MEMBER BROWN: That's my point.

MR. CARTE: So yes --

MEMBER BROWN: That's my point. Norbert, that's my point. You keep nibbling this thing down

to ridiculously low numbers when the focus on all of these safety systems and what we've done at least try to bring ourselves through them has been to make sure we could see that I could mentally and just qualitatively if nothing else, that there's a pretty low probability without going through a math hurricane of some kind.

So I'm just, you can't compare oil and gas to a nuclear power plant. If an oil and gas plant say has a catastrophic failure, you're not going to shut down all the, you'll build more.

If you do that with a nuclear power plant, you won't build any more. We've already done that '79 until now. What is that? Thirty, 42 years, 43 years? The consequences are different even if you, even if they're nebulous.

I mean, they were, the consequences were virtually nothing. Then you look what happened. You just got to be careful of the way you throw the comparisons around. That's all I'm saying.

The rest of the Committee members can speak out, tell me I'm off the wall, but that's my --

MEMBER MARCH-LEUBA: My gut feeling when you tell me 10 percent almost go failure is reasonable and expected. And it's not even covering an abundant

case which is 11 percent. I said you'd better use better components.

But going back to my original question then, if I expected all the probability failure is 11 percent. What I'm bounding you should use at least 20, 25. And then --

MR. CARTE: Right, so --

MEMBER MARCH-LEUBA: What redundancy you have? I mean, you, don't put two of them, just keep only one. You're not getting anything in that empty space.

MR. CARTE: Right. So basically we have an established acceptance criteria yet, but they will have, they would propose and justify a particular bounding value.

But we expect it to be relatively large rather than relatively small. It's kind of where we're at today.

MEMBER MARCH-LEUBA: But it has to be abundantly obvious to a reviewer familiar with the subject that it is conservative.

MR. CARTE: Well --

MEMBER MARCH-LEUBA: It's easy when you have thousands of components and you can look at the statistics over the last ten years. We typically don't

have that luxury. Okay, I just put it on the record. I see a little logic failure here when we're going through implementation.

MEMBER BROWN: And I would, let me amplify Jose's comment a little bit because our comment on the commercial dedication, we made the point that whatever components you picked in our letter back which you all responded to and that those parts have to be compatible with being incorporated into the architectures we use for the fire plants and you all did that.

You did, you converted a few words into regulatory sausage making, but it came out reading okay because you effectively say you have to have an, you have to know what your system looks like and that it will comply with our requirements before you can use the commercially dedicated component.

That was a good write up. So anyway, that's our thoughts. Joy, I interrupted you I think.

CHAIRMAN REMPE: It's okay. This is a very trivial question that I should have brought up during the subcommittee meeting. But it will, may be help in the future for me to understand something.

Why do you have in the SECY six times high safety significance SSEs instead of significant? Is there some reason for this or is it just a typo that

got repeated six times?

MR. DARBALI: I, we went through a lot of wordsmithing and that is the term we agreed on.

CHAIRMAN REMPE: But what's the meaning? Why do you say significance instead of significant there? Why is that terminology important, that distinction? Because it's really awkward and it gets repeated in other places and I just am curious.

MR. DARBALI: I need to check what we said in Branch Technical Position 7-019. Maybe we were looking for consistency, but the intent was the same.

CHAIRMAN REMPE: Okay, so again, I can, I get it will be repeated in the future here and I just, it really is an awkward way of wording it and that's why I'm asking that. Thank you.

MEMBER MARCH-LEUBA: But I thought you were more concerned, I'm simply more concerned about the modifier side whether you use significance or significant.

CHAIRMAN REMPE: Well it doesn't make sense to say significance to me.

MEMBER MARCH-LEUBA: Well what doesn't make sense to me is high. High is in the eye of the beholder. It's either a safety significant or it isn't.

CHAIRMAN REMPE: I agree with you on that too, but again I've seen this high safety significant at other places so that didn't (audio interference). Anyway, go ahead.

MEMBER DIMITRIJEVIC: Well this is Vesna. This is a better terminology. I mean this comes from the, you know, 50.69 that you defined the recent numbers actually which define I mean there is a risk measures.

And the values of these measure define is this kind or loss if it is significant component so. You know, you remember these four quadrants. You know --

CHAIRMAN REMPE: But Vesna, I get what the 50.69, but that's the high and the low, but didn't they use significant with a "t" instead of --

MEMBER DIMITRIJEVIC: Well they use the significance so that's a different in that.

CHAIRMAN REMPE: Yes.

MEMBER DIMITRIJEVIC: But I mean that this is not a value we hold that is clear criteria for these measures that I mean what is the high significance based on this contributing factor or factor vastly so.

MEMBER BROWN: There, I can help you out. I just looked at BTP-7-019 and there's a section in there that says acceptance of safety significance

determinations, the following criteria applies.

High safety significance or safety related SSEs are performed safety significant functions, work on that one for a few minutes. SSCs in this category have one or more of the following characteristics.

And then there are three bullets that follow up. They're credited in the FSAR to perform design functions that contribute significantly to plant safety.

They're relied upon to initiate and complete control actions essential to maintaining plant perimeters within acceptable limits established for a DBE or to maintain a plant in a safe state after it reach safe shutdown or their failure to directly lead to accident conditions that may have unacceptable consequences exceeding site doses limits of the DBE.

So it is defined somewhere as to what a high safety significance is in one of the BTPs. I'm glad I looked it up. I had totally forgotten that.

CHAIRMAN REMPE: So basically we're repeating some bad grammar from the PT meetings that we've --

MEMBER BROWN: I, if this is Rev 8, this was reviewed in 2021.

CHAIRMAN REMPE: Okay.

MEMBER BROWN: And it was in the last revision so we are compatriots in messing with something that's vague.

MR. CARTE: Norbert Carte, I&C. There's also another dimension about whether you're talking about a binary perimeter or some sort of continuous so if we say commensurate with safety significance, that gives you, the flexibility to have a more grated scale.

If it's safety significant or not it's a binary scale. And to be risk informed, we sort of need a graded scale, not just a binary scale or we want a graded scale and that could also be part of what, when any of those discussions, although I don't remember them right now.

MEMBER BROWN: Well, I'll tell you some more. Right after the high significance safety, there's another B as lower safety significance then they define safety related SSCs that is some other lower safety.

And then there's a C which is lower, I just, worst lowest safety significance so we've got high, lower and lowest. They are defined at least in the branch technical position whether those have meaning for if not there is something, there is a basis for

saying what those mean.

And there is a gradation. It's almost like the graded approach type thought process based on what Norbert just said. You can argue --

MEMBER DIMITRIJEVIC: So --

MEMBER BROWN: -- what the, where the defining lines are between those is, could be interesting. Go ahead, Vesna. I'm sorry.

MEMBER DIMITRIJEVIC: No, that's all right. I just want to say, is the, how that's defined it's not resistant which is actually risk-informed content that you approaches as they exist, you know, in that couldn't practices.

That's something new. I mean and obviously this great a preductal with something new and defined here so. I mean, you know, here the presenters are true risk-informed content of approach that those, you know, the risk-informed content that the project as defined in Reg. Guide 1174.

Or you know, this inform ranking is improving the 10-65-5069 at different than what Charlie just said.

MEMBER BROWN: Any other questions or comments? Samir? Take the spear out of your chest and you can proceed.

MR. DARBALI: Steven are you on, still on Slide 15 or are you done?

MR. ALFERINK: I have finished Slide 15. I was going to turn it back to you.

MR. DARBALI: Okay, thank you. We are now on Slide 16 to talk about Point 4. So Point 4 of SECY-22-076 maintains the intent from SRM SECY-93-07 regarding the need for independent and diverse manual control room displays and controls for the plant's critical safety functions.

These diverse displays and controls may be credited to meet Point 3 and that was part of the discussion before on the manual controls. Point 4 is essential in the Staff's ability to conclude with reasonable assurance that a proposed Digital I&C design does not adversely affect an operator's ability to manually control critical safety functions.

The Staff's position is that Digital I&C systems should not be able to take control of the facility away from the operator under all plant conditions whether they be anticipated or unanticipated plant conditions.

Point 4 is consistent with the application of existing regulatory requirements for the independence that are incorporated into the regulation.

Point 4 already incorporates an explicit element of risk informing as it is only applicable to critical safety functions and does not require the diverse displays and manual controls to be safety grade or hard wired.

MEMBER BROWN: What's GDC 22 again? I forgot. Does anybody remember?

MEMBER MARCH-LEUBA: You're very far away from the microphone. It's hard to hear?

MEMBER BROWN: Oh, what's GDC 22?

MR. DARBALI: Remember you got that on top of your head right now?

MR. CARTE: Yes, reliability and testability I think.

MEMBER BROWN: And --

MR. CARTE: It has that statement about design technique such as diversity so you'd be used to the extent practical.

MEMBER BROWN: Okay.

MR. CARTE: To prevent loss of tech disfunction. That's the last sentence of the --

MEMBER BROWN: Okay, 50.55a(h) has got 603-1991 in it. Right?

MR. CARTE: Yes.

MEMBER BROWN: If I remember correctly.

That's the architecture is in the principles of design, et cetera. Okay, all right. Thank you.

MR. DARBALI: And now on Slide 18, so this graphic is intended to depict the risk-informed scope of Point 4 which is shown in the green shaded area. As you can see, Point 4 is only applicable to those critical safety functions performed by the digital system.

Point 4 is not applicable to all of the critical safety functions performed by the system, only those that are those critical safety functions performed by the system and it's all, Point 4 is also not applicable to critical safety functions that are not performed by the Digital I&C system.

In other words, critical safety functions aren't performed by various systems in the plants where only focusing on the scope of the modification. Again, we recognize that the critical safety functions listed in the SECY and BTP-719 may not be the appropriate set for all reactor designs.

And the SECY does provide for the use of existing regulatory tools like extensions and alternatives to accommodate the signs with different critical safety functions, any of the Staff unconscious or reactor design where the policy would not be

applicable, the Staff would engage the Commission as appropriate.

MEMBER MARCH-LEUBA: This is Jose, can you give me an example so I can think of it of a safety function where it will be good in your mind of the digital system locks the operator and lesson lender breakthrough in at all which is what No. 34 is. Right?

I mean, is a classic idea of you flying a plane and the auto pilot is fighting you, your joystick. Pulling up his point. Give me a safety function with locking my joystick would be reasonable.

MR. DARBALI: And we can't think of one.

MEMBER MARCH-LEUBA: Me neither.

MR. DARBALI: Right, so and maybe that left side of the box that says plant safety, you know, let me --

MR. MARCH-LEUBA: It should, the left side of the box should be an empty set.

MR. DARBALI: Right.

MR. MARCH-LEUBA: Even if no set.

MR. DARBALI: Right. A safety system is going to have various levels, it's going to perform a lot of functions and some are considered critical safety functions.

Those are the ones like you said, you don't

want your pilot to not have control of the plane. So those are the ones that we are focusing on. If the safety system performs other functions that because they can be mitigated in some other way or they have some, there are some preventive measures or the risk of that function is not considered risk significant than they would fall outside of those critical safety functions.

MEMBER MARCH-LEUBA: Yes, let me give you an example to focus many, if I'm driving one of these modern cars and a cab breaks in front of me very suddenly, that should release the brakes for me which is good.

I mean it's a, the whole system takes control of my action, but if I want to brake more, I can. I can and then the moment you touch the brake, the safety function disconnects itself and then you can release the brake.

You just have to skid into -- anyway, I think I said enough. I don't see the point of having this caveat. I would, I don't see it would be applied anywhere.

MR. DARBALI: Which caveat specifically?

MEMBER MARCH-LEUBA: The plant safety functions not counting where the control system can

take control from the operator and won't allow the operator override it.

MR. DARBALI: But is that a comment specific to the language in Point 4?

MEMBER MARCH-LEUBA: No, it's a comment on your slide.

MR. DARBALI: Okay, understood. It may not have been clear. Okay. Now on Slide 19. So Point 4 has not been an amphetamine to modern digital control room designs.

For example, all recently approved designs meet this Point 4 including the new scale control room design and the AP-1000 control room design used at both units 3 and 4.

Licensees that want to use risk information to reduce the requirements for manual controls can request an exception or an alternative and the Staff would inform the Commission before approving or denying such exceptions and alternative.

The Staff has had several meetings with stakeholders to better understand their perspectives and believes that industry's concerns can be adequately addressed in implementing guidance.

MEMBER BROWN: What does that mean? Go so high tech that it would blow your brains out? Touch

screens, all kinds of good stuff like that, eliminate all the switches, nothing but glass and -- it seems to me you got to be careful about how principles might be bypassed when we go these paths. That's all. It's the --

MR. DARBALI: Understood. And that's why we, you know, that's the value we see in Point 4.

MEMBER BROWN: Let me ask you one other associated question then. We've got Reg Guide 1.152 is coming in for a review by the subcommittee on the 17th of November.

And that's been extensively revised, but it seems to me that is another one of the main players relative to how you address what's being allowed by the second.

Is that, I'm just about to start on that so I do know it's been revised extensively along with the ATP-7-19. Somehow this has got to be integrated with the stuff we've got out there right now.

And it's a little bit difficult to see. Are we going to have to revise 7-19 and ISG-6?

MR. DARBALI: So --

MEMBER BROWN: And then that design specific review standards, et cetera, et cetera, et cetera to be in compliance or to respect or to reflect

what's in this SECY?

MR. DARBALI: Right, so ISP-06 and the design specific review standards point to currently they point to SRM-SECY-93-087.

MEMBER BROWN: Yes.

MR. DARBALI: And so at least for ISO-06 its final resting place should be part, formalized as part of the SRP so it eventually will not be an ISG so and as we are performing a licensing reviews, we are gathering lessons learned.

So eventually the contents of ISG-06 will be updated and whatever comes out of the Commission on this SECY and the implementing guidance would be reflected in our licensing review guidance. Does that --

MEMBER BROWN: Any other questions on this slide?

MEMBER KIRCHNER: Yes, Charlie, this Walt.

MEMBER BROWN: Go ahead, Walt.

MEMBER KIRCHNER: Could you give us some examples of what industry concerns might be? Are you talking about new advanced non-LWR designs where the BTP critical safety functions might be somewhat different or what's the industry concern that we --

MR. DARBALI: So from our stakeholder

engagements, we've received feedback from the industry. On the critical safety functions, I don't believe that is a major aspect of Point 4.

I believe what industry is trying to say is that if you're not crediting the manual actions in Point 3, then you shouldn't be looking at Point 4. What we've tried to explain is that Points 1 through 3 are intended to address the CCF.

How does the facility cope with the CCF. So Point 1 and 2 you do your D3 Assessment. In Point 3, you identify ways of addressing that postulated CCF.

Point 4 has a different safety concern which is to allow the operators to be able to perform the manual actions. And that's why it requires the displacing controls and many of the controls to be diverse from your system so that your CCF doesn't take out, your CCF doesn't take out both your system and your manual controls for those critical safety functions.

I believe industry's argument is that the quality of new digital systems is very high and the reliability is very high where you would not consider, you would not even consider that CCF and you would not need to have the need for the operator to have manual controls.

Also, I believe the future that some in industry are envisioning is a, what we call a glass control room. Everything is a flat panel display run by the same software and so that would not need Point 4.

And so we think that you can have a control room made out of flat panel displays, but you're going to have to run those manual (audio interference) diverse software for those controls or whether they be hardwired.

But they have to be, our position is they have to be diverse from your safety system.

MEMBER KIRCHNER: Okay, that's good. What you're saying, it doesn't leap out of the language to me.

MR. DARBALI: Okay.

MEMBER KIRCHNER: I'm very encouraged by what you just said, but I can imagine certainly with some of the new advanced designs, their thinking is probably that scenario you just played out where it's entirely glass.

It would be important to, it goes back to Charlie's point about architecture. Make it very clear that you can go that route, but you would actually have two different systems in the control room and they

wouldn't share any comments off of their site to achieve those critical safety functions. And --

MEMBER HALNON: This is Greg Halnon.

MEMBER KIRCHNER: -- and that would be --

MEMBER HALNON: You wouldn't necessarily be in the control room if you had adequate time to get to a remote location and actuate them. Correct?

MEMBER KIRCHNER: Well yes, that's probably predates Digital I&C. That's my --

MEMBER HALNON: Well --

MEMBER KIRCHNER: -- experience where you had a, yes, a separate analog system for the shutdown function.

MEMBER HALNON: Well I'm just saying you had to actuate a pump, you can go locally and turn the pump on if you had adequate time to meet that we talked about earlier as far as manual actuation.

Also, there's some requirements prior protection that have diverse ability to operate outside the control room as well. So there's some synergies there that will probably be built on.

MEMBER KIRCHNER: My point, Charlie is that what was just said by the Staff makes eminent good sense, but it doesn't leap out of the language to me. But --

MEMBER BROWN: It's varied.

MEMBER KIRCHNER: -- because, yes.

MEMBER BROWN: The whole thing when you're running down that path, they have to have the ability to say no. And that's --

MEMBER KIRCHNER: Yes.

MEMBER BROWN: -- my biggest concern for all of this when you introduce this risk-informed approach to how you, you know, diverse and nondiverse or whatever.

You now, you have to prove the opposite. They can come in and say this is what we want to do and it's so good that we'll never have a problem. And then you have to prove the negative for the Staff to, I mean you could apply that to the entire application of risk-informed approaches or the entire parts of the plant which they're already going and doing.

So now this is one of the logical extensions that they're nibbling down to the grass roots and now it's down to the instrumentation control systems where people are turning switches and doing various things like that as opposed to the more of the other.

I'm still trying to figure out how risk informed the operation of an amplifier. You know, it either it trips or it doesn't trip. You know, if it's

a vice saver.

It, you risk inform the parts, but you don't buy such good parts and make them out of cruddy parts. It's an interest conundrum to have to deal with.

I think as a Committee, this is just an opinion that it would be difficult for us to walk through seeing something that didn't have adequate manual backup regardless of the circumstances under which it was being said to be needed.

That's just kind of a hard spot and from personal experience, I can, and very personal experience. If it hadn't been for manual backup, it would have been some severe consequences.

MEMBER HALNON: This is Greg. A question again back I guess, Samir. You mentioned that the digital systems are hard quality and, you know, the industry's saying that the uncommon causes shouldn't even have to be considered.

Doesn't that get flushed out in the D3 assessment early on to where you wouldn't have to consider them if the quality and frequency and, you know, probability of these things having a common cause failure is so far out there we don't have to worry about it?

MR. DARBALI: Yes, I think that's part of

what Steven was talking about. But again, the point of Points 1, 2 and 3 is exactly that. How do you cope with the loss of the safety function because of a CCF whereas the intent of Point 4 is you want to ensure that your operator has the ability to perform those manual actions and so that, and that a CCF doesn't take out those, that ability.

It's more about maintaining that function. We're not at a point yet where we feel comfortable saying, yes, you can say that your CCF is unlikely so you don't need to do any diversity for your digital system and also you don't need to do anything to ensure operators have the means to perform manual actions.

MEMBER HALNON: Okay. Do you see us ever getting there? I mean, how do we credit the better quality of electronics and digital systems? It had, if it doesn't matter, then you have to consider every CCF possible. But what is the risk-informed pieces?

MR. DARBALI: Well again, the risk-informed piece is for, again, for your Point 3 which includes critical safety functions and non-critical safety functions.

That's where you get the advantage of the risk-informed approaches. And you know, even for critical safety functions licensees can determine how

they want to meet Point 3.

But for those critical safety functions, Point 4 needs to ensure that those diverse, that those controls and displays are independent and diverse. So I agree, you know, when you think about it, you know, where do you get that benefit?

It's more likely on those functions performed on the system that are not critical safety functions.

MEMBER HALNON: Okay, thanks.

MR. BENNER: Even more, those functions, you can use the risk information to not need adapts diverse actuation systems.

MR. DARBALI: Right.

MR. BENNER: So you know there are elements of where the risk informing plays out, but I think it does go back to for these functions deemed to be the most critical safety functions the Staff's current position is that a CCF shouldn't lock the ability of the manual -- of the operators to take manual control of those actions.

Now for a single failure. Right? The code, the standards do require, you know, the manual capability. But that manual capability that can't be, shouldn't be able to be taken out by a single failure.

But it could be taken out by a common cause failure and that's why the, you know, the policy and the standards were in concert with one another.

MR. DARBALI: Thank you, Eric.

MEMBER BROWN: The complications with CCFs software is wide range. This software that's been software based systems that we've seen has lots and lots and lots and lots of the compliance code for one.

I mean you're talking hundreds of thousands of lines of code. And they are interrupt driven and the interrupts are there to do things that the vendor that designs the software he's trying to accomplish to approve something is okay or not okay as it goes through.

If you're trying to execute a safety function and it all of a sudden gets interrupted, that's a problem. If the interrupt doesn't come back ask them. If it doesn't, you know, go back to where it was, that's a problem.

And it gets very, very complicated to prove that without having, you try to compensate for that by, you know, typically due to corrupt data of some kind that stops and wants to stop something.

You have a synchronous performance so that none of the channels are operating in the same sync.

You have different detectors for everything so it's the same data that might be corrupt doesn't get to all of them because it's just sensors never ever read the same thing for all of them.

There is a lot of ways you can try to justify that, but you can't prove any of it. But there's just, they're feel goods that makes your stomach not turn over.

Non-interrupt driven systems are more predictable. That's where you process everything in a straight line. You never deviate and then you come back and start over again with a new set of data.

That's for each process, for each channel. These systems we've seen are not like that. The FPGA ones are a little bit closer. They're like an analog computer. You reprogram it and it's there.

You can have it individual keys fail inside, but it's unlikely to have it fail in the other one. And I would buy in on that. I don't know whether I'm right or wrong, but I would buy in on that. That's, we've accepted that.

So there's a lot of stuff that goes into trying to figure out what is a CCF in a computer-based system. So that's my speech for this part. Never pass up an opportunity.

MR. CARTE: Norbert Carte, I&C. So there's something very interesting in your speech, Charlie. So what we're really talking about is --

MEMBER BROWN: You going to tell me I'm wrong?

MR. CARTE: No. I'm going to tell you you're right. What we're really taking about is reliability of the I&C system. And a lot of these peripheral discussions have been about the adequacy of the control room design.

So these criteria aren't really a back door or control room design requirements. And they're not necessary and sufficient for control room design. What we're really aiming for is the reliability of the I&C equipment and for the points you mentioned it's in some cases it may be possible to show that your manual controls don't need to be independent or diverse.

But in reality, it's more efficient and effective to have simple independent diverse manual controls. Although we allow this policy allows some flexibility, but this is more about equipment reliability.

The equipment being able to perform a safety function when needed rather than on appropriate criteria for a control room design. Because obviously

this isn't enough for a control room design.

And you have to think balance what the non-safety system does and what the safety system does and it's a control systems design problem, control room design problem not an I&C equipment design problem.

We just want to make sure the equipment is reliable and that's what Point 4 is about. And it's not about the control room design.

MEMBER BROWN: Yes, Norbert, but also the architecture and the backup manuals all contribute to that reliability. That's a fundamental piece of that control room design for liability.

That's in my mind. Any other comments from the Members? You want to go on to the next slide whichever one that is, 20?

MR. DARBALI: Yes, so Slide 20 are the key messages that we presented back on Slide 6 so I won't repeat them here. And Slide 21 is our next steps. If the Commission approves the recommended expanded policy our next steps are to update the existing implementation guidance.

BTP-7-019 is one of the guidance documents we're considering for updating. And also to continue to engage stakeholders and the pubic to seek comments on our implementation.

MEMBER BROWN: Why not 1.52 and 1.62, I think it's, did I get that other number right? I've forgotten what 62 is.

MR. CARTE: Yes, it's 1.152 and 1.62.

MEMBER BROWN: Yes, those are the computer, kind of the computer based Reg Guides.

MR. CARTE: 1.62 is the manual controls Reg Guide.

MEMBER BROWN: Yes, okay, got it. All right, thank you. And 1.152 is the general application of computer systems.

MR. CARTE: It's design criteria to augment and supplement 603.

MEMBER BROWN: Yes. Which we're going to work on some more. Okay, so if you go forward with 1.152 and with this current revision you're working on, you're going to have to do that again if this thing gets accepted by the Commission. Is that correct? So you're going to do it twice?

MR. DARBALI: Well --

MEMBER BROWN: I'm asking you, my question is why are you doing 1.152 before you know where this Commission's going to do, what they're going to do with this.

MR. NGUYEN: Yes, Charlie. This is Khoi

Nguyen. I'm the one who prepared Reg Guide 1.052 which is the deterministic guidance.

MEMBER BROWN: Yes.

MR. NGUYEN: And it's for common cause failure we clarify the endorsement with the reference to BTP-7-19. So I don't think 1.52 necessary to revise to reflect the new SECY paper, but BTP-7-19 should be.

MEMBER BROWN: Yes, I noticed that. I took a quick look at it and I noticed it was, some references. There were some other good stuff in it. There was some other not so good stuff in it. But we'll deal with that on the 17th.

MR. NGUYEN: Thank you.

MEMBER BROWN: All right. Any other comments from the Committee Members?

MR. DARBALI: That's our presentation so thank you for the comments and are open to answer any other questions.

MEMBER BROWN: No more questions, Joy, I'll turn it back over to you.

CHAIRMAN REMPE: I think we need to ask if any members of the public --

MEMBER BROWN: Oh.

CHAIRMAN REMPE: -- would like to make a comment.

MEMBER BROWN: Well that's a good point. Thank you. We finished our part of the meeting. Is there anybody, members of the public who would like to make some comments on this presentation?

MR. DARBALI: I see Alan --

CHAIRMAN REMPE: I see a hand -- whoever's got their hand up, you're welcome to unmute themselves and speak. Alan Campbell.

MR. CAMPBELL: Hi, good afternoon this is Alan Campbell with NEI. So I'll keep my comments brief here. But NEI would like to thank the NRC for hearing the industry needs to allow risk insights to be applied to Digital I&C design and the licensing activities as it's been applied in other technical areas.

We truly appreciate the engagement and the urgency in which the NRC Staff has responded. NEI and our members believe that Points 1 through 3 provide the policy Staff change needed to allow risk insights to be considered.

And we're looking forward to future implementation guidance that further clarifies the application of these principles. We also believe that Point 4 remains overly prescriptive both in the scope and location requirements.

We fully agree with the Staff that manual

actions credited with responding to a CCF concurrent with a design basis event should not be subject to the same CCF.

However, to maintain the principle of simplicity and design, the scope of those manual actions should be driven by plant or application specific analysis not prescriptive policy requirements.

We believe the results of the CCF coping and D3 analyses provide reasonable assurance of adequate protection while responding to this beyond design basis event.

Additionally, existing human factors engineering approaches described in SRP Chapter 18 Appendix Alpha to that SRP Chapter and the associated New Regs provide adequate guidance for specific features including the location requirements for these credited manual actions.

So again, thank you to both the NRC Staff and the ACRS full Committee and we ask that the ACRS full Committee consider these requirements while deliberating your action. Thank you.

CHAIRMAN REMPE: Thank you.

MEMBER BROWN: Is there anybody else that would like to make a comment? Excuse me. Is there anybody else on that would like to make a comment?

Hearing no response, back to you, Joy, now.

CHAIRMAN REMPE: Thank you.

MEMBER BROWN: Thank you for reminding me.

CHAIRMAN REMPE: No problem. Okay, I know you have a letter that you'd like to read in and so at this point, I'd like the Court Reporter, I'd like to go off the record and invite the Court Reporter to return at 3:45 p.m. East Coast Time and then, thank you.

(Whereupon, the above-entitled matter went off the record at 2:26 p.m. and resumed at 3:45 p.m.)

CHAIRMAN REMPE: Okay, it's 3:45 p.m. and we're back in session. And at this time, I'd like to ask (audio interference).

MEMBER MARCH-LEUBA: Thank you, Ms. Chairman. We're going to be talking about Reg Guide 1.82 which deals with sources of water for SECS and other safety functions after LOCAs.

And at this point, I'd like to give the floor to the Staff. I believe Jim, you're going to make a presentation, an introduction?

MR. STRECKEL: Yes. Can you hear us okay?

MEMBER MARCH-LEUBA: Yes, we can.

MR. STRECKEL: Okay, good. Yes, I'll just

do a real brief introduction and turn it over to the technical staff to do the body of the presentation. So let me introduce myself. My name is Jim Steckel.

I'm a Program Manager in the office of Research, Division of Engineering and our branch does all of the work or of the PM work, the project management work on the regulatory guide system.

I'm also here with Ahsan Salman, he's the Senior Nuclear Engineer in NRR Division of Safety Systems. He'll be talking later on Appendix B of this Reg Guide Revision and also Steve Smith, Senior Plant Systems Engineer.

He is also in NRR's Division of Safety Systems. Today we'll present in summary fashion the main changes to Rev 5 of Reg Guide 1.82. These updates will be discussed by the Technical leads and will include the following: a) GSI-191, this issue constitutes the main body of the Reg Guide and Appendix A.

And included in this will be Reg Guide 1.82 Rev 5 status with respect to GSI-191 and some brief points about FLEX equipment strategies and defense in depth.

In Item B, a discussion will be presented on the use of Containment Accident Pressure, CAP, in

determining the net positive suction head margin for ECCS pumps and containment heat removal pumps.

This is the main purpose for Appendix B. I would now like to allow the presentation to continue by Steve Smith.

MR. SMITH: All right, thanks, Jim. We're going to go ahead and we'll turn our camera off now that you've gotten a chance to get a look at us and we will start presenting our slides. We have picked the right ones. Yes.

MR. STECKEL: Yes, you did.

MR. SMITH: Okay, so this is just our title slide. I'm going to move along to Slide 2 which just, it tells the major change that we made to the Reg Guide.

With respect to GSI-191, what we did was we added -- the biggest change that we added in vessel guidance and some other references that had been developed since the last revision.

The other major change to the Reg Guide is the addition of Appendix B for the use of CAP and NPSH calculations and I believe that ACRS is familiar with both of these topics.

They've been around for quite a while. I'm going to move along to Slide 3. And this slide lists the major changes made in Rev 5 that are related

to GSI-191.

If you have questions on any of these, just stop, I'm not going to go through them. We went through them in more detail in the subcommittee meeting. Let me know if you have questions on these or --

MEMBER MARCH-LEUBA: Yes, this is Jose just for the record. All you're doing, we have an echo.

MR. SMITH: Mine's off.

(Audio interference.)

MEMBER MARCH-LEUBA: How do you want to do this?

CHAIRMAN REMPE: Let's try again. I don't hear an echo. Can you hear us?

MEMBER MARCH-LEUBA: We muted everybody so you have to mute yourself.

MALE PARTICIPANT: Yes, we can hear you.

DR. SCHULTZ: I can hear you now on the line.

MEMBER MARCH-LEUBA: Okay, sorry about that. Technical difficulties. So the question is, the updates to the Guide are all there. Are they all consistent with the GSI-191 resolution of the issue that we have reviewed it for? Just for the record.

MR. SMITH: Yes, they're all consistent with what has been reviewed. Oh, I'm sorry. Yes, this

is Steve Smith again with the Staff and yes, all the changes we made to the Reg Guide in Rev 5 are consistent with what we have presented to the ACRS in the past.

MEMBER MARCH-LEUBA: Thank you. Keep going.

MR. SMITH: Okay, sorry about that. All right, so I'm going to move on to Slide 4. And this is the status of the Reg Guide with respect to DSI-191.

We don't anticipate any significant changes to the Reg Guide in the future for GSI-191 issue where things can come up that are not to assume, but at this point, we believe that Rev 5 is and that some of the information that is in Rev 5 is a complete guidance document for this topic.

Now we still have the tendency of R50.46(c) Rulemaking which is currently with the Commission which could have us add or remove some risk informed guidance that is currently referenced in this.

It will either be finalized or maybe it will be removed. We're not really sure. We're waiting for the Commission to tell us what they want to do with the 50.46C rule.

Slide 5 has a lot more information on it just because this is a little bit more complicated. I don't want to spend -- even though there's a lot of

worries here, I don't want to spend a lot of time on this slide so because it's not related directly to the revision.

But if you're interested or have got some interest in the FLEX equipment and its ability to provide defense and depth. So this slide talks a little bit about the defense and depth that may be available from FLEX.

And these for the issues that we're talking about today which would be a loss of MPSH margin either due to a CAP issue or due to a strainer clogging issue.

The one thing to note is the FLEX strategies were not developed or reviewed by the NRC for response populated accidents like the ones that we are talking about when we talk about drainer clogging or CAP.

They were developed for basically wide, large scale, you know, natural disaster type things so there's some differences between those type of events and what we are actually talking about in the pro-temp gap and these cooling issues.

So there are some differences between BWR and PWR FLEX equipment the way it's installed. PWRs have high volume direct RCS injection points that are either they're configured, they're not hooked up, but they can be readily connected to the pumps and can pump

directly into the RCS.

PWR only had low volume direct RCS injection and basically those are to make up either for a shutdown condition or if you had a say a RCP seal leak or something like that. That's what those are designed for the PWRs.

Now the PWRs may be able to reconfigure the high volume steam generator pump will eject to the RTS, but that's not something that's been pre-planned and pre-thought out.

It appears that the PWR FLEX strategies are more even applied than PWRs for these scenarios. The PWRs would take longer for I guess a high-volume concept up to the RTS if they could do it at all.

So that's the bottom line on the potential defense and depth that's been provided by the FLEX equipment. I'll just pause there and see if there's any questions that are on that slide.

MEMBER MARCH-LEUBA: This is Jose. Yes. Just a comment that I'm the one that asked you to include this slide on the presentation. Because since there are Reg Guide 182 deals with availability of water sources during this extended event, obviously FLEX is one of those water resources.

And it's good to know that BWRs will

probably improve to the significantly and PWRs that have been there with it or without it so. Thank you for presenting that.

MR. SMITH: Yes, I agree. I agree that what you said sounds correct to me. Okay. Then starting with the next slide, Ahsan is going to discuss the use of CAP for the MPSA margin calculations. Go ahead.

MR. SALMAN: Okay, thank you. This is Ahsan Salman. I'm a Senior Nuclear Engineer in the Nuclear Performance Systems Branch and the Regional Safety Systems.

I'll talk about the use of containment accident pressure in determining the NPS stretch of the containment here to move pumps and the ECCS pumps. There's this slide shows some background on the use of CAP.

This issue was highlighted about 15 years ago when NRC received EP applications from Browns Ferry and then from Monticello. Both were using CAP in their NPSH analysis.

At that time, the only published guidance was Reg Guide 1.1 which stated that CAP should not be used for NPS as how are some licensees were using CAP and NRC had approved its use.

The EPR reviews of the Browns Ferry and the Monticello were discontinued and put on hold. The Staff prepared a white paper documenting its position to ACRS.

Also, the BWR Owners Group submitted a topical report providing a standard approach for requesting user CAP. In return ACRS provided recommendations in a letter to EDO.

And the main one of them which were accepted also are mentioned in here, the licensee should use guidance in Reg Guide 1.82 so that's why the Reg Guide 1.1 was merged into Reg Guide 1.82.

And then operator actions to control CAPs should be reliable. Risks should be small. Support Staff for the SERS meant of problem with NPSHa the, variable NPSH less than NPSHr.

And then the SERS agreed with the owners group, BWR owners group tested the statistical calculations to calculate margin. And the last one which was also included in this Reg Guide was the margin between the available NPSH.

And the required NPSH should consider uncertainty in that the required NPSH. So then the Staff SECY paper was issued. In this SECY paper there was a Staff position for the use of CAP deterministic

analysis is used.

And the recommendation from ACRS was to use deterministic analysis and a plant specific PRA, but when it went to the Commission, the vote for the Commission was an Option 1 which was to just use a deterministic analysis, conservative analysis and include all those SER recommendations that I just listed.

MEMBER MARCH-LEUBA: This is Jose. Let me summarize what you said in my own words. And you tell me if it's correct.

MR. SALMAN: Okay.

MEMBER MARCH-LEUBA: In lesson C the wants to determine whether there is an ECCS pumps have sufficient operating margin, let's call it MPSH.

MR. SALMAN: Yes.

MEMBER MARCH-LEUBA: Will perform a dynamic calculation of the locker or what their event will concern with.

MR. SALMAN: Yes.

MEMBER MARCH-LEUBA: And as a function of time after the accident, you will calculate the pressures of the containment is at --

MR. SALMAN: Okay.

MEMBER MARCH-LEUBA: -- foregoing the

accident as it's supposed to develop or if you set those minutes, hours after the accident.

MR. SALMAN: Yes.

MEMBER MARCH-LEUBA: And it will impose conservative bounding numbers for the assumptions which are described in Appendix B of the Regulatory Guide --

MR. SALMAN: Yes.

MEMBER MARCH-LEUBA: -- so that when we are at the end calculate what is the pressures high containment as function of time with a ten minute that pressure is higher than that required to have the pumps operating.

MR. SALMAN: Right.

MEMBER MARCH-LEUBA: Is that correct?

MR. SALMAN: That is correct. And also, calculate the suppression pool of the sump water temperature conservative analysis for that so that the NPSH available is conservatively calculated based on the available, based on the temperature of the pool --

MEMBER MARCH-LEUBA: All right.

MR. SALMAN: -- because one of the terms in NPSH and negative term, the NPSH is the vapor pressure at the pool temperature.

MEMBER MARCH-LEUBA: Yes, and for my point of view, ACRS' main concern and which we still have differences, is that they should be plant specific risk analysis performed that this containment operation has been performed every percent reality.

I mean, you have to add additional failures like somebody alliance about in the incorrect position or containment had leakages before you had the accident and therefore you cannot hold the pressure.

MR. SALMAN: Yes.

MEMBER MARCH-LEUBA: Our Members agreement with the Staff, ASRC' agreement with the Staff was that this is likely to be very plant specific dependent and it would be wise to have a plant specific risk analysis.

MR. SALMAN: Exactly. Yes, that was only difference the, all the deterministic analysis calculation methods were incorporated in this Reg Guide.

And the only difference was the PRA that when a licensee whose CAP for an EPU or some other purpose they should present a plant specific PRA for that.

MEMEBER MARCH-LEUBA: Yes, and the ACRS position also was that and which you have accepted and

implemented into the Reg Guide is that a licensee should look first for how are changes that we give you the NPSH margin before taking credit for CAP.

MR. SALMAN: Yes, the changes that I have listed here, one of the major changes is the NPSH required should consider the uncertainty because the required NPSH is calculated or is determined by testing at the plant vendor and the pump vendor I mean.

And the differences between the test conditions and the plant conditions there should be an uncertainty so that is, that makes a required MPS at higher than the 3 percent --

MEMBER MARCH-LEUBA: Right.

MR. SALMAN: -- factory estimate so --

MEMBER MARCH-LEUBA: Yes.

MR. SALMAN: -- that is another margin uncertainty considered in this Reg Guide.

MEMBER MARCH-LEUBA: Yes, but my point is that some of the EPU applicants that wanted to use CAP credit ended up making some minor reasonable modifications to the plant.

Some did heaters changer, some did alignment of pumps, so that after those modifications, they did not require a CAP. So what --

MR. SALMAN: That -- what I think the Reg

Guides says is the Staff will either reviews a CAP application should consider that there are no reasonable, the licensee has performed a sufficient scope analysis that no original modifications can be implemented.

MR. SALMAN: Yes, yes. The one, this is one of the summary that if the plant, first of all, the plant should consider modification. If the modification is impractical, then they can apply reusing this amount, this much amount of a CAP. And that is included in the Guidance and the --

MEMBER MARCH-LEUBA: Excellent.

MR. SALMAN: And the last slide of this presentation, there's a summary and that includes that, but the plants, the EPU that were discontinued at that time were Monticello and Browns Ferry.

And both of them they were using CAP but without all these requirements that are now in the Reg Guide. So finally it ended up that one of the plants I remember was Peach Bottom.

They did hardware modifications, plant modification by using two heat exchangers to reduce the pool temperature, the suppression pool temperature and so that there was no CAP used.

And another plant Browns Ferry first

obligation which was I think 2005 they were using CAP, but then afterwards, the applications submitted in 2015 they did not use CAP, but they approved the performance of the heat exchangers so that the pool temperature goes down and the vapor pressure is suppressed.

MEMBER MARCH-LEUBA: Okay, thank you. You can continue.

MR. SALMAN: Okay. So I go to slide, next slide which this is stating what is the margin. The margin is calculated by the available NPSH minus the effective NPSH which the effective NPSH is the 3 percent that is a test done by the hydraulic institute standard and that includes uncertainties.

So that is one of the major changes before this Reg Guide was issued. And for special events for the BWR which is a space station blackout or Appendix R or the aqueous events, the Reg Guard allows the user the 3 percent which is without the uncertainties and use realistic inputs for the calculation of containment accident pressure in the pool temperature.

Another point here is the negative NPSH margin is acceptable if tests demonstrate that proper performance safety function and that is, that were highlighted in the previous meeting, what are the different requirements for a negative NPSH. And if

you want to go, I have to open my slide before.

MEMBER MARCH-LEUBA: No, no. We can look at a transcript of the SUCO meeting unless a member wants to ask about it.

MR. SALMAN: Yes, yes. We, I have to open the other. So anyway, the Monte Carlo analysis was recommended in the BWR owners group report to calculate the margin.

In the conservative analysis, the deterministic analysis, it will only say that heavy are doing terminist analysis, which is conservative, but the question from ACRS was always so what is the margin?

So in order to determine margin in the conservative analysis, this Monte Carlo 95-95 calculations was recommended by the ACRS also and it is included in the, in this Reg Guide that any plant who is using CAP above the vapor pressure should determine what is the margin, what, how much is, what is a conservatism in the deterministic analysis?

Another item is if the CAP up to the vapor pressure, the pool temperature can be used without Monte Carlo analysis. So that is most BWRs, there is some temperature is higher, much higher than the atmospheric.

Then so those plants, they can use CAP up to the vapor pressure of the pool temperature without any Monte Carlo analysis. And if it is more than that vapor pressure the whole temperature, then the Monte Carlo analysis and another item in this is the plant should monitor a pre-existing leak during normal operation.

This was done also by Monticello. Yes, they agreed or in the EPO application and the Staff SER it was Staff required them to monitor a pre-existing leak in the containment during operation.

MEMBER HALNON: So this is Greg. One quick question back on the safety side. The test, does it demonstrate promptly performed safety function? This kind of brings me back to a mission time type discussion that seems to be in circular motion in the industry.

Is it, is the guidance clear enough that we're not going to run into that problem of arguing about what the mission time will be for these tests that have to demonstrate a safety function for a degraded system?

MR. SALMAN: Are you, I'm sorry, are you talking about a negative margin when the --

MEMBER HALNON: Yes.

MR. SALMON: When the -- yes, there are requirements. Let me read what are the requirements. I have the subcommittee presentation here. And those requirements are important. Yes, the slide in this previous presentation with respect to the margin section --

MEMBER MARCH-LEUBA: Yes, on this issue while you look for it, if a slide is --

MR. SALMAN: Okay, use of CAP --

MEMBER MARCH-LEUBA: -- presented in the meeting, it is part of the record. Right?

(Simultaneous speaking.)

(Audio interference.)

MEMBER MARCH-LEUBA: Okay?

MR. SALMAN: Yes, that is, we have a report and safety, does the pump has a negative margin and the red light says it is acceptable if the tests are done to demonstrate the actual pump or a similar pump, will perform at for a limited time duration less than hundred hours.

Actual pump or similar model pump is tested, tested at the same speed as at the plant site and tested at actual predicted available NPSH and the test duration is for the time you're in this NPSH margin is negative.

And the flow and discharge help should be greater than that required for the safety analysis.

MEMBER MARCH-LEUBA: This is Jose, the mission time is that of or the result of the calculation, the continuing calculation that we perform to determine that CAP was needed.

So the time where the MPSH is violated is calculated, there is no argument about it.

MEMBER HALNON: Okay so the test durations for the period for negative margin is that test continued and because the pump is now a degraded state because of the potential capitation in your interpretation and during the tie?

MEMBER MARCH-LEUBA: The pool temperature finally cool down and now you recover NPSH.

MEMBER HALNON: Okay.

MEMBER MARCH-LEUBA: And I suppose it demonstrates that the pump didn't break up that much.

MEMBER HALNON: That's a generalized statement when you just said it had to be plant specific so.

MEMBER MARCH-LEUBA: No, it has to be. This completion is plant specific.

MEMBER HALNON: Okay. I just wanted to make sure we weren't going to get into a circular

discussion about mission time. It looks like you've got that covered so I'm okay with --

MR. SALMAN: Okay, so containment leakage, that's another item in this slide which the licensee should demonstrate loss of containment, integrity and loss of containment isolation cannot occur and monitor leakage during operation.

And quantifying of the NPSH margin for the DBA LOCA the calculation should use considerable debonding inputs and to demonstrate margin, they can use real estate and Monte Carlo analysis to determine the conservatism.

And require NPSH should include uncertain. So that's for DBA LOCA, but for special events, the NPSHr may use without uncertainty. The next slide is a guidance summary which I talk most of these points and already talk, but if you want to go through it again, I'm willing to, I'll be willing to.

CHAIRMAN REMPE: This is Joy and I do have a question and I apologize, I had communication issues during the subcommittee meeting and I tried to hone in on this, but basically on the loss of containment, integrity venting for example shouldn't occur during CAP use.

And if I look at the guidance on Page 83

out of 88, it does talk about the fact you shouldn't allow them to be venting and using CAP at the same time.

But I'm thinking again about what happened after Fukushima and so if an applicant comes in with an LAR and they are trying to say, okay, we can use CAP and they try and justify it. Are you guys going to try and implement this guidance?

Are you going to say, let us see your severe accident management guidance so we know that you're going to check and see that you don't need CAP before you go to early venting?

Because I mean, that's I would want to see that if I were checking into it and how will the regulators know how to check? Because the severe accident guidance isn't really required to review, you know, to be submitted as part of this. I mean, how are you going to implement this?

MR. SALMAN: Well when a licensee submits an application for the use of CAP, that application should be consistent. The analysis for the usage of CAP should be consistent with the procedure they're using for the DBA LOCA.

And that's how this guidance is written. This does not consider any severe accident procedure in this Reg Guide.

CHAIRMAN REMPE: Okay, but then during a real event, where they have a long-term station blackout and maybe they tried to use CAP during that event and things went south, shouldn't somebody be checking to make sure that during the severe accident that they basically don't need the CAP anymore to run the pumps before they vent?

And, I mean, how will that interface be taken care of is what I'm asking? And it seems like somebody ought to be checking that.

MEMBER KIRCHNER: By definition, if the pumps function -- I shouldn't answer for the Staff. My logic would be the following: if you're in design basis accident space after 15, you do the dynamic analysis to ensure you have sufficient and net positive substantive head on those cooling pumps.

If they function, then you shouldn't have a severe accident. If you lose CAP and you lose the functioning of the pumps, then you're in trouble obviously and your gone beyond the design basis accident.

So I think the Staff guidance is, revolves around a design basis event, not a severe accident.

CHAIRMAN REMPE: So --

MEMBER KIRCHNER: Once you get into severe

accident space then the correct --

CHAIRMAN REMPE: So let's think of --

MEMBER KIRCHNER: -- both of those other things, but for purposes of analyzing design basis accidents, the presumption is in my mind that if you have sufficient capacity and net positive suction CAD for the pumps, then you're going to deliver the ECCS cooling and containment cooling necessary to prevent the severe accident.

CHAIRMAN REMPE: So --

MEMBER KIRCHNER: So you haven't moved on to Chapter 19 yet.

CHAIRMAN REMPE: Okay, so during Fukushima, --

MEMBER KIRCHNER: Well that's --

CHAIRMAN REMPE: -- for example, they didn't know how high the water was in the core. They didn't know it was a severe accident. And when I tried to bring this up and I had communication issues during the subcommittee meeting, Dennis tried to hone in on it by saying the operators don't have a little gauge in the control room saying I'm in a design basis event versus --

MEMBER KIRCHNER: Okay.

CHAIRMAN REMPE: -- a severe accident.

And so if I were wanting to be very --

(Simultaneous speaking.)

CHAIRMAN REMPE: You'd hope so.

MEMBER KIRCHNER: -- in trouble.

CHAIRMAN REMPE: Yes, but I mean basically there were some, an intended venting due to expansion of the seals on the PCV and things so again temperatures and pressures are dictating when people start to think about we need to start doing early venting because they don't want to have a problem.

But I, what I'm back to is if I wanted to be thorough, I might say, this means I need to think about what's in the severe accident management guidance to make sure that this will not occur.

And that was actually in one of our letters about GSI-191. In the past we said, well no, I'm trying to remember. Maybe it was one of the post-Fukushima letters I guess.

They said, you know, this seems okay, but we need to think, it was in one of our prior letters where we said, think about, maybe it was the Monticello letter when we approved their EPU that we said, you know, you may need to think about this --

MEMBER MARCH-LEUBA: I was going to --

CHAIRMAN REMPE: -- what can happen in

severe accidents. And I can pull up that letter. But that's why I think it's important to kind of, and I know it's in your draft letter to think about this.

MEMBER MARCH-LEUBA: Yes. I was going to give you a hint, a preview that the letter makes that accommodation.

CHAIRMAN REMPE: Yes, it's --

MEMBER MARCH-LEUBA: And I think it's wise to do.

CHAIRMAN REMPE: Yes, it --

MEMBER MARCH-LEUBA: And the Staff should look at it during the review, but as one more checkmark to do, nothing showstopper.

CHAIRMAN REMPE: Because they don't usually look at the severe accident management guidance and that type of thing.

MEMBER MARCH-LEUBA: Yes.

CHAIRMAN REMPE: Okay, but anyway, I just think I've homed in on my point of what I was trying to make and I had some communication issues the last subcommittee meeting.

MR. SALMAN: One of the requirements in this Reg Guide is the loss of containment integrity. And but then in parenthesis it says venting should not occur during CAP.

So if a licensee is presenting an analysis for the use of CAP and they have this venting in the analysis and then they are asking to use CAP, then the analysis should cover that.

CHAIRMAN REMPE: So again, I'm looking at your guidance on Page 83 where you have that section and it's focused on design basis events. And --

MR. SALMAN: Right.

CHAIRMAN REMPE: -- what I'm saying is that the world isn't so cut and dried and so I think that means going into the severe accident --

MR. SALMAN: Right.

CHAIRMAN REMPE: It's a process too.

MR. SALMAN: So if you've got --

CHAIRMAN REMPE: Sometimes people don't have a fine or they tend to segregate this and they think only one way because that's what they're supposed to think on that topic.

MR. SALMAN: So the CAP analysis that they present to us if it includes venting, then the analysis should consider that venting and then calculation of CAP and the pressure and the containment.

CHAIRMAN REMPE: Okay, but then I think also that it would behoove the Staff to think about severe accident guidance or make the applicant

demonstrate that this won't cause problems in severe accidents is all --

MR. SALMAN: Okay.

CHAIRMAN REMPE: -- I'm trying to say.

MR. SALMAN: Yes, the procedure should be then consistent with analysis.

CHAIRMAN REMPE: And see --

MEMBER MARCH-LEUBA: That is an excellent phrase. You should frame it and put it in your wall. I believe you finish your presentation, Ahsan?

MR. SALMAN: Yes, that is all. If there is any question on the guidance summary which I mentioned before all these points, please let me know so we can answer the questions.

MEMBER MARCH-LEUBA: Members, you have any more questions for the Staff? Hearing none, any members of the public that would like to make a comment? Unmute yourself and do so right now.

We don't have any comments from the members. Chair, you are --

CHAIRMAN REMPE: Okay.

MEMBER MARCH-LEUBA: -- it's your microphone.

CHAIRMAN REMPE: Okay. Thank you very much. Thanks to the Staff. At this point, it's not

been going that long so how about we just take a few minutes until Sandra can come back and bring up your letter and let's not have an official break or you want to have a ten-minute break?

MEMBER MARCH-LEUBA: I don't need it.

CHAIRMAN REMPE: Okay, so as soon as we can, we'll resume with letter writing and then --

MEMBER MARCH-LEUBA: Yes, and then --

CHAIRMAN REMPE: -- stay tuned all of you.

MEMBER MARCH-LEUBA: -- we're off the record and what time?

CHAIRMAN REMPE: Oh, yes. Thank you very much. I'd like to also ask to go off the record and ask the Court Reporter to come back tomorrow morning at 8:30 a.m. Okay? Whether it's you or someone else from your organization. Okay. Yes, thank you very much.

(Whereupon, the above-entitled matter went off the record at 4:20 p.m.)

Reg Guide 1.82, Revision 5

Advisory Committee on Reactor Safeguards

November 1, 2022

Ahsan Salman

Steve Smith

RG 1.82 Changes in Rev. 5

- GSI-191 (Main body of RG and Appendix A)
  - Updated to include new information on the effects of debris on long-term core cooling
  - Major change was to add information and references regarding the in-vessel effects of debris
- Use of CAP (Appendix B)
  - Added new Appendix B - guidance on the use of CAP in determination of NPSH margins
  - RG 1.1 states only containment pressure prior to LOCA should be used in NPSH calcs
  - RG 1.1 withdrawn (4/2015); new CAP guidance is now included in RG 1.82, Rev 5.

GSI-191 Related Changes

- In-Vessel Guidance Updates
- Penetration Testing Guidance
- Improved Clarity and Detail
- Updated Knowledge Base Report
- BWR Evaluation of Lessons Learned
- Updated Jet Testing
- Test Debris Preparation Guidance
- Risk-Informed Resolution – Draft RG 1.229

RG 1.82 Status With Respect to GSI-191

- Revision 5 to RG 1.82 was made after the closure of GSI-191
- RG 1.82, Rev 5 is a complete guidance document for the effects of debris on long-term core cooling
- Additional risk-informed guidance may be issued as the result of the 10CFR50.46c rulemaking currently with the Commission

FLEX Equipment – Defense-in-Depth

- FLEX strategies are designed for beyond-design-basis external events initiated by natural phenomena
  - Not intended or reviewed for response to postulated accidents
- Flex equipment and strategies are different between BWRs and PWRs
  - BWR FLEX includes equipment for direct connection to the RCS and the ability to vent containment
  - PWR FLEX RCS injection only has low volume pumps with connections to the RCS
    - For Shutdown or low leakage only, includes borated water supply
    - Decay heat is removed via the steam generators with higher volume pumps
    - Connecting steam generator FLEX pumps to the RCS may be possible for some plants but has not been pre-planned or verified to be feasible in general
    - No pre-determined strategy for containment pressure reduction
- BWRs FLEX strategies are more suited to provide DID for cooling by direct connection to the RCS
- PWRs FLEX strategies may be less effective as DID for long-term cooling
  - Effectiveness depends on plant-specific equipment capacities, layouts, connections, etc.
  - No boration available at higher flow rates
  - Lower flows could be adequate if it takes a long time for strainer blockage to occur

UNITED STATES
NUCLEAR REGULATORY COMMISSION
WASHINGTON, D.C. 20555-0001

RG 1.82, REVISION 5, APPENDIX B

GUIDANCE FOR THE USE OF CONTAINMENT ACCIDENT PRESSURE IN DETERMINING THE NET POSITIVE SUCTION HEAD MARGIN FOR EMERGENCY CORE COOLING SYSTEM PUMPS AND CONTAINMENT HEAT REMOVAL PUMPS IN BOILING WATER REACTORS AND PRESSURIZED WATER REACTORS

CONTENTS

1. Background

- ACRS critique on use of CAP; discontinue EPU reviews
- NRC approved BWROG topical report describing standard approach for crediting CAP
- Staff white paper (2008) to ACRS summarizing regulatory and technical bases on CAP
- ACRS recommendation in letter to EDO included in RG
  - Licensees to use guidance in RG 1.82 to demonstrate positive NPSH margin
  - Operator actions to control CAP should be reliable, risk should be acceptably small
  - Before CAP credit, licensees to justify impractical to modify plant
    - Modification not needed for small CAP credit
  - Support staff reassessment of problems with NPSHa ≤ NPSHr
  - Agree with BWROG statistical calcs to calculate margin.
  - Margin (NPSHa – NPSHr) to consider uncertainty in NPSHr
- Staff SECY - (1) deterministic analysis; ACRS – (2) deterministic analysis + plant specific PRA
- SECY-11-0014, Commission voted for Option (1)
- Commission directed staff to credit CAP using guidance in SECY-11-0014, Enclosure 1
- RG 1.82, Revision 5, Appendix B is based on SECY-11-0014, Enclosure 1

2. Use of CAP in Determining NPSH Margin

- NPSH margin = (NPSHa – $NPSHr_{eff}$), where $NPSHr_{eff}$ = $NPSHr_{3\%}$ + uncertainties
- For DBA NPSH analysis, $NPSHr_{eff}$ should be used to determine the NPSH margin
- For BWR special events, $NPSHr_{3\%}$ and realistic inputs may be used
- Negative NPSH margin is acceptable if tests demonstrate pump will perform safety function(s), Monte Carlo analysis 95/95 lower limit to demonstrate margin in deterministic analysis
- CAP up to the vapor press at the pool temperature can be used without Monte Carlo analysis
- CAP above vapor press at pool temperature, Monte Carlo, pre-existing leak monitoring necessary

3. Containment Isolation and Containment Leakage

- If CAP is used, the licensees should demonstrate loss of containment integrity and loss of containment isolation cannot occur, monitor leakage during operation.

4. Quantifying NPSH Margin

- DBA LOCA- Conservative bounding inputs, realistic and Monte Carlo analysis to determine conservatism, NPSHr should include uncertainty.
- BWR special events - realistic analysis, NPSHr may be used without uncertainty

5. Guidance Summary

- For DBA, NPSH analysis should use NPSHreff = (1 + uncertainty) $NPSHr_{3\%}$
- For BWR special events, $NPSHr_{3\%}$ may be used to calculate margin
- Maximum flow rate for NPSHa analysis ≥ flow rate used in safety analysis
- Loss of containment integrity (venting) should not occur during CAP use
- NRC-approved operator action to control CAP is acceptable.
- Negative NPSH margin if tests on same or similar pump demonstrate adequate performance
- Propose a method to determine pre-existing leakage rate during plant operation
- BWRs - follow NEDC-33347P-A/NEDO-33347-A
- PWRs - use the vapor pressure corresponding to the sump water temperature or use a procedure a statistical process similar to the BWROG.
- Mission time for pump using CAP to include recovery time from the accident.

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

Advisory Committee on Reactor Safeguards
November 1, 2022

Technical Staff Presenters

- **Samir Darbali** – Electronics Engineer, NRR/DEX
- **Steven Alferink** – Reliability and Risk Analyst, NRR/DRA
- **Norbert Carte** – Senior Electronics Engineer, NRR/DEX

Digital I&C Project Managers

- **Bhagwat Jain** – Senior Project Manager, NRR/DORL
- **Michael Marshall** – Senior Project Manager, NRR/DORL

Working Group Members

- **NRR/DEX**
  - Norbert Carte
  - Samir Darbali
- **NRR/DRA**
  - Steven Alferink
  - Shilp Vasavada
  - Sunil Weerakkody
- **NRR/DSS**
  - Charley Peabody
- **NRR/DORL**
  - Bhagwat Jain
- **OGC**
  - Sheldon Clark
- **RES/DE**
  - Sergiu Basturescu
- **Additional NRR and RES Support**
  - Sushil Birla
  - Ming Li
  - Michael Marshall
  - Wendell Morton
  - Khoi Nguyen
  - David Rahn
  - Richard Stattel
  - Michael Waters
  - Steve Wyman

Presentation Outline

- Introduction
- Background and Key Messages
- Purpose of SECY-22-0076
- Staff Position on ACRS Questions
- Proposed Expanded Policy
  - SECY-22-0076 Points
- Next Steps

Background

- Nuclear power plants continue to install digital I&C technology
- SRM-SECY-93-087 directs that, if the D3 assessment shows that a postulated CCF could disable a safety function, then a diverse means be provided to perform that safety function or a different function
- The staff developed SECY-22-0076 which provides recommended language for an expanded policy that allows for greater use of risk-informed approaches to address DI&C CCFs for high safety significance systems

Key Messages

- The proposed expanded policy in SECY-22-0076 encompasses the current points of SRM-SECY-93-087 (with clarifications) and expands the use of risk-informed approaches in points 2 and 3
- The four points when taken together provide criteria for the assessment of diversity and defense in depth against CCF
- Use of risk-informed approaches will be expected to be consistent with the Safety Goal Policy Statement, PRA Policy Statement, and SRM-SECY-98-0144
- The current DI&C CCF policy will continue to remain a valid option for licensees and applicants
- Point 4 ensures the health and safety of the public and already incorporates an implicit element of risk informing as it focuses only on those critical safety functions needed to ensure the safety of the facility

SECY-22-0076 Purpose

- To request that the Commission expand the current policy for digital I&C CCFs to allow the use of risk-informed approaches to demonstrate the appropriate level of defense-in-depth, including not providing any diverse automatic actuation of safety functions.
- This expanded policy would apply to requests for new or amended licenses and design approvals, for all nuclear power plant types, under 10 CFR Part 50, “Domestic Licensing of Production and Utilization Facilities,” and 10 CFR Part 52, “Licenses, Certifications, and Approvals for Nuclear Power Plants.”

Staff Positions on ACRS DI&C Subcommittee Questions

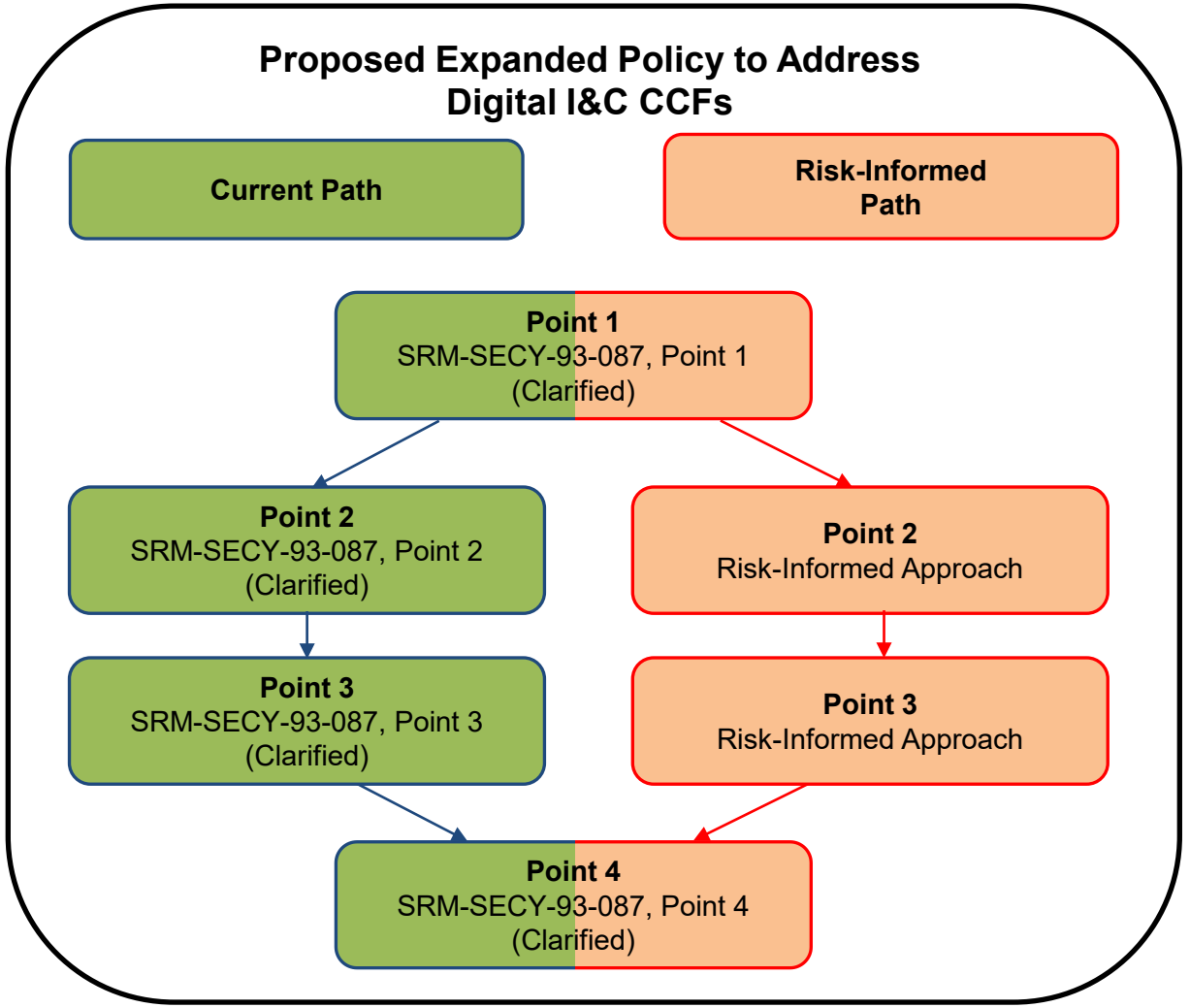
ACRS Question 1: *Would the revised policy be applicable to advanced reactors?*
Answer: The proposed expanded policy would apply to requests for all nuclear power plant types licensed under 10 CFR Part 50 and 10 CFR Part 52, including advanced reactors.

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.

Proposed Expanded Policy to Address DI&C CCFs

The Current Path allows for the use of best estimate analysis and diverse means to address a potential DI&C CCF



The Risk-Informed Path allows for the use of risk-informed approaches and other design techniques or measures other than diversity to address a potential DI&C CCF

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 1 Commentary

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

- This clarifying aspect of point 1 would be implemented consistent with the review guidance for graded approaches to digital I&C CCF in BTP 7-19, Revision 8.

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 2 Commentary

- Staff's goal is that the acceptance criteria for risk-informed approaches for digital I&C CCFs will be consistent with the NRC's broader (i.e., not specific to digital I&C) practices and guidance for risk-informed decision making.
- For example, the NRC staff will review license amendment requests for conformance to the guidance in RG 1.174 for applications employing risk-informed approaches.

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 3 Commentary

- The staff expects that for a license amendment request, the risk significance of CCFs will be determined by any increase in risk to the facility from a postulated digital I&C CCF and that this risk increase would be determined using a quantitative bounding assessment.
- Current experience is insufficient to establish confidence in quantifying the probability of occurrence of digital I&C CCFs.
- The NRC staff will not be able to approve risk-informed quantitative approaches based on reducing the probability of occurrence of digital I&C CCFs through design techniques for high safety significance SSCs.

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.

SECY-22-0076: Point 4 Commentary

- Point 4 is essential in staff's ability to conclude with reasonable assurance that a proposed digital I&C design does not adversely affect an operator's ability to manually control critical safety functions
- The staff's position is that the digital I&C system should not be able to take control of the facility away from the operator under all plant conditions (anticipated or unanticipated)
- Point 4 is consistent with the application of existing regulatory requirements for independence that are incorporated into the regulation (10 CFR 50.55a(h) and GDC 22)
- Point 4 already incorporates an implicit element of risk informing (in both SRM-SECY-93-087 and SECY-22-0076).
  - Point 4 is only applicable to critical safety functions (defined in SECY-93-087 and SECY-22-0076) and not to all the safety functions performed by the digital I&C system.
  - The diverse displays and manual controls do not have to be safety-grade or hardwired.

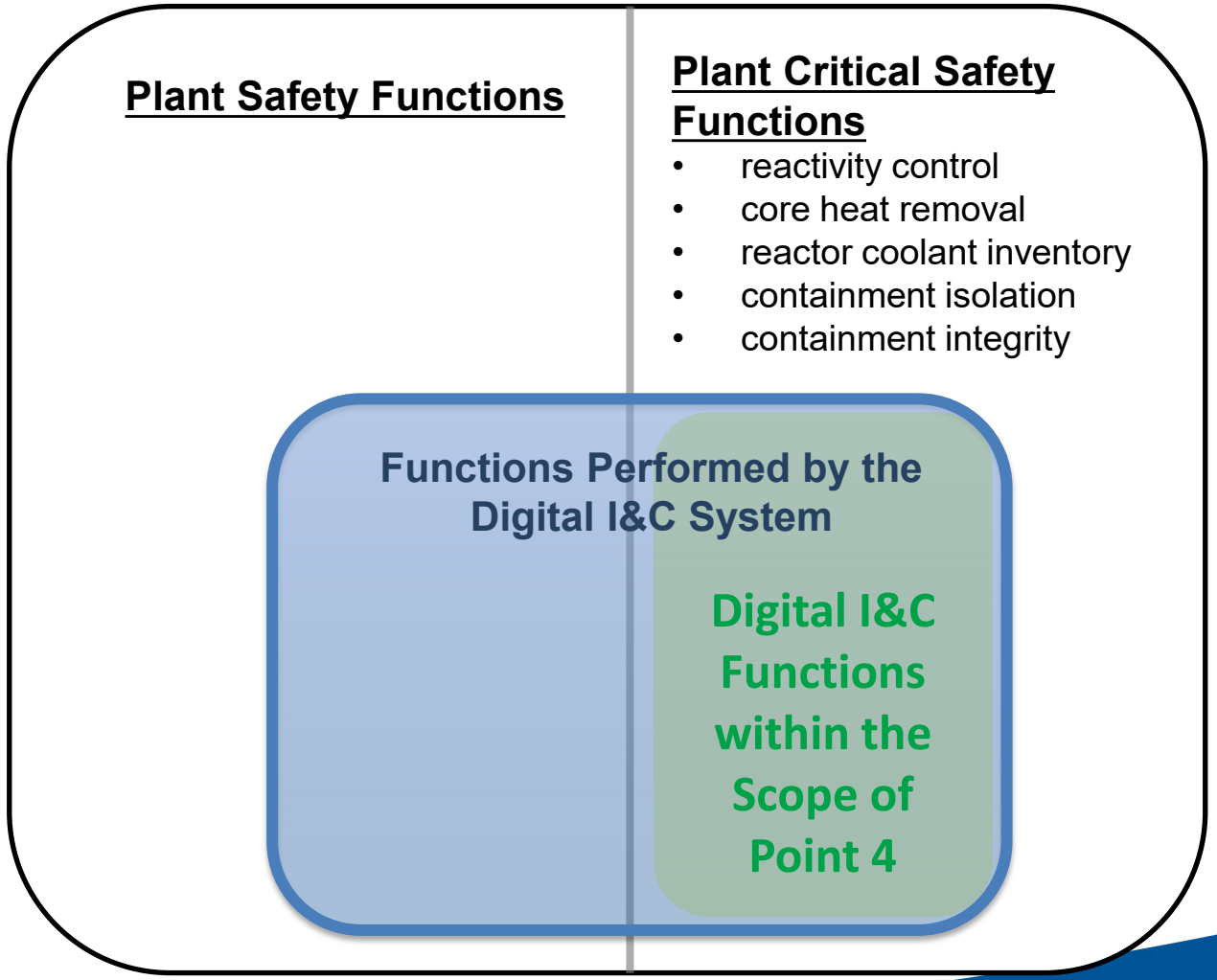
SECY-22-0076: Point 4 Commentary (contd.)

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.

SECY-22-0076: Point 4 Commentary (contd.)

- Point 4 of SECY-22-0076 has not been an impediment to modern digital control room designs
  - e.g., the NuScale and Vogtle 3 & 4 designs meet the current Point 4 of SRM-SECY-93-087
- Licensees that want to use risk information to reduce the requirements for manual controls can request an exemption or an alternative to 10 CFR 50.55a(h) and the staff would inform the Commission before approving or denying such exemptions and alternatives
- The staff believes industry concerns can be addressed in implementing guidance

Key Messages

- The proposed expanded policy in SECY-22-0076 encompasses the current points of SRM-SECY-93-087 (with clarifications) and expands the use of risk-informed approaches in points 2 and 3
- The four points when taken together provide criteria for the assessment of diversity and defense in depth against CCF
- Use of risk-informed approaches will be expected to be consistent with the Safety Goal Policy Statement, PRA Policy Statement, and SRM-SECY-98-0144
- The current DI&C CCF policy will continue to remain a valid option for licensees and applicants
- Point 4 ensures the health and safety of the public and already incorporates an implicit element of risk informing as it focuses only on those critical safety functions needed to ensure the safety of the facility

Next Steps

- If the Commission approves the expanded policy, the staff will:
  - update the existing implementation guidance to address digital I&C CCFs, and
  - continue to engage stakeholders and the public to seek comments on the staff's implementation of the expanded policy.

Questions?

Acronyms

BTP	Branch Technical Position
CCF	Common Cause Failure
D3	Defense-in-Depth and Diversity
DI&C	Digital Instrumentation and Control
ESFAS	Engineered Safety Features Actuation System
GDC	General Design Criteria
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