Official Transcript of Proceedings

NUCLEAR REGULATORY COMMISSION

Title: Digital Instrumentation and Control Systems Subcommittee Meeting

Docket Number: N/A

Location: Rockville, MD

Date: 05-17-2018

Work Order No.: NRC-3733

Pages 1-283

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

1
2
3
4 DISCLAIMER
5
6
7 UNITED STATES NUCLEAR REGULATORY COMMISSION'S
8 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS
9
10
11 The contents of this transcript of the
12 proceeding of the United States Nuclear Regulatory
13 Commission Advisory Committee on Reactor Safeguards,
14 as reported herein, is a record of the discussions
15 recorded at the meeting.
16
17 This transcript has not been reviewed,
18 corrected, and edited, and it may contain
19 inaccuracies.
20
21
22
23

1 UNITED STATES OF AMERICA

2 NUCLEAR REGULATORY COMMISSION

3 + + + + +

4 ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

5 (ACRS)

6 + + + + +

7 DIGITAL INSTRUMENTATION AND CONTROL SYSTEMS

8 SUBCOMMITTEE

9 + + + + +

10 THURSDAY

11 MAY 17, 2018

12 + + + + +

13 ROCKVILLE, MARYLAND

14 + + + + +

15 The Subcommittee met at the Nuclear

16 Regulatory Commission, Two White Flint North, Room

17 T2B1, 11545 Rockville Pike, at 8:30 a.m., Charles H.

18 Brown, Jr., Chairman, presiding.

19 COMMITTEE MEMBERS:

20 CHARLES H. BROWN, JR. Chairman

21 RONALD G. BALLINGER, Member

22 VESNA B. DIMITRIJEVIC, Member

23 WALTER L. KIRCHNER, Member

24 JOY L. REMPE, Member

25 GORDON R. SKILLMAN, Member

1 ACRS CONSULTANT:
2 MYRON HECHT
3
4 DESIGNATED FEDERAL OFFICIAL:
5 CHRISTINA ANTONESCU
6
7 ALSO PRESENT:
8 NEIL ARCHAMBO, Duke Energy
9 ROBERT E. AUSTIN, EPRI
10 ERIC BENNER, NRR
11 LUIS BETANCOURT, NRO
12 JOHN CONNELLY, Exelon
13 SAMIR DARBALI, NRR
14 MAURICIO GUTIERREZ, RES
15 RAY HERB, Southern Nuclear
16 WENDELL MORTON, NRR
17 DAVID RAHN, NRR
18 PAUL REBSTOCK, RES
19 JASON REMER, NEI
20 SERITA SANDERS, NRR
21 KEN SCAROLA, NAE
22 RICHARD STATTEL, NRR
23 DINESH TANEJA, NRO
24 BRIAN THOMAS, RES
25

ALSO PRESENT:

MICHAEL WATERS, NRR

DEANNA ZHANG, NRO

*Present via telephone

TABLE OF CONTENTS

Page

I. Opening Remarks by Chairman
Charles Brown.....5

II. Opening Remarks by Digital I&C
Steering Committee Chairman
Serita Sanders.....9
Eric Benner.....12

III. Revision to ISG-06 "Digital I&C
Licensing Process," Rev. 2
Samir Darbali, Richard Stattel,
Deanna Zhang, and Michael Waters.....20

IV. Public Comments.....143

V. Status of NRC CCF Activities
Mauricio Gutierrez, Ross Alvarado,
Dinesh Taneja, and Michael Waters.....156

VI. Public Comments.....235

VII. Closing Remarks by Chairman
Charles Brown.....256

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

2 (8:34 a.m.)

3 CHAIRMAN BROWN: The meeting will now come

4 to order. This is a meeting of the Digital

5 Instrumentation and Control Subcommittee. I am

6 Charles Brown, chairman of this subcommittee.

7 ACRS members in attendance are Vesna --

8 I'm not going to pronounce your last name --

9 Dimitrijevic. Did I get it close? Thank you. Joy

10 Rempe, Walt Kirchner, Dick Skillman, Myron Hecht, our

11 consultant, and Ron Ballinger. The designated federal

12 official for this meeting is Christina Antonescu, who

13 is seated to my left.

14 The purpose of the meeting is for the

15 staff to give a presentation to the subcommittee on

16 the latest revision to ISG-06, maybe it's the

17 revision, Revision 2, Digital I&C Licensing Process

18 and to brief the subcommittee on the status of the NRC

19 Common Cause Failures activities.

20 The ACRS was established by statute and is

21 governed by the Federal Advisory Committee Act. That

22 means that the committee can only speak through its

23 published letter reports. We hold meetings to gather

24 information to support our deliberations.

25 Interested parties who wish to provide

1 comments can contact our offices requesting time after
2 the meeting's Federal Register notice is published.
3 That said, we also set aside 15 minutes for spur of
4 the moment comments, for members of the public
5 attending or listening to our meetings. Written
6 comments are also welcome.
7 The ACRS section of the U.S. NRC public
8 website provides our charter, bylaws, letter reports,
9 and full transcripts of all full and subcommittee
10 meetings, including all slides presented at the
11 meetings.
12 We will hear presentations from the NRC
13 staff. The subcommittee will gather information,
14 analyze relevant issues and facts, and formulate
15 proposed positions and actions, as appropriate, for
16 deliberation by the full committee.
17 The rules for participation in today's
18 meeting have been announced as part of the notice of
19 this meeting previously published in the Federal
20 Register. As an add on to this particular previous
21 two couple of sentences, should be all public people
22 that are in the audience, as well as the staff should
23 be aware that comments by the subcommittee members
24 themselves, individually, are not necessarily words
25 spoken for the full committee. Those are only -- I

1 just wanted to reemphasize that those opinions, if
2 determined to be valid and useful, will be included in
3 our letter. Otherwise, we'd like to have our comments
4 considered if there is subsequent work to be done but
5 they do not have the strength of the full committee
6 behind them.
7 We have received a written comment and
8 request from Mr. Ken Scarola for time to make any oral
9 comments as a member of the public regarding today's
10 meeting.
11 As always, we have one bridge line
12 established for interested members of the public to
13 listen in. Also, the bridge line will be open at the
14 end of the meeting to see if anyone listening would
15 like to make any comments.
16 A transcript of the meeting is being kept
17 and will be made available, as stated in the Federal
18 Register notice. Therefore, we will request that
19 participants in this meeting use the microphones
20 located throughout the meeting room when addressing
21 the subcommittee. The participants should first
22 identify themselves and speak with sufficient clarity
23 and volume so that they may be readily heard.
24 And then, also, please silence all cell
25 phones, pager, iPhones, iPads, all appropriate other

1 noisy appliances that you may have in your possession.
2 And mine is -- my high quality, latest version flip
3 phone from 2002 is on manner mode. It works.
4 Where did I leave off? We will now
5 proceed with the meeting.
6 I call upon Mister -- hold it. Who have
7 I got? I was going to call on you to make comments.
8 Did you have any -- have at it Eric or Serita, whoever
9 is going to make comments for the staff. Fire away.
10 Oh, sorry. I apologize. I forgot
11 something. She didn't hit me.
12 During our morning comment period, there
13 are three industry individuals, Jason Remer, Ray Herb,
14 and John Connelly, who will be making some comments at
15 the end of the morning session. And in the afternoon,
16 Mr. Ken Scarola will be making a comment at the end of
17 the afternoon session.
18 Okay, now, Serita, Eric, take charge.
19 Turn the microphone on. The little green -- there,
20 you've got it.
21 MS. SANDERS: Okay, sorry about that.
22 CHAIRMAN BROWN: Also, please be careful
23 when you move paper because if it hits that
24 microphone, our transcription expert will probably
25 scream.

1 MS. SANDERS: Okay, thanks for that one,
2 too, because I would have.
3 Good morning, everyone, and welcome.
4 Before I get started, I would like to go over a few
5 housekeeping items. Charlie covered the cell phones.
6 So make sure you have your handouts. That you please
7 sign in, it's in the back of the room.
8 Escorts, if you need to go out soon -- oh,
9 Christine, you'll take care of all of that?
10 CHAIRMAN BROWN: Yes, that's all taken
11 care of. You don't have to worry about this stuff.
12 MS. SANDERS: Oh, good. Okay, that's a
13 switch. Okay, so now I can just --
14 MEMBER SKILLMAN: But thank you for your
15 accountability.
16 CHAIRMAN BROWN: Yes, don't take those
17 comments as negative.
18 MEMBER SKILLMAN: Yes, thank you.
19 MS. SANDERS: Okay, so I would like to
20 introduce Eric, who is our chair for the Digital
21 Instrumentation and Controls project and Mike, who is
22 the branch chief, NRR. He is also on the committee
23 for Digital I&C.
24 So we can start with the agenda, if you
25 will go to the next page. So we had our introductions

1 and the purpose.

2 So today we will discuss the -- just an

3 overview of the integrated action plans and we will

4 discuss also digital I&C 06, give a presentation on

5 Revision 2. And the staff has selected some

6 activities that they will go over to give you an

7 update of Common Cause Failure update and they'll also

8 tell you the next steps.

9 So since ACRS has got it together, I'm

10 just really going to turn this over to Eric to give

11 the opening remarks and then Mike will take it from

12 there.

13 MR. BENNER: Good morning. Thank you for

14 the opportunity for us to be here this morning and

15 brief you. As has been alluded to, this is my first

16 briefing of the subcommittee on this matter. I'm Eric

17 Benner. I'm the director of the Division of

18 Engineering in NRR and also the chair of the Digital

19 I&C Steering Committee, whom you know a number of us

20 -- and I will go through introductions momentarily to

21 talk about the composition. And I'm taking over the

22 efforts that were initiated by John Lubinski in this

23 area.

24 So we last briefed the -- everyone else

25 here, not me -- last briefed the subcommittee a year

1 ago on some of these topics and a lot has progressed
2 since then. And as you could expect in this field,
3 we've had to evolve over that time, based on feedback
4 and priorities of our stakeholders, both internal and
5 external.
6 So we greatly appreciate you accommodating
7 our schedule. We know we've changed some of the
8 topics for the series of briefings we have of you to
9 help accommodate those priorities.
10 So this slide reflects our key messages
11 that we'll share on the progress of the Integrated
12 Action Plan. We feel we're making good progress on
13 the objectives of the IAP. We issued the second
14 revision to the IAP in January of this year and are
15 working on another revision, as we speak, mainly
16 because what I would say are two reasons. One, you
17 know we're actually making some tangible progress and
18 are going to have some successes here in the near
19 future. And two, as part of the evolution, there has
20 been dialogue between the NRC staff and the industry
21 about the priorities for the remaining tasks in the
22 IAP.
23 So we're looking at the next update to the
24 IAP. We'll have some re-baselining to it as to the
25 path forward.

1 MEMBER SKILLMAN: Eric, is there a
2 licensee waiting in the wings itching to use Rev. 2?
3 MR. BENNER: We have heard assertions that
4 there are but we haven't heard any details of whom
5 that may be. So, I think as the industry
6 representatives some of their comments later, we would
7 love for you to ask that question of them.
8 MEMBER SKILLMAN: That was a curiosity
9 question.
10 MR. BENNER: No, we're curious too.
11 MEMBER SKILLMAN: Thank you. Thanks.
12 MR. BENNER: So our highest focus on those
13 activities that support those near-term upgrade needs
14 by industry. And I think, you know as is evidenced by
15 this meeting, that clarity on how to address common
16 cause failures of digital systems has been the highest
17 technical priority for the industry, primarily
18 upgrades made under 10 CFR 50.59.
19 So this afternoon, we're going to discuss
20 the status of CCF issues, some of which affect our
21 regulatory guidance for 50.59.
22 We have a regulatory issue summary that
23 we're looking to issue later this month, which is an
24 intermediate step for licensees to do digital
25 modifications under 10 CFR 50.59, i.e., without NRC

1 review and approval. So we're close on that.
2 So the next priority closely behind this
3 is the update to ISG-06, which we are going to be
4 doing a more detailed briefing of today. That
5 guidance is how the staff will conduct licensing
6 reviews for those things that are submitted to the NRC
7 for review.
8 The draft ISG is targeted to be issued for
9 public comment in the end of July. So we're looking
10 forward to a formal ACRS letter, ideally a positive
11 ACRS letter, on that activity to support the public
12 meeting and our completing that activity.
13 So the team this morning and this
14 afternoon are going to discuss these activities and
15 some other activities in detail.
16 Finally, we'll continue to maintain
17 interactions with our public stakeholders and the ACRS
18 on these activities and further modernization efforts.
19 So before I turn it over to Mike, I'll do
20 some introduction of the speakers.
21 Serita Sanders, who you've already heard
22 from, is our project manager and has worked closely
23 with Christina to make this briefing happen. So we
24 thank -- I thank, personally, both of them because I
25 know, again, for both the scheduling and the

1 finalization of the topics and getting you all the
2 appropriate information, they did a lot of heavy work
3 to make that happen.
4 CONSULTANT HECHT: Eric, excuse me. Could
5 you clarify? You said you were looking for ACRS
6 letter to endorse -- was it the --
7 MR. BENNER: ISG-06.
8 CONSULTANT HECHT: ISG-06. I'm sorry.
9 Okay, did you hear that? Okay, thank you.
10 MR. BENNER: Yes, so we're looking for a
11 formal letter on ISG-06.
12 CONSULTANT HECHT: ISG-06, not the update
13 to RIS 2002?
14 MR. BENNER: No.
15 So for the briefing on ISG-06, we'll have
16 Samir Darbali, Rich Stattel, Deanna Zhang discussing
17 that. Mike Waters, who is a branch chief in NRR will
18 do a kickoff for that activity.
19 And then, in the afternoon, we'll have
20 Mauricio Gutierrez, Dinesh Taneja, and Mike again to
21 talk about just the topic of CCF more broadly,
22 particularly communications we intend to have with the
23 Commission on the subject.
24 We have a number of technical support
25 staff in the room, who will be seated at the tables to

1 answer any questions you may have and they include
2 Bernie Dittman, Wendell Morton, Dave Rahn, and Ismael
3 Garcia.
4 Also I said I'm the chair of the Steering
5 Committee. The Steering Committee has representatives
6 from the offices of NRO -- Bob Caldwell, who is at one
7 of the back tables, and Brian Thomas from the Office
8 of Research.
9 So we're well represented here today. So
10 the hope is we will be able to answer any of the
11 questions you have.
12 So with that, I'm going to turn it over to
13 Mike Waters.
14 MEMBER SKILLMAN: Before we transition,
15 let me ask a question, please.
16 I spent a lot of time as a qualified 50.59
17 reviewer for GPU. And the substance of that training
18 was causing all of those, all of us who were
19 qualified, to come to a full understanding that 50.59
20 is not a change process; 50.59 is a screening process
21 to determine whether or not a license amendment is
22 required. Right?
23 MR. BENNER: Correct.
24 MEMBER SKILLMAN: As I was reading the
25 material, the supplement, the Rev 2 of the ISG, I was

1 wondering. And this is the question I pose: How much
2 of the turbulence on this issue is the result of
3 licensee individuals not understanding that 50.59 is
4 really a screening process as opposed to their
5 believing it is, in and of itself, a minor mods change
6 process?
7 I ask that question because after I left
8 Three Mile Island in an engineering capacity, I did
9 consulting for a long time, and most of the plants I
10 went to were not 95003 and 95002 plants or 0350
11 plants. And that was a common understanding or a
12 common learning from those licensees that while the
13 staff understood they needed to 50.59s, they were
14 actually treating 50.59 as a change process versus a
15 screening process. That got them into a lot of
16 trouble which is why I think you have the supplement.
17 So my question is how much of what we are
18 going to talk about today is at least in part due to,
19 if you will, a failure to fully understand what 50.59
20 is intended to accomplish.
21 MR. BENNER: I think we'll discuss that a
22 little today. I don't think we're going to get in-
23 depth. I can tell you that in our interactions with
24 the industry, particularly on the RIS -- because
25 sometimes you'll hear thrown out there well, you know

1 these things are very safe. And we point out, the
2 staff points out that it should all be safe. Whether
3 you do it under 50.59 or whether you come in for a
4 license amendment, a licensee needs to convince
5 themself that what they're doing is safe.
6 And like you say, 50.59 is about merely
7 determining whether something needs to come to the NRC
8 --
9 MEMBER SKILLMAN: Correct.
10 MR. BENNER: -- for review.
11 So I think we reiterate that position,
12 both in the digital I&C arena and, unfortunately, the
13 50.59 staff who have been supporting us on this are
14 not here today but they, in both the interactions we
15 have had and other more general interactions with the
16 industry reemphasized that point.
17 I think the fact that we're doing some of
18 these things in parallel, both the 50.59 guidance and
19 the licensing guidance, I think that allows us to
20 reemphasize that point in a more rich manner because
21 some of the core issues of safety, particularly for
22 common cause failure, are the same. And really when
23 we talk about 50.59, we are reemphasizing that an
24 individual plant's licensing basis is a box and 50.59
25 just helps them decide is this change they're going to

1 make in that box or not, not is that change safe or
2 not.
3 So we certainly empathize with the concern
4 you raise. We think we've reiterated that point
5 several times. I have it on good faith from industry
6 that once the RIS goes out, there's going to be
7 training by the industry of industry potential users
8 of the RIS on the use of the RIS. And we'll
9 reemphasize that part of the training that needs to
10 improve that point.
11 MEMBER SKILLMAN: Thank you, Eric. Thank
12 you.
13 CHAIRMAN BROWN: Just to follow-up on
14 Dick's comment, I mean the RIS supplement that is
15 going to be discussed this afternoon did point out, I
16 think on page 2, that there were two problems that the
17 staff at NRC had identified inconsistencies in the
18 performance of the documentation that was used for
19 engineering evaluations and that evaluations of the 10
20 CFR 50.59 criteria were apparently not very clear to
21 some folks. And that was one of the purposes of this
22 supplement was to amplify that.
23 So I think that's where you were kind of
24 headed with this. So I mean it sounds like people,
25 licensees, or whoever it is that are doing their

evaluations, may end up falling into hey everything's okay as opposed to no, we need to submit an amendment based on the documentation that was reviewed.

So that is a concern and it is also supposed to be addressed by the supplement and is the subject of a little bit of a discussion this afternoon.

Did I clarify what you were saying suitably?

MEMBER SKILLMAN: Yes, I'm not trying to establish a different momentum for this meeting.

CHAIRMAN BROWN: No, that's okay I just didn't want it to be --

MEMBER SKILLMAN: When Eric was on bullet 3, I was thinking back of the experience that I bring to the table and I was reminding myself how often licensees failed to use 50.59 as a screening tool and, rather, they were using it as a mini-mod process. And they were saying now everything's okay; this is really not safety related. When in reality, it did take the plant outside the license box.

Thanks, Charlie. That's all I was trying to say.

MR. BENNER: Okay. With that, I'll turn it over to Mike Waters.

1 MR. WATERS: Good morning, Charlie and
2 ACRS members.
3 As Eric noted, we last briefed the
4 subcommittee last year, May. We provided a detailed
5 briefing on an Integrated Action Plan for Digital I&C.
6 And I believe we are tentatively scheduled to brief
7 the subcommittee next month on the updating IAP as
8 well.
9 Just to provide some context and
10 background for our presentations today, these are some
11 elements of the Commission direction to Digital I&C to
12 provide a basis of why we're going to talk about ISG-
13 06 and common cause failure status.
14 To summarize, the Commission directed the
15 staff to develop an integrated strategy to modernize
16 infrastructure of digital I&C, to consider a broader
17 context of challenges, including common cause failure
18 technical issues, 50.59, and incorporation of IEEE-603
19 into the regulation.
20 The Commission directed us to focus on
21 approaches of guidance on acceptable approaches to
22 comply with requirements and for the actual I&C safety
23 requirements to be technology neutral.
24 The Commission reemphasized some points of
25 stakeholder interactions to identify common problems,

1 common priorities, and potential solutions to address
2 them.
3 With that, next slide, please.
4 This is just a very broad overview of the
5 Integrated Action Plan. It represents the current
6 structure and format of the plan. We divided high
7 priority work into four main Modernization Plans and
8 you can see some have sub-activities. Just to provide
9 a little bit of a roadmap for the committee and the
10 audience, what you see in yellow are the plans we're
11 going to talk about today, this morning. We talked
12 about ISG-06, labeled as MP 4A. And this afternoon we
13 will provide a status update of activities for common
14 cause failure of MP 1.
15 With that, if there's any questions, we
16 can do a swap of staff and start ISG-06.
17 CHAIRMAN BROWN: Have at it.
18 MR. DARBALI: Good morning. My name is
19 Samir Darbali. I'm a technical reviewer in the
20 Instrumentation and Control Branch in NRR. I am
21 joined by Mike Waters, Rich Stattel, and Deanna Zhang.
22 And today we will be presenting on Draft Revision 2 of
23 ISG-06 titled Licensing Process.
24 I would like to emphasize that the staff
25 is asking for ACRS review and comments on this draft

1 revision.

2 The outline of this presentation is as

3 follows. First, we will describe the scope and

4 purpose of the ISG and explain how it relates to the

5 Integrated Action Plan. We will provide some

6 background information on the current version of ISG-

7 06, Revision 1. We will then describe Draft Revision

8 2 of the ISG, which will supersede Revision 1, and

9 discuss the two review processes described in Revision

10 2.

11 The first process is an improvement of the

12 Revision 1 review process and the second is a new

13 process for approval at an earlier development life

14 cycle stage. We are referring to this new process as

15 the alternate review process.

16 Finally, we will describe the next steps

17 in the ISG-06 revision project.

18 This slide describes the purpose and scope

19 of ISG-06. ISG-06 defines the licensing process used

20 to support the review of license amendment requests

21 associated with safety-related digital I&C equipment

22 modifications I operating plants and in new plants

23 once they become operational. This guidance is

24 consistent with the NRC's policy on the digital I&C

25 equipment and it is not intended to be substituted for

1 NRC regulations.

2 This ISG provides guidance for activities

3 performed before license amendment request submittal

4 and during review. The NRC staff uses the process

5 described in the ISG to evaluate compliance with NRC

6 regulations.

7 CHAIRMAN BROWN: I just want to make one

8 comment relative to this. I think you may have said

9 this but I wanted to say it slightly differently.

10 The ISG is not a set of regulations for

11 the licensees to follow. It's merely telling them

12 what you are going to do when you review their

13 submittals --

14 MR. DARBALI: Right.

15 CHAIRMAN BROWN: -- to ensure that they

16 have content that allows you to process, to go on

17 through it in a somewhat more detailed manner than

18 what may be available by looking at the regulations.

19 Is that a satisfactory statement?

20 MR. DARBALI: Yes.

21 CHAIRMAN BROWN: Richard is looking at me

22 real strangely here.

23 MR. DARBALI: The ISG by itself is

24 guidance to the staff but it is a document that

25 industry can use to understand which set of

1 regulations they would need to address and the
2 guidance documents as well.
3 CHAIRMAN BROWN: Okay.
4 MR. STATTEL: You're looking at me,
5 Charlie.
6 CHAIRMAN BROWN: I don't know. You're
7 looking at me. And anytime I see you looking at me
8 like that --
9 MR. STATTEL: Yes, what Samir said is
10 correct. The original revision of the ISG, it really
11 was prompted by the industry because the industry had
12 a lot of questions about submitting what it takes to
13 submit a digital I&C modification because there is a
14 lot of regulatory guidance. It's complicated. It's
15 difficult to figure out for someone who doesn't work
16 in this area all the time. And that's ten years ago.
17 So one of the objectives of the original
18 version of the ISG was to give some clarity and let
19 the industry know what information would need to be
20 provided to the NRC to support a safety evaluation of
21 a reactor protection system, for example.
22 So we've carried that into the new
23 revision of the ISG as well.
24 CHAIRMAN BROWN: Okay, thank you.
25 MR. DARBALI: So this slide describes how

1 the ISG-06 Revision 2 draft relates to the Integrated
2 Action Plan. The Integrated Action Plan established
3 the following ISG-06 revision goals: first, to reduce
4 the scope of licensee document submittals; and second,
5 to provide an alternative for earlier approval, which
6 would precede factory acceptance testing, for digital
7 designs that are based on approved topical reports.
8 The Modernization Plan 4A Working Group
9 under the IAP worked with industry and internal
10 stakeholders to improve the licensing process in ISG-
11 06.
12 The results of the ISG-06 draft revision
13 are that the tiered or Tier 1, 2, and 3 review process
14 that is original to the Revision 1 has been improved.
15 We will describe this process in later slides.
16 Also a new alternative review process has
17 been introduced for license amendment request approval
18 before factory acceptance testing. We will also be
19 describing this new process in later slides.
20 CHAIRMAN BROWN: A comment, just an
21 observation, actually, a question that I wasn't quite
22 sure I understood talking about prior to factory
23 acceptance test. And I'll probably ask this question
24 again, once you get farther along.
25 The focus, from what I read out of this,

on Tier 1, 2, and 3 was all aimed at topical reports approved, Tier 1; deviation was Tier 2; 3, you want to do something that doesn't have an approval yet. And the alternate review is the approval of the LAR before factory acceptance test.

There seemed to me to be a differentiation that this total focus is on a platform. That was the way I read the ISG Tier 1, 2, 3. No emphasis at all on what an architecture of how the platform would be applied in a design, whether it be a protection and safeguards upgrade, or whether it be a turbine generator voltage regulator, or governor of feedwater pump control, et cetera.

And I guess I wanted to get that out. There's an explanation that is going to be given later as to why the only important thing is the platform and how it is going to be used is really the most critical part, and how it's arranged in an overall system architecture.

Obviously, I'm particularly interested relative to how it would be used for reactor trip system and safeguard system upgrades. The feedwater -- you know what I call component controllers, a little bit different in terms of how you would apply it and it's recognized.

1 So that was a concern I had as I started
2 reading, as I went on through and then saw the
3 standard Section D, all the boilerplate about here's
4 all the stuff to look at in various circumstances.
5 So I had a little bit of a lack of concern
6 -- I had considerable concern when I saw Tier 1, 2,
7 and 3 had no system architecture associated with it at
8 all, as well as -- in other words, if you're using
9 this platform, we don't really -- pick a work very
10 carefully -- I don't want to say you don't care but it
11 wasn't important for determining whether you needed to
12 submit a license amendment or not. You could go to 10
13 CFR 50.59 without the license amendment, if you met
14 the Tier 1 requirements for an approved topical
15 report.
16 MR. DARBALI: So we will have a slide that
17 will compare all processes, as far as how they use a
18 topical and how they address an architecture. We will
19 also have a slide that will compare what we call
20 Enclosure B of the ISG.
21 CHAIRMAN BROWN: I'm obviously referring
22 to Enclosure B, which is very good, by the way. It is
23 very clear as to what technical requirements out of
24 Section 2 had to be followed. And there were
25 virtually nothing but software processes for Tier 1,

2, and 3, for the most part. For the most part.

MR. DARBALI: So we will be clarifying that. Yes.

CHAIRMAN BROWN: Okay, I just wanted to get out on the table.

MR. DARBALI: Okay.

CHAIRMAN BROWN: It's probably the biggest point of the whole thing because some of the downstream stuff is kind of what you put in everything, what was in the previous ISG as well, although abbreviated.

MR. STATTEL: This is Rich Stattel. We will be getting into some of those detailed discussions. However, I will just provide an overview.

One of the things that makes digital I&C modifications, license amendments different, unique, different from other disciplines, mechanical systems, electrical systems is the fact that the development process is really done in two parts. One is the platform because we are using platforms that have a lot of software and a lot of hardware design that goes into them before we even consider what the application needs to do and what the safety functions are. That's really not the case with electrical systems or other

1 types of systems.

2 CHAIRMAN BROWN: I agree. I understand

3 your point.

4 MR. STATTEL: So it is really a dual

5 review, right, so think of it that way.

6 And we're trying not to differentiate

7 within the ISG because this is review guidance and we

8 apply ISG-06 for both reviewing of platforms and

9 reviewing of the license applications themselves,

10 which has the details that you're looking for.

11 So that's one major difference.

12 And the other concept that ISG-06

13 introduced that really wasn't part of our framework

14 leading into the original version of ISG-06 was the

15 fact that it allows us to be involved because these

16 development process -- because we're talking about two

17 different system developments, essentially, they take

18 place over an extended period of time, two, three,

19 four, sometimes even five and six years go by and the

20 development activities are occurring over these

21 extended periods.

22 So traditionally, the NRC, if we're

23 looking at a piping system or an electrical system, we

24 see a relatively completed design at the onset at the

25 time of the license amendment submittal and we review

1 that and evaluate that with the regulatory criteria.
2 Well, in the case of I&C, we're missing the
3 opportunity to look at what takes place over the
4 course of the five years, that extended period of
5 time.
6 So what the ISG introduces is a parallel
7 review process. That's what Tier 1 evaluation is all
8 about. It allows us to perform an evaluation of the
9 processes that are used to develop the platform and
10 the system initially, on an initial submittal, and
11 have the actual system development, the safety
12 function development occur in parallel with our, the
13 NRC being involved in the review. And just basically,
14 these two things happen in parallel.
15 And then at the end of the day, really the
16 factory acceptance test has always been our milestone
17 for everything kind of coming together at the end.
18 It's really -- I want to point out that the factory
19 acceptance test itself is not that critical of an
20 activity, as far as the licensing evaluation, but it
21 is more of a milestone because we know that the
22 systems are completed, built, operational at the time
23 of factory acceptance testing.
24 So it's really more of milestone, just a
25 place keeper. And that's were kind of everything

1 comes together.

2 But the concept that ISG-06 introduced was

3 the fact that we can perform the review in parallel

4 with the design, development, and implementation

5 activities that take place over an extended period of

6 time. And later on we do have a slide that has kind

7 of calendar, a time line layout that kind of

8 illustrates that. So we can talk a little bit more in

9 detail about what's entailed with that. But that's

10 really what's different about ISG-06.

11 And the alternate review process is really

12 changing the time line a little bit. It takes a

13 little bit of the purview away from the NRC but we

14 also have the inspection activities that would keep

15 us involved.

16 Okay? I hope that helps.

17 CHAIRMAN BROWN: Yes, I'm a little bit

18 more confused but that's how old my old brain here.

19 MR. STATTEL: Well, we'll work through the

20 details as we go.

21 CHAIRMAN BROWN: But fundamentally, when

22 I looked at it and I combined that with your Figure

23 C.1, along with Enclosure B, and along with your

24 definition of the tiers, and what the alternate review

25 process involves, the alternate review process gets

1 right involved immediately in system architectures.
2 In other words, it's almost like -- similar to what we
3 see in some of the new plant designs that come in, we
4 see figures, one-line diagrams, how you're going to
5 protect yourself relative to the software corruption,
6 the watchdog timers, all that shmear that we go on,
7 and on, and on about in those design reviews.
8 I know this does not apply to -- I
9 understand that this does not apply to new plant
10 designs, such as the AP1000 or other type plants.
11 It's for new plants after they become operational or
12 existing operating plants.
13 MR. STATTEL: I have an answer for you but
14 I would prefer to wait until we get to that section.
15 CHAIRMAN BROWN: That's fine. I'm just
16 trying to get my thought process. Out of all this
17 stuff in this whole ISG, I'm still struggling with
18 trying to integrate now relative to the earlier last
19 thing that we did eight years ago how we -- bear in
20 mind I have no problem with understanding. I have got
21 a Common Q platform. You know what it is. It has
22 been put in place. It's used on two or three new
23 plant designs. You know what it looks like. You've
24 approved it, several versions of it. You don't have
25 to mouse milk the Common Q platform for other than

1 what I call system requirements that you need to look
2 at.
3 I don't see how that gets applied in terms
4 of the Tier 1, 2, 3 in this ISG in your initial
5 reviews. That's where I had a hang-up on the ISG.
6 So we can wait. That's just fine. I
7 don't want to slow this down.
8 Deanna, you are moving your mouth up and
9 down like you'd like to --
10 MS. ZHANG: No, I mean if Rich wants to
11 wait until later, we can wait until later.
12 CHAIRMAN BROWN: That's fine. All I
13 wanted to do was make sure you understood what I was
14 looking at and some of the thoughts I had, so that you
15 could at least calibrate yourself as you went along.
16 MR. STATTEL: Okay, thank you.
17 CHAIRMAN BROWN: Okay.
18 MR. DARBALI: Okay. So we will now be
19 providing some background information. As we go
20 through our presentation, we will be talking both
21 about Revision 1 and Revision 2 of the ISG. So we
22 will try to be clear as to which provision we are
23 talking about.
24 We will start by describing some key
25 concepts that are part of the existing ISG Revision 1.

1 And then we will highlight some of the lessons learned
2 from using Revision 1.
3 Revision 1 was the initial issuance of
4 ISG-06 and it introduced the concept of tier labels as
5 a general guide for defining the scope or complexity
6 of a review. This enables the use of a graded
7 approach based on how or if a modification is based on
8 a preapproved platform topical report.
9 When we refer to a tiered or a Tier 1, 2,
10 3 review process, we are referring a to review process
11 that is common to all three tiers, although the scope
12 or complexity of the review may vary. This tier
13 review process is the process that is currently
14 described in Revision 1 and it is maintained and
15 improved in Revision 2.
16 I would like to point out that this
17 concept of tiers is unique to ISG-06. So if you've
18 heard the word tier somewhere else, it is separate
19 from that.
20 Revision 1 also introduced the concept of
21 phases as a general guide for defining the NRC staff
22 activities to be performed during the review. This
23 phased approach allows the staff and the licensee to
24 coordinate the scheduling for submitting documents,
25 discuss license amendment request review activities,

1 and discuss post-license amendment activities.
2 This phased approach also allows licensees
3 to submit early design and planning information with
4 the license amendment request as part of Phase 1 or
5 the license amendment request submittal.
6 Under Phase 2, licensees submit detailed
7 design implementation and testing information as a
8 supplement to the license amendment request. As you
9 will see in later slides, the concept of Phase 2 or
10 supplemental information submittal only applies to the
11 tier process and not to the alternate review process.
12 MR. STATTEL: Okay, hold for just a
13 second.
14 So at this point, I'd like to address one
15 of
16 your questions, Charlie, with regard to the Tier 1
17 process, the way it was originally developed in the
18 ISG.
19 So because we have two phases of review,
20 essentially Phase 1 addresses, like Samir mentioned,
21 the planning aspects and the initial design, the high-
22 level design, without having design detail.
23 So your question about architecture, at
24 the Phase 1 portion of the review, the architecture is
25 not necessarily completed. Right? So that

1 information is not there and that's why that's not
2 described and that's why it's not mentioned -- really
3 that section was originally targeted to just the
4 alternate review process, which we'll talk about next.
5 Now in Phase 2, I'll note that Phase 2
6 includes several sections. There are several sections
7 that I'll get into the details of that later. There
8 are several sections but Phase 2 includes detailed
9 design, a much higher level of detailed design than
10 even the alternate review process would provide. So
11 we're looking for what we normally see and we've been
12 through this process several times. We normally see
13 detailed design requirements documents in the area of
14 both hardware and software.
15 So in software, we would see software
16 design descriptions that they are either docketed for
17 our review or we evaluate those as part of an audit.
18 But those are very detailed documents.
19 And to give you an example of that, for
20 the Oconee system that we evaluated, the software
21 design description was a book on the order of 4,000 or
22 5,000 pages long. Similarly for the Diablo Canyon
23 license amendment, the software design description
24 was, again, it was a 3,000-4,000 page document.
25 There's a lot of information, a lot of details in

1 there, including hardware design details such that we
2 have the architecture. The detailed architecture is
3 in front of us.
4 So we're not looking at a concept that
5 will be implemented in the future. For our Tier 1
6 review, we are looking at the actual detailed
7 architecture of the system and that is part of that
8 evaluation process.
9 You might recall in the Diablo Canyon
10 application we did evaluate the architecture. We
11 described the architecture in the front part of our
12 safety evaluation.
13 So I don't want you -- because -- I
14 understand the perception that is presented here
15 because we have an architecture section that's new
16 that applies only to alternate tier process. I don't
17 want you to have the impression that we don't perform
18 the architecture review for our Tier 1 process because
19 we have been doing that all along.
20 And we did receive that comment and we are
21 in the process of working through those comments. And
22 one of the things that we're considering is making
23 that section applicable to basically, regardless of
24 the tier or the type of process you are using, the
25 guidance in that section should be applicable.

1 CHAIRMAN BROWN: Yes, in Enclosure B I put
2 little Xs all across the board.
3 I understand your point. I was trying to
4 do exactly what you are talking about --
5 MR. STATTEL: Yes.
6 CHAIRMAN BROWN: -- looking at the Phase
7 1 from your figure.
8 MR. STATTEL: Yes.
9 CHAIRMAN BROWN: Whatever it is -- C.1.
10 And then seeing Phase 2, if I can find the figure.
11 Sorry, that's the wrong one. Phase 2 then became the
12 next round as you moved out of the Phase 1 and down
13 into the Phase 2. I said okay, is it in there. And
14 I went back to look at the enclosure and it has
15 absolutely -- it starts with D.9. D.2 is not even
16 discussed in any one --
17 MR. STATTEL: Right but I would point out
18 that --
19 CHAIRMAN BROWN: And where it occurs, I
20 don't want to say I don't care. It's just a matter it
21 needs to be -- at some point, it needs to be there
22 however it is.
23 MR. STATTEL: Yes, so let me just explain.
24 The D.2 is kind of a special section in the ISG. And
25 it's really more of an artifact of how we got to this

1 point, how we developed this.

2 So we had a team that developed the new

3 guidance that was necessary for -- to support the

4 alternate review process. And they weren't thinking

5 about the existing processes. Right? So what was

6 left over essentially spilled into D.9.

7 D.9 has several sections to it, several

8 sub-sections to it. And it includes several

9 documents, several implementation artifacts that

10 licensees would provide to us that are not available

11 in the alternate review process. And that's where a

12 lot of these things will spill over into.

13 And when we get to those figures, I'll be

14 happy to --

15 CHAIRMAN BROWN: Okay, all I was trying to

16 say is I sprung from one to the other.

17 MR. STATTEL: Yes.

18 CHAIRMAN BROWN: It's just the D.9 stuff

19 is almost all software development, operating

20 environment software, software program documents for

21 software descriptions and all that other kind of

22 stuff, all necessary for the overall system that

23 you're looking at.

24 MR. STATTEL: But keep in mind, with the

25 alternate process, we don't have access to this.

1 CHAIRMAN BROWN: I understand that. I'm
2 very, very clear from --
3 MR. STATTEL: That's the key point.
4 CHAIRMAN BROWN: I'm very, very clear from
5 the enclosure. And I was trying to translate that
6 into the C.2 as to where -- I understood the alternate
7 review process but, in itself, seemed to be a little
8 bit incomplete also because the stuff in D.9 is not
9 available -- is not obvious.
10 MR. STATTEL: Right.
11 CHAIRMAN BROWN: That's probably a better
12 way of phrasing it.
13 So that's my major concern with what we
14 see here is not decoupling a total agreement with what
15 something looks like from a system architecture
16 standpoint so that it's not all software. I mean it's
17 just not all software. The software is not going to
18 protect me on a system design basis. If anything,
19 it's going to make things worse. You've heard me say
20 that before.
21 So that's why I was concerned about the
22 defensive architecture thought process that we've
23 focused on in almost all, whether it's Diablo Canyon
24 -- we had tons of discussions on Diablo Canyon
25 relative to how they really made the new system very,

1 very independent and very reliable from a standpoint
2 in terms of -- or at least that's my personal opinion
3 and I think we agreed with that in our letter to you
4 fairly clearly.
5 Okay, thank you for your thoughts. If you
6 want to go on, we'll proceed.
7 MR. DARBALI: So ISG-06, Revision 1 has
8 been used to review the Diablo Canyon plant protection
9 system digital modification, the Hope Creek Power
10 Range Neutron Monitoring System digital modification,
11 as well as various digital I&C topical reports.
12 For the use of Revision 1, the staff has
13 identified various lessons learned. One of these was
14 the recognition that the tiered label and review
15 phase concepts are useful to the staff in performing
16 the reviews.
17 When the original ISG was first developed,
18 and as has been previously mentioned, it was intended
19 to be a one-stop shop, meaning a place where all
20 guidance information could be found. This approach
21 led to several challenges. In particular, guidance in
22 Standard Review Plan Chapter 7 and IEEE Standard 603
23 and 7-4.3.2 was duplicated in Revision 1 of the ISG;
24 references to regulatory guides and other documents
25 became outdated; and also, Revision 1 focused more on

1 identifying specific documents, instead of the
2 information needed to make the required safety
3 determination.
4 Next slide.
5 The staff also recognized that the tier
6 process could be further improved and streamlined.
7 Additionally, industry has expressed
8 concerns that significant resources are required for
9 procuring, developing, and testing a full digital I&C
10 design before the license amendment is issued.
11 These lessons learned, along with industry
12 feedback on Revision 1 have helped the staff draft
13 Revision 2 of ISG-06.
14 So this slide I hope can address your
15 questions regarding the --
16 CHAIRMAN BROWN: Can you back up one slide
17 again?
18 MR. DARBALI: Sure.
19 CHAIRMAN BROWN: One more. The question
20 on -- and I've forgotten how long ago it was we tried
21 to upgrade the rules to go from IEEE 603 1991 to 2009.
22 Is that correct?
23 MEMBER SKILLMAN: That's correct. Good
24 memory.
25 CHAIRMAN BROWN: That's about the only

1 thing left sometimes.

2 And you actually went to the Commission to

3 do that and the Commission rebuffed us and you. Right

4 now, 1991 is still in play. There's no, although I

5 see references to later, like 7.4.3.2, which is not in

6 the rule either. It's not in the rule either, is it?

7 MS. ZHANG: No.

8 CHAIRMAN BROWN: No, okay. But yet you

9 talk about the other versions in several

10 circumstances.

11 Is there going to part of this whole

12 process at the end to get the later revisions of the

13 IEEE standard into the rule again or are we just kind

14 of throwing dust in the wind to think about that?

15 MR. STATTEL: Did you want to start, Mike?

16 MR. WATERS: Right now we are in a holding

17 pattern of whether or not we're going to have a

18 proposed rulemaking and incorporate the latter

19 revision.

20 The next update to IEEE-603 I think is

21 scheduled to be completed in the summer or fall, Rich,

22 to be published.

23 CHAIRMAN BROWN: That's the IEEE, the

24 munching around on that and changing it some more.

25 MR. WATERS: At that point, based on other

1 lessons learned and considerations, we'll consider our
2 next steps on endorsing that either through regulatory
3 guidance or rulemaking but we have made no decisions
4 at this time.
5 I guess Rich can elaborate on how 603 is
6 referenced in ISG-06.
7 MR. STATTEL: Well, I just want to mention
8 I am on the working group for development of new
9 revision to IEEE-603. The current -- the latest
10 version is the 2009 version that the incorporation by
11 reference was rejected by the Commission, as you
12 mentioned.
13 The new version we expect, the working
14 group expects that to be published this year. So we
15 expect it to be a 2018 version. It has been through
16 balloting at the IEEE and we're expecting a
17 recirculation ballot very shortly, like in the next
18 month. So that's where that stands.
19 I also want to recognize Frank Novak is in
20 the room and Frank is the chairman of that working
21 group, the IEEE Working Group.
22 Now additionally, I will mention that the
23 rulemaking effort completed about two or three years
24 ago. The outcome of that included -- we had developed
25 several documents regarding statements of

1 consideration and guidance and it addressed problems.
2 The rulemaking package identified several problems
3 that we had with the regulation that needed to be
4 corrected.
5 The NRC contacted the IEEE and transferred
6 that documentation to the IEEE and the IEEE agreed to
7 accept those and work on those as part of the new
8 revision to the IEEE. So those are being considered.
9 The issues that were identified during the
10 rulemaking effort are being considered by the working
11 group and the fix is, at least from the IEEE's
12 perspective, are being addressed in the 2018 version
13 of the IEEE standard.
14 So our goal you know we're kind of
15 anticipating. We don't know what the final decision
16 is going to be, whether to incorporate the new version
17 into regulation or to endorse it by the Reg Guide, as
18 Mike had mentioned. But we're expecting this new
19 version, which does better address digital technology
20 than a 1991 version. We expect that to be endorsed
21 and/or incorporated into regulation by the NRC at some
22 time in the near future.
23 CHAIRMAN BROWN: One of my concerns always
24 is when outside group, like the IEEE, starts modifying
25 stuff and the industry gets involved if you start

1 throwing out some of the babies with the bath water.
2 In other words, some of the useful stuff
3 that the NRC, that we, would like to see in our plant
4 designs in terms of requirements gets softened. I'm
5 not aware that we've seen anything as to when it would
6 be projected, how it would be revised or what the
7 revisions would look like.
8 Is that published anywhere or is that
9 still within the IEEE Standards Committee itself?
10 MR. STATTEL: Well, it's certainly within
11 my purview because I'm on the working group. So, I
12 can see the changes that are being proposed and being
13 made. And I have been meeting with NRC staff and we
14 have provided ballot comments from the NRC perspective
15 to the IEEE. And on the working group, we are working
16 through those comments.
17 So I think the NRC is fully aware of the
18 changes that are being made to the standard.
19 CHAIRMAN BROWN: Oh, I don't doubt that.
20 Can you share those with us? I've been fairly vocal
21 on some items, as you probably remember.
22 MR. STATTEL: I'm trying to think. It's
23 not published. It's not published but I have shared
24 it with several members of the NRC staff as part of
25 the balloting process.

1 I'm really not prepared today to discuss
2 the changes that are being made to this.
3 CHAIRMAN BROWN: That's fine. I don't
4 expect you to.
5 MR. STATTEL: Okay.
6 CHAIRMAN BROWN: I just hate to leave it
7 to the time when you become -- incorporating it in the
8 regulations under a new rulemaking that comes through
9 here and now the committee doesn't agree with
10 incorporating it, which would be a shame.
11 MR. WATERS: Right. Part of the process,
12 of course once it's finalized, we'll take a look at it
13 to make the decision if we want to incorporate it into
14 rulemaking, including whether or not we would take
15 exception to parts of the standard and/or have
16 additional requirements or conditions added. That's
17 part of the process.
18 I think also to note which we also have
19 the companion IEEE-7.4.3.2 guidance, which Deanna
20 Zhang represents NRC on. So, some of the technical
21 issues may be also dispositioned in that guidance
22 document -- in that standard as well. So when we look
23 at 603, we'll probably be looking at 7.4.3.2 at the
24 same time, the overall fabric of the standards as far
25 as what would be acceptable to the staff.

1 CHAIRMAN BROWN: They're not trying to
2 merge 7.4.3.2 into the 603 to make a single document?
3 As of right now, you've got a little comparison of
4 here's the 7.4.3 listing number by number and then the
5 1991 version number by -- or the 2009 version.
6 MR. STATTEL: Oh, the IEEE is not changing
7 their position on that. The idea behind that is that
8 IEEE-603 is a technology neutral document.
9 CHAIRMAN BROWN: Okay.
10 MR. STATTEL: And 7.4.3.2 is intended to
11 address digital instrumentation. So, it has a lot of
12 language and terminology that is specific to digital.
13 CHAIRMAN BROWN: Okay. Okay, I understand
14 the point.
15 MR. STATTEL: Okay.
16 CHAIRMAN BROWN: I just want to avoid the
17 circumstance. I agree that taking exceptions after --
18 when we see it later in the game and start trying to
19 put exceptions into the regulation, the Reg Guides, as
20 you write them, and/or a rule change becomes --
21 MR. WATERS: We agree as well. Of course
22 the goal would be to be a clean endorsement. That's
23 our ultimate goal.
24 And although, as you know, IEEE is a code
25 and standard and we participate but, at the end of the

1 day, we have to look at what they found and published
2 to make that decision.
3 CHAIRMAN BROWN: I just want to make it
4 clear that -- and I think you do -- because we did
5 make comments the last time with wanting to make some
6 exceptions to it. I think the rulemaking we wrote
7 comments back to you on few instances.
8 MR. BENNER: Charles, this is Eric Benner.
9 I think what I'm hearing from you is you don't want to
10 get to the end game of we're doing the rulemaking and
11 that's the first time we have any engagement with you
12 or the first time you see any of this. So I think we
13 can take that back to look at.
14 Certainly, when the standard is published,
15 I would tend to think we can share that with the
16 committee and we can talk about whether there can be
17 any intervening communications prior to the staff
18 making any sort of formal recommendation that we would
19 be looking for your endorsement on.
20 CHAIRMAN BROWN: If they wait long enough,
21 I might be dead. I don't know. You never know what's
22 going to happen.
23 MR. STATTEL: I would mention one thing,
24 though. There's one area in the IEEE standard that
25 was part of the rulemaking -- it was identified as an

1 issue as part of the rulemaking effort, and that's the
2 area of diversity and defense-in-depth, and addressing
3 common cause failures.
4 And the 2009 version that we were looking
5 at at the time really did not provide any additional
6 guidance in that area. That section of the IEEE
7 standard is being revised, a significant revision to
8 that section, where it's been challenging for the
9 working group. But we're attempting to write it in
10 such a way that it doesn't conflict any of our
11 existing policies or any of our licensees that rely on
12 that section, you know that language for their basis,
13 and provides the opportunity to address future
14 developments and research results that come out in the
15 future.
16 So we're trying to both predict -- address
17 the past, not conflict with the past, not conflict --
18 not invalidate any licensing basis that's in place but
19 also we want to make it so that we're flexible enough
20 to be able to handle future developments in the area
21 of common cause failure, addressing common cause
22 failures.
23 So it's been challenging but that's pretty
24 much that's the section that has the most significant
25 revision in IEEE-603.

1 MR. THOMAS: Charlie, if I may. Brian
2 Thomas.
3 CHAIRMAN BROWN: Oh, there you are, Brian.
4 MR. THOMAS: Brian Thomas. I truly
5 appreciate your requests that you raise. I do want to
6 second what the working group is saying, as well as
7 what Eric said. This is on the radar for the Steering
8 Committee. We are, in effect, looking at what is the
9 comprehensiveness, if you will. What is the
10 completeness of what is being incorporated into 603
11 versus what parts of it is being incorporated into
12 7.4.3.2? How complete is it in addressing the issues
13 that were raised in the IBR that went up to Commission
14 and got rejected, basically.
15 So we are looking at that and that is part
16 of our task. And you raise a very good point. It's
17 part of our task and our action going forward prior to
18 getting to what's being validated and what's being put
19 before the SCO. We want to make sure that all of the
20 issues that were raised are adequately being addressed
21 in the different rulemaking efforts -- the rulemaking,
22 as well as what you do in 7.4.3.2, even though that's
23 not in the rule.
24 The other thing I want to point out is
25 Mike said, Mike Waters said that you know whole IEEE-

1 603 effort is, in part, currently sort of on hold to
2 an extent. I want to emphasize that the Steering
3 Committee is looking at that from the standpoint that
4 we do have the -- we are expecting the information
5 from the Innovation and Transformation Team, if you
6 will, who looked at how do we address IEEE-603 in our
7 evaluation process and does it afford us the kind of
8 efficiency and effectiveness in our whole licensing
9 process.
10 And there is expectation or anticipation,
11 if you will, that we will get a recommendation from
12 the Transformation Team that may be along the lines of
13 -- and I'm speculating a little bit about it because
14 we have a sense of what's forthcoming from the
15 transformation team, which has yet to be addressed by
16 the Commission level -- but it's along the lines of
17 there is a possibility they may be saying that we need
18 to find a way to address IEEE-603 in other mechanisms,
19 other than via the rulemaking.
20 So that's part of the moving forward with
21 603, like Rich says, and what we're doing there. But
22 part of what we're thinking about is how is that to be
23 influenced by what comes out of the recommendations
24 from the Transformation Team.
25 CHAIRMAN BROWN: I understand, you know,

1 that it's a consensus document. That's just the way
2 it is. It's been around.
3 It's a technology neutral consensus
4 document. I just don't want to lose -- I mean, right
5 now it's in the rules.
6 So, right now somebody ho -- when somebody
7 wants to apply, they raise that little flag up. And
8 if they meet that flag in the rulemaking, you're --
9 and there's the back and forth sometimes.
10 And sometimes you succeed and sometimes
11 you don't. And a lot has changed since 1991.
12 Including my phone, so.
13 (Laughter.)
14 CHAIRMAN BROWN: So, there's a good reason
15 for that. So, I don't -- we can go on. I mean, I
16 understand it's -- we can deal with exceptions if it
17 gets to the point that it's not an NRC document.
18 It's an IEEE general consensus, you know,
19 technology document that they're putting out and
20 they're updating that's fine. I just didn't want to
21 lose sight of the fact.
22 And I didn't want us to get to the
23 endpoint when we finally have to do something where we
24 haven't seen anything at all. Or at least it's going
25 to be addressed with us at some point.

1 MR. STATTEL: You may recall that the
2 primary reason for the Commission rejecting the
3 rulemaking effort was those conditions and extra
4 things that the NRC was adding on. There was no real
5 objections to anything really in the standard itself.
6 That the Commission did not express any
7 objections to anything in the 2009 standard. It was
8 just the conditions that were being imposed, or being
9 added by the rulemaking effort.
10 So, with that in mind, we have made an
11 effort to communicate with IEEE to address those
12 conditions in the new versions of this Standard and
13 the 7432 Standard. So that, I'm very optimistic, and
14 I hope that the -- if we go through a rulemaking
15 effort again to endorse this new version, there will
16 be no conditions.
17 It would be just a clean endorsement. And
18 it should be -- it should be accomplished in a pretty
19 short order I would hope.
20 CHAIRMAN BROWN: Okay. Go ahead.
21 MR. DARBALI: So, Slide 15 hopefully
22 addresses some of your questions on the use of topical
23 app -- topical report platforms in our reviews.
24 The way the slide is constructed, on your
25 -- on the left side you will see the current Revision

1 review focus. In the middle you'll see the Tier 1, 2, 3 process in Revision 2.

And on the right side you'll see the new Alternate Review Process of Revision 2. I want to focus your attention on that top row, where we talk about the approved platform topical report.

All three processes, the one in the current version, and the two in the Revision 2, rely on the use in the approved platform topical report. You do know that for a Tier 3 review, a preapproved platform has not -- is not being referenced.

So that review is concurrent to the license amendment request review. But essentially for Tier 1 and 2, and your alternate review process, you are relying on a preapproved platform topical report.

Your second row has to do with the staff's review of the application specific system design, and that meeting regulatory requirements. And that's true for all processes.

So, when we're talking about, you know, watchdog timers, all of that is reviewed regardless of which review process we're talking about.

CHAIRMAN BROWN: Is that Phase Two, or is that in Phase One?

MR. DARBALI: For --

1 CHAIRMAN BROWN: That's where I couldn't
2 -- if that's in there, but where --
3 MR. STATTEL: It's primarily Phase Two.
4 CHAIRMAN BROWN: Okay. And that's where
5 I lost the bubble in terms of how that -- because
6 Phase Two with all the two or four through whatever
7 the number, last number is, was fundamentally focused
8 on process, software processes, QA, I mean, I could
9 read all of them.
10 But I don't want, you know, reliability
11 analysis et cetera. There's absolutely zero
12 architecture thought processes in terms of how the
13 platforms are applied in a real system.
14 For particularly reactor trip and
15 engineered safeguard systems as we see those applied
16 to nuclear power plants.
17 MR. DARBALI: And that is good feedback.
18 The staff is so used to using the tier process that
19 maybe we already have that information in the back of
20 our minds.
21 And if it's not explicitly stated, we
22 don't miss it. So, we can certainly take a look at
23 that and make the language clearer.
24 CHAIRMAN BROWN: Per your Figure C.1, I
25 would have seen that application specific design. In

1 other words, that's the system design, would come
2 under the Phase 2 line under your Figure C.1. for the
3 Tier 1, 2, and 3 processes.
4 Is that what you're saying?
5 MR. DARBALI: I think we do have a backup
6 slide of that Figure. So we could go to that.
7 CHAIRMAN BROWN: All I'm looking for is
8 somehow the ISG has to -- to me it doesn't say that
9 right now.
10 MR. DARBALI: Okay.
11 CHAIRMAN BROWN: I don't know whether
12 anybody else -- I'm just looking around. I guess I'm
13 asking the question.
14 MEMBER KIRCHNER: I've struggled with the
15 same approach. But, it's not my field. And maybe I'm
16 not -- you always start with an architecture and a
17 system that defines functional requirements.
18 And if you're going to plug in a platform
19 or whatever it is, and it doesn't matter whether it's
20 a pump or a digital component. I don't see the
21 difference personally.
22 You have to have -- it has to meet an
23 architectural set of requirements, functional
24 requirements. And then somehow in the system manner
25 be tested to ensure that it delivers those, you know,

it meets those functional requirements.

Is that what you mean by specific system design? It meets regulatory requirements?

MR. DARBALI: Correct. Yes. So, the application of the platform to the plant should meet those regulatory requirements.

So, again, if the language in the ISG is not clear, we will take a look at that. But the intention is for it to be the same regardless of the review process.

What we will see later in the time line how and when information is provided. But the idea is -- the idea to focus a section D-2 on system architecture for the alternate review process is to tell the staff and the licensee, you won't be able to see the finished complete tested design.

Therefore, that description needs to be provided up front.

CHAIRMAN BROWN: I don't disagree with that. That's what we do in the new plant designs.

MR. DARBALI: Right.

CHAIRMAN BROWN: The factory acceptance test is not on -- I mean, a real proving design characteristics and system architecture is right now --

1 MR. DARBALI: Right.

2 CHAIRMAN BROWN: On a specific proposed
3 licensed plant by a licensee.

4 And we've seen exactly what you're talking
5 about. It's fundamentally an alternate review
6 process.

7 It's all done before a factory acceptance
8 test. And that's just fine. No problem with that.
9 And my concern is that based on the reading in the
10 ISG, Tier 1, 2, 3, take that all out.

11 I mean, it's just the platform, the
12 platform, the platform. The only one that maybe in
13 question is Tier 3.

14 Although that was largely focused on
15 making sure the platform conforms to the desires for
16 platform requirements. How you review those.

17 And when you have a topical report with --
18 like the Common Q platform that's used in some of the
19 plants. If I don't get shot for saying that, has a
20 topical report. It is followed.

21 And if anybody's got perturbations, we
22 discuss those as part of the overall architectural
23 review.

24 MR. DARBALI: Okay.

25 CHAIRMAN BROWN: So, that doesn't -- but

1 the topical report doesn't even talk about a system
2 architecture.
3 MS. ZHANG: So, I was going to talk about
4 all this when I come up. And my slides come up.
5 CHAIRMAN BROWN: Okay. All right. That's
6 fine.
7 MS. ZHANG: I can talk about --
8 CHAIRMAN BROWN: I've made my point. I
9 have this severe problem of reiterating. If I don't
10 say it 14 times, I'm not satisfied.
11 So, I want to make it very, very clear.
12 Okay.
13 MR. STATTEL: I would just call your
14 attention to the Enclosure B document. I think we can
15 go over this.
16 CHAIRMAN BROWN: That's what I'm looking
17 at.
18 MR. STATTEL: There is a section in the
19 Tier 1 process, the table, the second table. There's
20 an as manufactured system configuration documentation.
21 And we're already talking about adding
22 references to Section D.2 and D.3 into that table.
23 But, fundamentally, the -- we have the hardware
24 documentation.
25 We've -- this is kind -- like I mentioned

1 before, this is kind of an artifact of how we're
2 developing this. Because we're kind of adding the
3 alternate review process on top of an existing
4 process.
5 Now the existing process, I mean, maybe
6 the titles aren't that great. But -- and it's reduced
7 from what it was in the first revision of the
8 document. Right?
9 But again, we're pointing at information
10 to be provided. We have -- we have always had full
11 view of what the architectures of these replacement
12 systems are.
13 And typically in our experience, in my
14 experience with Diablo Canyon, the architecture pretty
15 much mirrors what the existing architecture of their
16 Eagle 21 System was for example.
17 CHAIRMAN BROWN: Absolutely correct.
18 MR. STATTEL: And of course we're looking
19 at that. And we're evaluating that.
20 So, in Section D.2 we've provided some
21 more specific guidance. Now, it was written with the
22 idea of the alternate Tier process.
23 But we also recognized that that guidance
24 is still -- is good guidance as well for the existing
25 processes. So, we intend to correct that.

1 CHAIRMAN BROWN: I like the word correct
2 that. Just is that going to be corrected before it
3 goes out for public comment in July?
4 Mr. STATTEL: Yes.
5 MR. DARBALI: The idea is before we go for
6 public comment, we will take -- the ISG is currently
7 going for internal concurrences. So, we're getting
8 comments from different groups.
9 And we'll also look at any recommendations
10 from the ACRS. So, all of those will be looked at and
11 then try to address those before we take it for public
12 comment.
13 CHAIRMAN BROWN: Well, if you haven't
14 figured it out, that's probably going to be comment on
15 our letter. If I can convince the Committee that
16 that's needed.
17 MR. DARBALI: Fourteen times, right?
18 CHAIRMAN BROWN: Yeah. I'll only say it
19 once in the letter.
20 (Laughter.)
21 CHAIRMAN BROWN: I understand -- when I go
22 back, you commented on those sections about as
23 manufactured system configuration document D.5.
24 If you go look at D.5 it says, it's a --
25 it says you've got to have paper that's a

1 configuration of management activities. Which is
2 paper.
3 MR. DARBALI: Okay.
4 CHAIRMAN BROWN: It's not a -- there's --
5 my point being is, there's got to be some type -- now
6 I'm very much in favor of this whole ISG thing.
7 If you remember from eight years ago, I
8 was touting what we're doing. Because it is too
9 complicated by the time you walk your way through how
10 the licensees know what they're supposed to provide.
11 And that's what the guide reg is. I don't
12 want to lose sight of the architecture, the defensive
13 architectural approach to doing these whole things.
14 And I understand that you can knock off
15 some of the reviews and reduce the reviews necessary
16 based on approved platforms and other topicals that
17 you've used. But the overall system architecture is
18 -- and Richard's right from the Diablo Canyon thing.
19 I mean, they -- it was cookie cutter
20 almost. I mean, they kept everything. They just put
21 everything in each division and maintained the
22 existing architecture.
23 Which made the review from our standpoint
24 say hey, we can really agree with you. It's a piece
25 of cake. Go forward.

1 I don't even remember that we had any
2 comments in our letter when we agreed with your
3 proceeding.
4 MR. DARBALI: Right.
5 CHAIRMAN BROWN: So, anyway, go ahead.
6 MR. DARBALI: Sure. And I would also like
7 to say that, you know, when the licensee uses a
8 topical report, there's going to be a list of plant
9 specific action items. And some of those are intended
10 to address the architecture.
11 So, --
12 CHAIRMAN BROWN: Well, the topical
13 report's not going to have that.
14 MR. DARBALI: But the plant specific
15 action item in the safety evaluation approving the
16 platform. It will be an action item telling the
17 licensee, this cannot be reviewed during the platform
18 generic review.
19 Therefore, the licensee needs to address
20 the use of the platform for this specific activity.
21 CHAIRMAN BROWN: The application, yeah, or
22 the platform.
23 MR. DARBALI: Correct.
24 CHAIRMAN BROWN: Somehow that needs to get
25 its way in here. I don't know where you're going to

1 put it.

2 MR. DARBALI: Okay.

3 CHAIRMAN BROWN: But that's how you're

4 going to do it. But that's fine.

5 MR. DARBALI: Okay. Understood.

6 CHAIRMAN BROWN: All right. Go on. So,

7 you're really moving here.

8 MR. DARBALI: All right. So, we spoke

9 about the consistency of the first two rows. The

10 difference between the current Rev 1 Tiered process,

11 the Rev 2 process, and the Alternate Review Process,

12 as in how it addresses or focuses on the second two

13 rows.

14 So, currently Rev 1 not only focuses on

15 the application software design, implementation and

16 testing plans, as well as processes, making sure those

17 are acceptable. It also focuses on that the

18 application system development and testing produce

19 acceptable outputs or an acceptable product.

20 Does that realize that if you're looking

21 at the final product then the planning documentation

22 is not as critical. So, that kind of helped inform

23 the improved Tier process and the Alternate Review

24 Process.

25 In the Tier process, although there will

be planning documents, the focus will be on that finished product. Whereas in the Alternate Review Process, which is meant to produce a license amendment before factor acceptance testing, we won't be able to look at that finished produced.

The focus is more on your planning and processing. Making sure those will create that acceptable output. Next slide.

So this slide is a time line comparison of the licensing and oversight activities for the Tiered Review Process and the Alternate Review Process.

Not that these activities are not to scale. So there might be some variance in when an activity starts or how it lasts.

The middle portion shows the licensee activities related to the data INC modification development. The top portion of the slide shows the NRC staff activities that are performed under a Tiered 1, 2, 3 Review Process.

And the bottom portion of the slide shows the NRC staff activities that would be performed under an Alternate Review Process. For both of these processes, the slide shows when a license amendment request is expected to be submitted and when the license amendment is suspected to be issued.

The wide box in the middle represents the Phase Two submittal that is unique to the Tier 1, 2, and 3 process. Note that the Alternate Review Process eliminates the Phase Two submittal. All information required to make a safety determination is to be provided with the license amendment request.

The key differences between the two processes are that for the Alternate Review Process, the license amendment is suspected to be issued earlier before completion of the total hardware and software design implementation and test activities.

And also, the completion of these activities would be covered by optional NRC vendor inspections.

MEMBER SKILLMAN: Let me ask this question, please. For the Diablo Canyon change and for the Oconee change, did the NRC staff conclude that the licensee, versus a contractor that might have produced the five thousand pages and the three thousand pages, that the licensee really understood the depth and breadth of the changes, and incorporated appropriately the change.

Because this ISG is really about change control. It's a modification to your -- whatever the system is. Appropriately incorporated the change into

1 the maintenance rule activities, to their system
2 descriptions, to their technical specifications, to
3 the surveillances?
4 Now your question is about the degree to
5 which the licensee really took ownership and
6 demonstrated ownership.
7 MR. STATTEL: I would like to thank you
8 for asking that question. Because initially I would
9 say the answer was no.
10 With Oconee they had a perception that
11 because they were referencing a license topical report
12 that had already been approved by the NRC that they
13 did not need to take that ownership or provide a lot
14 of oversight to the vendor.
15 They simply could do a turnkey project.
16 Purchase it. It's already approved. And put it in
17 without having that understanding.
18 And that created a lot of conflict.
19 Particularly with Oconee. Because that was really the
20 first time we had applied that.
21 It was resolved though, I will say.
22 Because that project, the NRC was kind of realizing
23 that the licensee did not have that ownership. And
24 that the vendor didn't have the appreciation for what
25 their obligations were.

1 So, part of the resolution of that is we
2 had discussions with the licensee. We explained to
3 them that they needed to understand the processes that
4 the vendor was using.
5 And they needed to provide oversight. In
6 Oconee's case they provided that oversight after the
7 fact. After we had identified this.
8 And they performed formal audits of the
9 vendor, AREVA and Alpharetta, and identified problems.
10 And I think that was very useful to us because those
11 audit reports that the licensee had provided us told
12 us that look, it's not just us that's seeing these
13 issues at the vendor. Now the licensee is aware of
14 them.
15 And because the contact is between the
16 licensee and the vendor, you know, now the ownership
17 really goes to the licensee, right. So, they did take
18 ownership. And that was resolved before we issued
19 that license amendment.
20 So, in Oconee's case I definitely would
21 say that they did have that understanding. And they
22 did understand the processes that were being used by
23 the vendor.
24 Now Diablo Canyon, we had the benefit of
25 the experience of Oconee. So we had these discussions

1 with the licensee before they even made the submittal.
2 And we explained to them, you need to
3 provide oversight to these vendors. You need to
4 understand their processes. You need to understand
5 the interfaces.
6 And they were dealing with two different
7 vendors. So it was an even more complicated. So, we
8 were very aware of this.
9 And we find it more effective for the
10 licensee to be providing that oversight rather than
11 for us to be providing the oversight.
12 MEMBER SKILLMAN: Now Rich, is that
13 codified? At least codified to the extent that the
14 Agency and particularly your inspectors can strike
15 that lightning bolt early to make sure that there is
16 ownership at the licensee level?
17 MR. STATTEL: It probably could be better.
18 The requirements are there for providing oversight.
19 The responsibility is always the license holder.
20 MEMBER SKILLMAN: Um-hum.
21 MR. STATTEL: But sometimes we have to go
22 out and point this out to them. Right? So, we have
23 changed the way we're writing our license topical
24 reports.
25 And we're trying to articulate this in

1 what we call plant specific action items within those
2 topical reports. But, again, you know, I think we
3 have made a lot of improvements in this area.
4 And we certainly have an awareness of it.
5 And any licensee that comes to us, we make them aware
6 of this.
7 So, it's really not an ongoing issue for
8 us. As far as codification, we do write this into our
9 topical reports as we go forward. But we don't always
10 have the opportunity.
11 Some of the topical reports are from the
12 1993, 1998. And they don't have the language in there
13 to ensure this happens.
14 MR. WATERS: Just to chime in. Ultimately
15 we have of course the quality assurance requirements,
16 Appendix B Program, which is codified. Which would be
17 one key regulation we go out and inspect against.
18 And some things that we have realized in
19 developing this is in forms of licensees' vendor
20 oversight plan. And you need to expect as part of the
21 ultimate review process we would go out and inspect
22 that through the inspection branch with the quality
23 assurance experts and the INC experts to verify that
24 the licensee is adequately overseeing the vendor
25 development.

1 Because we have the same questions as well
2 about that process.
3 MEMBER SKILLMAN: Well, and I would think
4 in a live coordinate, the first team that would be
5 coming out swinging would be the INC techs at the
6 plant. They would come out and say wait a minute,
7 what are you doing?
8 I've become comfortable with this thing.
9 And now you're going to give me a frontal lobotomy.
10 And how in the world am I going to catch up to this,
11 because you're changing the tech specs. You're
12 changing procedures. You're changing all of my
13 maintenance activities.
14 So, anticipating that, it would strike me,
15 words are important. Words matter. That maybe the
16 front end of this ISG should contain words that
17 recognize this is a change process.
18 This is a configuration management
19 process. And unless the licensee takes ownership at
20 the first round, the gap can begin to widen between
21 what your functional performance requirements document
22 is, and what your vendor is going to provide, and what
23 you're going to do to your plant.
24 And I'm a plant person. If someone said
25 hey, you better understand, we are really going to

monkey around with your control -- with your RPS or the ESFAS, that would get my attention very quickly if I was -- had plant engineering.

MR. STATTEL: And it should.

MEMBER SKILLMAN: Exactly. And so as arcane as that might sound, as one who has sat in the role for years and years, which I thank you for giving me the heads up.

And I'm going to convene a team to make sure I've got ops and maintenance in tune as the drum beat picks up. So that when we get to the point where we're actually dealing with the vendor, I know what's coming from my plant.

Again, the whole ISG begins with the words, this is about a license amendment request. Well, a license amendment request is at its very foundation, in my view, a major change to your license.

The reason it's LAR is because it's a big deal. But because you're normally into the RPS or the ESFAS or another system of that pedigree, warning the licensee you better get on top of this right in the beginning in the ISG, seems to me to be good policy.

MR. STATTEL: So, my response is I do believe, you know, we -- over the years, we have

1 learned and we have become a lot more aware of the
2 issue and the responsibilities.
3 And where the opportunity has come up, we
4 have made changes to our standard review plan to our
5 license topical reports. I think the issue that I
6 mentioned really kind of centered around the
7 preapproved topical report and what does that mean.
8 And we wanted to provide a better
9 definition of what exactly that means. What is it
10 that we're approving? And what are we not,
11 specifically not approving?
12 And therefore, in the more recent license
13 topical report evaluations, you'll see a much more
14 detailed and much more open list of what those items
15 are that still need to be addressed during the actual
16 license amendment.
17 This also touches on the area of
18 inspection space. So, for example, I had mentioned,
19 you know, we had performed inspections at Oconee.
20 And they had identified issues with
21 procedure. Because typically, procedures are
22 developed after the license amendment.
23 That's -- I expect that to still be the
24 case. And some issues came up during the Oconee start
25 up where, you know, they didn't think writing the

1 procedures was going to really affect the way they
2 operate the system.
3 Or they didn't think the system, the new
4 system would really significantly impact the
5 procedure. But as it turned out, they learned that
6 lesson too.
7 Because they were testing out these
8 procedures on their simulator. And they found that
9 some things didn't work the way they expected them to.
10 And they were nuances of the system,
11 whatever. But they had to be addressed. And so our
12 inspectors were there. I was part of that inspection
13 team.
14 And Samir also was part of an inspection
15 team there. And we kind of worked through that. And
16 the inspectors appreciated that too.
17 And they appreciated having the
18 application specific action items documented in the
19 license topical report evaluation. Because it kind of
20 guided them right towards what was important.
21 And then that's getting those procedures
22 right. And providing that oversight. Now, we made a
23 choice when we revised this ISG not to include
24 guidance for inspections, right, in this ISG.
25 Now we do have guidance for inspection in

1 our standard review plan, in Chapter Seven. And that
2 was updated as a result of the Oconee experience and
3 our inspection experiences.
4 So, I'm not here to say that it's perfect.
5 And that we've solved this problem. Okay?
6 But we have made a lot of improvements.
7 MEMBER SKILLMAN: What I hear you say is,
8 it's sufficient for what you've learned to date. It
9 can always be improved for the --
10 MR. STATTEL: Correct.
11 MEMBER SKILLMAN: For this time in
12 history, it is sufficient to move ahead.
13 MR. STATTEL: That is correct.
14 MEMBER SKILLMAN: Okay. Thank you. Thank
15 you.
16 MR. DARBALI: Next slide. So the next two
17 slides are going to be focusing on the specifics of
18 the new Alternate Review Process.
19 This slide summarizes the characteristics
20 of a license amendment request using the new Alternate
21 Review Process.
22 CHAIRMAN BROWN: Let me stop you for a
23 moment. We're due for a break at 10:15, in five
24 minutes.
25 There's several slides associated with the

1 Alternate Review Process that we're going through.
2 So, my suggestion is that we go ahead and take our
3 break now.
4 Is that acceptable so that we can have
5 continuity of this discussion?
6 MR. DARBALI: Sure.
7 CHAIRMAN BROWN: So, with that in mind, we
8 will break for 15 minutes. So we are in recess for --
9 until 10:25. By that clock as Mr. Skillman would say.
10 (Whereupon, the above-entitled matter went
11 off the record at 10:09 a.m. and resumed at 10:29
12 a.m.)
13 CHAIRMAN BROWN: Okay. We are going to be
14 back in session. Samir, have at it.
15 MR. DARBALI: Thank you sir. We're on
16 Slide 17. So Slide 17 and 18 will be talking about
17 some of the specifics of the ultimate review process.
18 This slide summarizes the characteristics
19 of the license amendment request using the new
20 Alternate Review Process. The license amendment
21 request would provide the necessary and sufficient
22 design information to demonstrate regulatory
23 compliance.
24 License amendment requests would describe
25 the licensees' vendor oversight plan as we discussed.

1 The vendor oversight plan ensures the vendor executes
2 the project consistent with the license amendment
3 request. And consistent with the requirements of the
4 2015 version of NQA 1.
5 The license amendment request would
6 include appropriate commitments to complete plant
7 specific action items that are included and referenced
8 in the platform topical report. And the license
9 amendment request would include appropriate
10 commitments to complete life cycle activities under
11 the licensee's QA Program.
12 CHAIRMAN BROWN: Okay. Let me ask a
13 question. The Alternate Review Process uses an
14 approved topical report.
15 MR. DARBALI: Correct.
16 CHAIRMAN BROWN: Tier 1 uses an approved
17 topical report. So, you all make the decision, right?
18 As to what review process -- I mean, this is not a
19 licensee issue.
20 This is your process. What tells -- how
21 do you make the decision as to which process you're
22 going to use?
23 MR. DARBALI: So, it's a joint decision.
24 CHAIRMAN BROWN: Other than the factor --
25 I mean, is there something -- I understand the factor

1 acceptance test part of it.

2 MR. DARBALI: Right. It's a joint

3 decision. During Phase Zero or pre-application

4 meetings, the licensee would come in and say, this is

5 the type of modification we want.

6 And they'll say, this is the type of

7 review process we want. They might say we want to do

8 an ultimate review process because we would like to

9 get that safety evaluation license amendment before we

10 request more funding for implementation and test

11 activities.

12 So, the licensee would be the one

13 proposing the process. The staff would be fine with

14 either process as long as the requirements for using

15 the process are met.

16 CHAIRMAN BROWN: Okay. So it's a joint

17 decision to try to suit their desires if it's

18 appropriate. If you dealt it -- if you deemed it not

19 appropriate you --

20 MR. DARBALI: Correct.

21 CHAIRMAN BROWN: You would say no.

22 MR. STATTEL: Well, let me give you some

23 examples of situations that I expect to encounter.

24 So, one example would be a licensee has basically

25 completed, they've built the system.

1 They have it completed. The factory test
2 is complete. And now they decide they want to install
3 it in their plant. So they come for a license review.
4 So during that pre-application meeting, it
5 would not make sense for them -- they have final
6 products. Right? So they have a completed design.
7 They have final products. It really
8 doesn't make any sense to use an alternate process in
9 that case, because we can simply review the final
10 product.
11 That would be one scenario.
12 CHAIRMAN BROWN: That's an LAR.
13 MR. STATTEL: Right. As part of the
14 license amendment they would submit, here's the final
15 product. Okay. That's it.
16 Another applicant might come in and let's
17 say they don't have funding, or they don't have
18 approval for the complete implementation of the
19 project. So they do -- they basically contract with
20 a vendor.
21 They develop the design without building
22 any hardware or implementing the design. And before
23 they commit the rest of the resources to do the
24 implementation, they'd like to have NRC approval as a
25 means of mitigating risk.

1 So then an Alternate Process makes a lot
2 of sense to them. Because they can submit that -- the
3 higher level design, architecture. Right? Design.
4 Without having tested it. Without having
5 built it. Without having implemented that design.
6 They could submit that to the NRC, get an NRC approval
7 with commitments to complete the implementation before
8 the license amendment goes into effect.
9 And in their case, an Alternate Review
10 Process might make a lot of sense. Now, a couple of
11 other factors in the decision would be now in our
12 experience between completion of design,
13 implementation, building, all the activities that lead
14 up to a factory acceptance test, it is not uncommon
15 for design changes to be made.
16 Okay? As a matter of fact I for one have
17 never seen a design go from completion design to
18 completion of a factory test without changes. And
19 sometimes they're minor.
20 Sometimes they're significant. You know,
21 because it's as you implement, you discover things.
22 You find out system behaviors that you were not aware
23 of.
24 So these changes are going to take place.
25 Right? So, a licensee that chooses a Tier 1 process

1 might want those changes to be under the purview of
2 the NRC. They want the NRC to be seeing these changes
3 as they occur prior to issuance of the license
4 amendment.
5 That way the license amendment covers all
6 of those changes. There's no subsequent license
7 amendment.
8 Now another licensee that chooses to use
9 an Alternate Process, they get the license amendment
10 early. But, that whole window up to the factory test,
11 those changes, those changes are either going to have
12 to be processed through 50.59 evaluations and their
13 change processes.
14 And I understand the difference. Okay?
15 And/or there could be subsequent license amendments.
16 So an amendment to the amendment. Okay? To address
17 those changes. Because there's a distinct possibility
18 of that occurring.
19 But, that licensee may value having that
20 license amendment in pocket. Right? Having it
21 approved and take the risk of having to come back in
22 for an amendment if a significant change is required
23 prior to putting that system into operation.
24 So, those are the kind of scenarios, kind
25 of the things that would feed into the decision of

1 which process to use.

2 CHAIRMAN BROWN: Okay. Take -- go back to

3 your first one. The one where they have a complete

4 design. They've designed it, built it, tested it.

5 They come in for a license amendment.

6 MR. STATTEL: Yes.

7 CHAIRMAN BROWN: A request. Which -- is

8 that a Tier 1?

9 MR. STATTEL: Typically we see those as

10 Tier 1s.

11 CHAIRMAN BROWN: Okay.

12 MR. STATTEL: We actually do see a lot of

13 those type of amendments. So, an example would be

14 implementation of an NUMAC system on a power ranked

15 neutron monitoring system.

16 CHAIRMAN BROWN: Um-hum.

17 MR. STATTEL: Well, the -- obviously it's

18 referencing an approved topical report. They are the

19 15th plant to do this same modification. They're not

20 altering it from what other plants have done.

21 Therefore, it makes a whole lot of sense

22 -- I mean, they have a complete design. It makes a

23 whole lot of sense to use the --

24 CHAIRMAN BROWN: Okay.

25 MR. STATTEL: The Tier 1 process.

1 CHAIRMAN BROWN: Now, if the licensee came
2 in with a new reactor trip system and safeguard system
3 upgrade completely designed, tested, all the i's are
4 dotted and all the t's are crossed, is that a Tier 1
5 Review?
6 MR. STATTEL: I would expect that to be a
7 Tier 1 Review.
8 CHAIRMAN BROWN: Okay. And again, I get
9 back to my question about now that I've got a system
10 design, an architecture --
11 MR. STATTEL: Well, I was assuming that
12 you had a completed system design when you mentioned
13 that case.
14 CHAIRMAN BROWN: Well yeah. They did it.
15 But you didn't know it. They just finished it.
16 MR. STATTEL: Right.
17 CHAIRMAN BROWN: And now they come to you,
18 here's our complete -- we're going to replace it all.
19 We're going to rip out all the old stuff.
20 Here's the new architecture. Here's the
21 new stuff. Here's the network we're installing. All
22 this other kind of stuff. We think it's the greatest
23 thing since sliced bread.
24 And now is that a Tier -- approved topical
25 report. No changes. They used the software or

1 whatever the programming standards are. All that kind
2 of stuff.
3 And they now want their license amendment
4 approved. And it's a Tier 1. How do you then make a
5 judgment -- I'm getting back.
6 I'm obviously mouse-milking my comment on
7 architectures here. Because I would get the
8 implication that there is no architecture discussion.
9 Is that part because they're replacing the entire
10 combination of the RTS and ESFAS systems?
11 MR. STATTEL: Well, let me say
12 unequivocally, the architecture is in the purview of
13 the --
14 CHAIRMAN BROWN: And I'm trying to figure
15 out where that is. All right. I've just --
16 MR. STATTEL: And we've received that
17 comment from other --
18 CHAIRMAN BROWN: I tried to use your
19 example, okay, to make the --
20 MR. STATTEL: We've received that comment
21 from other sources too. So, we intend to include
22 that.
23 CHAIRMAN BROWN: Okay.
24 MR. STATTEL: It was not -- there was no
25 intention to omit architecture evaluation from any of

1 these review process.

2 CHAIRMAN BROWN: Okay. I asked this

3 question relative to how you decide intentionally, so

4 I could try to get a feel for the thought process.

5 MR. STATTEL: Okay.

6 CHAIRMAN BROWN: So, based on your earlier

7 answer I presumed that was the answer. It's just a

8 matter of how the ISG or how your process gets that

9 actually done.

10 Based on if I was a licensee it says hold

11 it, I'm only -- this is -- I've followed your ISG.

12 And therefore, why are you pulling the string on me

13 somewhere else?

14 MR. STATTEL: So, I view these two

15 different processes as just having different

16 perspectives on the same activity. So, in the

17 Alternate Review Process, you're kind of reviewing it

18 with the perspective of you see the design.

19 You see what's on paper. But it hasn't

20 been implemented yet. And you know that there's going

21 to be a lot of activities done in the future.

22 So you want to have some assurance that

23 those activities will be performed correctly. You

24 want to have commitment from the licensees. You want

25 to have conditions if necessary, to make sure that

1 that end product is going to be what it needs to be to
2 meet regulations.
3 The perspective of the Tier 1 Review is
4 different. Because we don't issue the license
5 amendment until after the design is complete,
6 implemented, tested. Okay?
7 So, in this case what got you to that
8 point is less important. I'm not going to say it's
9 not important. But the quality of your planning and
10 requirements is less important than the final product.
11 So in a Tier 1 Review, we see the final
12 product. And you can simply concentrate your
13 evaluation efforts on that final product. And make a
14 determination that that final product meets the
15 appropriate regulations.
16 CHAIRMAN BROWN: I got that. And I guess
17 to reiterate, it's not -- it was -- it's not clear
18 from looking at that that the vendor -- or the
19 licensee would expect to see, since it's already
20 completed, that that first part of the complete design
21 and its architecture was not included based on the way
22 the ISG is framed right now.
23 And you said you're going to fix that.
24 And so I will take you at your work. But I just
25 wanted to clarify all of our earlier, a little bit

1 more amorphous discussion, with the very clear
2 examples as you have stated just now.
3 Okay. Yeah, Myron?
4 CONSULTANT HECHT: I have a question with
5 respect to NQA 1, which I admittedly have not read.
6 And does it address FPGAs and programmable devices in
7 general in the same way it does for software?
8 MR. DARBALI: I do not -- it's been a
9 while also since I've read it. So, I'm not familiar.
10 I don't think it specifically mentions
11 FPGAs. But it might be neutral to this device.
12 CONSULTANT HECHT: Okay. Well, I guess
13 the question is, is there the possibility of a hole if
14 software is mentioned? But, you know, FPGAs and all
15 of those VHDL-based devices are not.
16 CHAIRMAN BROWN: That's a soft -- that's
17 a development tool for programing, --
18 CONSULTANT HECHT: Right.
19 CHAIRMAN BROWN: FPGA, that's what you're
20 referring to, how does that work?
21 CONSULTANT HECHT: It could be. Or it
22 could be considered well, this is not software at all.
23 This is --
24 CHAIRMAN BROWN: Right. Well, it's not
25 theoretically hardware. But it's designed for soft --

1 programed as software to burn all the little tool.
2 MR. STATTEL: Our view and our policy has
3 always been that FPGA is developed using software
4 tools. We do have guidance and we do perform
5 evaluations of those tools.
6 So, I've been involved with reviews of
7 FPGA and CPLD-based platforms that don't use
8 microprocessors. The technicality that software is
9 not running during operation of the system is really
10 not relevant.
11 We consider the soft -- we consider the
12 development of logic, the tools used for that
13 development to be as critical as safety related
14 software would be in a microprocessor.
15 What we've seen in industry is -- so for
16 example, IEEE 7-4.3.2 was originally written from the
17 perspective of software for computer-based systems.
18 And that same guidance is now applied,
19 they've basically repurposed that standard or rescoped
20 that standard to include all digital devices, all
21 programmable digital devices.
22 So, although there are differences in the
23 technology and how it's implemented, we consider -- we
24 consider the fundamental principles and the guidance
25 in those documents to be applicable.

1 Even if it's just scope for software, we
2 do apply those to FPGA-type devices.
3 CONSULTANT HECHT: Okay. You -- when you
4 first started talking, you said our regulations cover
5 software tools. Then later on you expanded that to
6 really refer to what I would call the models that end
7 up being burned into the hardware.
8 MR. STATTEL: Yes.
9 CONSULTANT HECHT: You know, they were --
10 that register transfer logic leading to the synthesis.
11 It covers also the RTL-based documentation and
12 analysis as well.
13 So that's subject to that same kind of
14 thing?
15 MR. STATTEL: So, when we evaluate a CPLD
16 or an FPGA-based application, we understand that the
17 logic that's burned into those chips is -- we don't
18 treat it any differently then software --
19 CONSULTANT HECHT: Okay.
20 MR. STATTEL: In a microprocessor. So,
21 when we evaluate those, we look for information that's
22 equivalent to what a software design description, what
23 a software requirement's documentation would be.
24 So we look for the equivalent
25 documentation to support correct implementation

1 verification. We also apply the same principals of
2 verification and validation.
3 So, we apply the IEEE 1012 concepts to
4 those systems as well.
5 CONSULTANT HECHT: Okay. So, the point
6 that you have up there about NQA 1, you would also
7 include 7-4.3.2 in that? Is that when you say the
8 characteristics of an Alternate Review Process?
9 MR. DARBALI: Right. When the licensee
10 uses the Alternate Review Process, and you can see it
11 in Section D.6, I believe, is a mapping of the IEEE
12 603 and 7-4.3.2 sections.
13 So the licensee is expected to address
14 those sections. The vendor oversight plan is more of
15 how the licensee makes sure the vendor -- how the
16 licensee is performing that oversight that the vendor
17 is implementing those activities.
18 CONSULTANT HECHT: I see. Okay. Thank
19 you.
20 MR. DARBALI: Yes.
21 CONSULTANT HECHT: That's a conclusion.
22 CHAIRMAN BROWN: Dinesh, did you want to
23 say something?
24 MR. TANEJA: No. I was just going to
25 point out that NQA 1 is an industry standard nuclear

1 quality assurance. It's produced by ASME.
2 And it's endorsed by the NRC for
3 implementing the 10 CFR Appendix B quality assurance
4 program. Subpart II.7 specifically addresses in that
5 standard in a hard to do quality assurance of the
6 software-based, you know, whether it's for analysis or
7 whether it's for, you know, equipment in the plant.
8 So, the Appendix B programs that each of
9 the licensees or the applicants have, usually are
10 using NQA 1 of the way of implementing their quality
11 assurance program.
12 So, give you an example, NuScale has an
13 FPGA-based, you know, protection system. Their
14 computer program is also based on NQA 1.
15 What they have done, see, what they've
16 created is a daughter standards. You know, and I
17 think that's what we've seen.
18 They call them software quality assurance
19 programs, which are daughter standards that come out
20 of their NQA 1, which specifically detail out the
21 technology and how they're going to meet the overall
22 system requirements that are laid out in Subpart II.7.
23 So that's really the framework of how that
24 works. Just wanted to give you that insight since you
25 asked the question.

1 CHAIRMAN BROWN: I wanted to -- Dinesh
2 referenced NuScale. And I -- if anybody wants a
3 reference to NuScale right now, you've got to be
4 careful what you -- we have some considerable
5 restrictions on what we can address or not address in
6 an open meeting.
7 MR. TANEJA: Okay.
8 CHAIRMAN BROWN: So, okay, I didn't hear
9 anything that was contrary to that. I just want to
10 warn anybody that if you intend to use that as an
11 equivalency or as an example, there are some very
12 severe consequences if we --
13 MR. TANEJA: Right. I understand.
14 CHAIRMAN BROWN: Bill or happen to touch
15 into closed meeting type issues. Okay?
16 MR. TANEJA: Okay.
17 CHAIRMAN BROWN: All right. Thank you.
18 That was a nice reminder.
19 CONSULTANT HECHT: Just following up on
20 that point --
21 CHAIRMAN BROWN: Well, don't ask him
22 anything about whatever.
23 (Laughter.)
24 CONSULTANT HECHT: I will not ask him
25 that. I only know how to say FPGA and CPLD.

1 CHAIRMAN BROWN: Okay.

2 (Laughter.)

3 CONSULTANT HECHT: So, I guess there's

4 just a question of how the standards are interpreted.

5 MR. TANEJA: Right.

6 CONSULTANT HECHT: If software is really

7 intended to refer to any description of a logical

8 language, then I guess we're covered.

9 But, I don't know if the interpretation

10 that's being used here and by the licensees would say

11 no, no, software is what you write in C or Ada. But

12 it's not what you write in Verilog or VHDL.

13 MR. TANEJA: You know, like I said, you

14 know, their daughter standards that most of the

15 licensees and applicants that we have seen, you know,

16 get into that level of detail. Based on the

17 technologies that they have selected and how it mats

18 to their quality assurance program.

19 They -- each of the licensees and

20 applicants, you know, have a quality assurance program

21 that they have to produce the products under. Okay.

22 So this specific Subpart deals with just,

23 you know, the software related products that need to

24 be, you know, how they need to meet the intent of

25 that, you know, overarching quality assurance program.

1 So, you know, so yeah, we have seen, you
2 know, they call them different names. But typically
3 it's software quality assurance program, which is a
4 substandard or a tiered down version of implementing
5 the overarching requirements of the quality assurance
6 programs.
7 So that's a licensing commitment. That's
8 really where it comes from.
9 MR. DARBALI: So, when -- if a licensee or
10 depending on how a licensee, a particular licensee
11 would treat an FPGA or a CPLD, would be addressed in
12 either the pre-application meetings, or during the
13 review.
14 But also remember, they're using a
15 preapproved platform. So those discussions already
16 occurred during the platform review.
17 CONSULTANT HECHT: Well, it's possible
18 that that platform might not have -- might not specify
19 very much about the FPGA. It's possible.
20 MR. DARBALI: The staff would have
21 performed that review. So, if a platform contains
22 FPGAs such as several platforms the staff has
23 reviewed, the requirement specification, design
24 specification just would have been part of the
25 platform review.

1 CONSULTANT HECHT: Okay. So, I guess it's
2 been implied but not clearly stated that when you're
3 talking about an oversight process that whether it's
4 for software or whether it's for FPGAs, the same NQA
5 1, Part II, Subpart II-7 applies.
6 MR. DARBALI: Correct.
7 CONSULTANT HECHT: Okay.
8 CHAIRMAN BROWN: Are we ready?
9 CONSULTANT HECHT: I'm ready. Thank you.
10 CHAIRMAN BROWN: Okay. Go on Samir.
11 MR. DARBALI: Next slide. As mentioned in
12 a previous slide, the Alternate Review Process relies
13 on the license amendment request containing licensing
14 information and additional regulatory commitments to
15 implement remaining development basis by the
16 licensee's QA Program after the license amendment is
17 issued.
18 The NRC staff may likely translate some of
19 the regulatory significant commitments into licensed
20 conditions as part of the approval. An example of
21 this could be to perform, you know, factory acceptance
22 testing.
23 I will now turn it over to Rich who will
24 provide a description of the ISG-06 Revision Two
25 structure.

1 MR. STATTEL: Okay. Thank you Samir. So,
2 at this point, I'd really like to get in -- under the
3 hood and look at what's inside ISG-06. And talk a
4 little bit about what it's content is. Where the meat
5 of this document is.
6 The figure that you see here is an
7 illustration. And I'm going to go back and forth
8 between this figure and the enclosure. Because the
9 enclosure also provides a pretty good outline of
10 what's in the procedure itself.
11 So it illustrates the new structure of
12 ISG-06. So, because the document will now provide
13 guidance for two different regulatory evaluation
14 processes, it contains sections that are common to
15 both processes, as well as sections that are unique to
16 each of those processes.
17 So, for example, Section D.1 provides
18 guidance for evaluating and describing the system
19 being modified. Since the evaluation is the same,
20 regardless of the type of review being performed, the
21 team saw no need to duplicate this guidance.
22 So, one of our objectives was to remove
23 duplication in the guidance. That was one of our
24 charter objectives.
25 Therefore, Section D.1 is used for both

1 Tier 1, 2, and 3 process, as well as for the Alternate
2 Review Process. Section D.2 on the other hand
3 provides guidance for system architecture that was
4 intended right now, we're reconsidering this now, but
5 it was intended to be unique to the Alternate Review
6 Process.
7 So it was written with the idea of the
8 Alternate Review Process in mind. And thus, is it
9 only references Alternate Review Process Tables of
10 Enclosure B.
11 Now conversely, Section D.9 provides
12 guidance for evaluating the design products that would
13 be available -- that would not be available for the
14 Alternate Review Process. Therefore, Section D.9 is
15 only referenced in the Tier 1, 2 and 3 processes.
16 Now if you go to the next slide. So this
17 is really just the Enclosure B tables that we've
18 already talked about.
19 In the original version, I really want to
20 talk -- explain how we got to this place. In the
21 original version of the ISG, these tables were
22 probably three times longer. Okay?
23 It doesn't mean we're only reviewing a
24 third of the information that we were before. Right?
25 We're really not -- the amount of information is

1 really not the point of this table.

2 We're really trying to establish pointers

3 from here to the relevant sections of the document.

4 We had no intention of omitting review areas such as

5 architecture from the Tier 1 process. I'll just make

6 that clear.

7 Now, in the process of basically

8 consolidating a long table into a short table, we

9 choose topics, we merged topics together. We choose

10 topics -- there were some decisions made on what

11 topics were the most important ones and what we would

12 use as the headers.

13 Once we did that of course we're breaking

14 a lot of the pointers to the sections in the standard

15 itself. So, we had to reestablish those pointers.

16 And that's the -- the pointers are what

17 you see in parenthesis here, D.2, D.4, and so on and

18 so forth.

19 So, I think we're -- based on the feedback

20 we've received from various places, and including

21 yourself, I don't think we've -- I think there's some

22 pointers that we may have missed. Okay.

23 So, I was looking -- while Samir was

24 talking, I was looking at an example of this. And I

25 choose architecture of course.

1 So in system architecture, if I look at
2 the original ISG, the Revision One of ISG,
3 architecture was really covered by four different
4 topics. So there were four different line items in
5 that table.
6 And what happened was, of course, we
7 merged some together. And we ended up with just one
8 line item.
9 And the pointer essentially got broken
10 because it had pointed to the system description.
11 Okay.
12 And sure enough, in the system description
13 there is guidance for what needs to be provided and
14 evaluated for -- in regard to architecture. So the
15 system description needs to describe the architecture
16 that's being implemented in the license amendment.
17 So, again that was the reason why we
18 didn't include the Xs in that area, in that particular
19 area here. I think we are going to be -- revisit that
20 and make sure we do that.
21 Now the other thing I'd like to point out
22 is this is just guidance. Okay. We can move these Xs
23 around. We can add Xs. We can take Xs away,
24 depending on the specific application we're getting
25 and what we feel is necessary.

1 So it is guidance. You see the waterfall
2 effect on the left side in the table here. And this
3 is really pointing out to how the ISG is implementing
4 these different purviews or different perspectives
5 that we have with the various Tier processes.
6 So, as an example, if you look at item 1.2
7 in this diagram, you see it points to only the
8 Alternate Review Process. And it talks about software
9 planning and processes. Okay.
10 It's not that these aren't important.
11 But, if we're performing a Tier 1 review and we're in
12 phase two, and we receive completed design, we feel
13 that it's more important to concentrate your review
14 effort on the completed design then the plans that got
15 you to that point.
16 It's not out of scope, I mean, the
17 reviewer always has the prerogative to go back and
18 look at those plans. But, we've had cases in the past
19 where we see some inadequacies in the plans, and we
20 write RAIs.
21 And the applicant responds and changes
22 their plans. But they don't change their products.
23 Because the products had been developed before that.
24 So changing plans after the fact really
25 doesn't impact safety. So, we felt it was more

1 important to emphasize the output product in the case
2 of Tier 1, 2, and 3, and put a bigger emphasis on
3 software planning and processes in the Alternate
4 Review Process.
5 And this is -- this is how -- this table
6 really illustrates how that's done within the ISG.
7 CHAIRMAN BROWN: I don't disagree with
8 you. I mean, I just -- with an approved topical
9 report theoretically, if you referred that you've
10 already reviewed and understood how they got to where
11 they were in the first place.
12 So you're just not retreading old ground
13 for the most part. I'm not saying there aren't
14 probably some outliers or some exceptions that you
15 might run across.
16 But by in large, haven't you --
17 MR. STATTEL: And again, we're trying to
18 write a process that covers a large spectrum of types
19 of systems.
20 CHAIRMAN BROWN: Yeah. I understand that.
21 MR. STATTEL: What you just said makes a
22 lot of sense for a system like a pneumatic PRMS.
23 CHAIRMAN BROWN: Exactly.
24 MR. STATTEL: Because I know a lot about
25 that pneumatic PRMS by reading the topical report, but

1 if I read the Tricon topical report, I don't even know
2 what kind of system it's going to be. I don't know if
3 it's going to be an RPS. I don't know if it's going
4 to be a PAMS. I don't know if it's going to be a
5 PRMS.
6 (Simultaneous speaking.)
7 MR. STATTEL: I have no idea what it's
8 going to be, right? We use the term, "It's a box of
9 Legos." I don't know what they're going to build with
10 that box of Legos.
11 So in that case, and these topical reports
12 are all over the spectrum. On the extreme left would
13 be the pneumatic systems which we know exactly what
14 they're going to be, and on the right would be HFC,
15 Tricon, which we have no idea what these systems are
16 going to be used for in the future.
17 So, and again, we're trying to write
18 guidance that covers all of them and there's ones that
19 are in the middle too. So again, it's guidance we can
20 tailor, right?
21 So I would say there's also differences in
22 the topical reports with regard to what processes are
23 evaluated during the LTR review. So in some cases,
24 some vendors have submitted very detailed software
25 development processes or guides, right, as part of a

1 licensing topical report.

2 So they have a software program manual

3 that really gives us a good view of what processes are

4 going to be used to develop applications. Other

5 vendors don't submit that, so we have no idea.

6 So if a vendor has an approved software

7 program manual, I would say I don't need an X in the

8 area of reviewing, planning, and processes, but if a

9 vendor hasn't submitted that, if I look at the topical

10 report, I really don't - it hasn't been evaluated,

11 then, yeah, I'm going to add an X in there.

12 CHAIRMAN BROWN: Whether it's a Tier 1,

13 whether it's an AR or whether it's a Tier 1, 2, or 3.

14 MR. STATTEL: I don't even care what kind

15 of tier it is.

16 CHAIRMAN BROWN: Exactly, okay.

17 MR. STATTEL: So the point is this is a

18 guide. There's no way this is going to fit every or

19 actually any one application. It really does need to

20 be tailored and customized for the applicant.

21 Now, one of the lessons we have learned

22 and one of the real benefits of ISG-06 that we've

23 found over the years is this table itself, this

24 Enclosure B table, because this table, and Diablo

25 Canyon was the first to do this, they essentially

1 lifted this table out of the ISG, put it into a
2 spreadsheet format and created a matrix, an ISG-06
3 matrix, and they laid it out phase one, phase two, and
4 they put the appropriate pointers to their specific
5 documents.
6 And in their table, they pointed - you
7 might recall. We discussed this during the Diablo
8 Canyon evaluation. They pointed to the ALS vendor for
9 how those areas were addressed in that area in that
10 part of the system and they pointed to Tricon for the
11 same areas, right?
12 So they were able to use this enclosure in
13 a matrix format to provide us a very clear map of how
14 all of the requirements were being satisfied in that
15 application, and I expect that to continue.
16 We've really consolidated this table.
17 We've got it a lot shorter, but again, it's not that
18 we're reducing the amount of information necessarily.
19 We're trying to avoid submittal of information that we
20 don't use in an evaluation because we've had that
21 problem in that past. So we are really trying to
22 concentrate on what's important here and do the right
23 amount of evaluation at the right level.
24 So I would say regardless of the tier, or
25 alternative review process or normal review process,

1 we want this guide to get the evaluators and the
2 licensees to concentrate on what's important and
3 what's necessary to support the safety conclusions of
4 that system.
5 CHAIRMAN BROWN: Okay, I don't disagree
6 with what you're saying.
7 MR. STATTEL: Okay.
8 CHAIRMAN BROWN: I appreciate that. The
9 one point -
10 MR. STATTEL: So at this point, I really
11 am kind of open to any questions about the detail.
12 CHAIRMAN BROWN: The one point I would try
13 to make is that, you know, we, as a Committee, we have
14 some oversight requirements that we're required to do
15 by law and in accordance with the FACA requirements,
16 as well as anything else in terms of what we provide
17 to the Commissioners.
18 And fundamentally, the primary area where
19 we provide or can gather, make ourselves feel most
20 comfortable is not necessarily trying to understand
21 every secure development and operational environment
22 nuance, or every software design document, or every,
23 you know, programming technique that somebody may use.
24 If it hasn't been noticed, our primary
25 emphasis has been on the architectures and how those

1 defensive architectures are constructed to ensure that
2 if something doesn't get done exactly as we expect it
3 to be done, that there are some safeguards in the
4 architecture that allow the system to perform
5 properly.
6 And that's been the primary focus of our
7 Committee, but the subcommittee and the
8 recommendations at least we've made to the full
9 Committee in all of the new license, you know, new
10 design developments, the new plants, as well as the
11 plant upgrades of which the Diablo Canyon upgrade is
12 the latest or the most visible one, and so that's a
13 little - that's one of the basic reasons for the,
14 beating this particular horse even more dead than I
15 could possibly make it.
16 My comment is not critical because I
17 understand what you're saying, but in my personal
18 view, and hopefully the full Committee will agree,
19 that we need to ensure that when we review these
20 upgrades, total RTS and safeguards upgrades, that the
21 information has been developed and evaluated and can
22 then be presented to us so that we can look at it.
23 We do depend on you for these others
24 because it's obvious we're not going to go through
25 every one of those ourselves. We are not experts in

1 each and every one of those areas, so that's why the
2 emphasis I've made in this particular meeting to
3 ensure -
4 The enclosure is very valuable. I looked
5 at this. I went back and looked at the Rev 1
6 enclosure. I also looked at the Rev 1 words. It's
7 about twice the size in terms of words.
8 MR. STATTEL: That's correct, yes.
9 CHAIRMAN BROWN: And it's way too wordy.
10 You've kind of subsumed it down to, "Here's what you
11 ought to be looking at, not telling you again what we
12 have in those other documents and provided."
13 MR. STATTEL: We agree, and that was also
14 one of our charter goals was make it more
15 understandable, cut to the chase, emphasize what's
16 important, and that's really what we've tried to do
17 here, so I agree with everything you've said.
18 CHAIRMAN BROWN: Okay.
19 MR. STATTEL: I would also like to point
20 out that there's a couple other changes to this
21 enclosure. The original document had additional
22 tables. It had a table for, that provided guidance on
23 what to audit.
24 CHAIRMAN BROWN: Yes.
25 MR. STATTEL: Okay, we removed that. We

1 just felt it was -

2 CHAIRMAN BROWN: You can audit when you

3 want to.

4 MR. STATTEL: We can audit when we want,

5 right? Exactly, so really everything is fair game for

6 audits, and we've done enough audits now that we have

7 a pretty standard process for identifying what areas

8 to concentrate during those audits, so we didn't feel

9 it was really being helpful in this enclosure.

10 The other area was for inspection, so we

11 made a decision. We received guidance from the

12 Steering Committee that this document would not

13 provide guidance for performing inspections, so those

14 tables were removed. It's really, this procedure

15 really ends at the time that we issue the license

16 amendment.

17 We do have guidance for providing input to

18 inspection plans, but it's not in here. It would be

19 in Chapter 7 of the SRP, so we kind of reduced the

20 scope of the ISG in that respect, okay?

21 MEMBER SKILLMAN: Rich, let me ask this.

22 While you've been talking, I've been going through

23 Appendix B, going back to the first paragraphs of the

24 ISG. As I stated an hour or two ago, at least my view

25 is this ISG is really about changing your license.

1 That's why it's a license amendment request.
2 MR. STATTEL: That's correct.
3 MEMBER SKILLMAN: The next tier down in my
4 mind is facility modification, documentation, and
5 hardware. The next tier down in my mind is
6 configuration management and configuration control,
7 paper, and hardware. So I'm kind of going down the,
8 receiving this on the plant side and what I'm doing.
9 So I get into the ISG. The only place
10 configuration management is described is in D.4.2.5,
11 and there it only applies to software. Here's where
12 I'm going. Appendix B, 10 CFR 50, good old criterion
13 three, it's the number one snare for people at the
14 plant, design control. Why isn't there a hardware
15 configuration control chapter in your ISG?
16 Certainly you've got the software side,
17 but as Myron said a little while ago, there are
18 hardware implications, and some of the changes that
19 licensees will make, they'll keep part of the original
20 hardware and they'll change pieces such that there may
21 not be compatibility, or if there is, that
22 compatibility should be demonstrated.
23 So my question is should there be among
24 your matrix here another line item that really speaks
25 to configuration control and configuration management

1 insofar as this is a change to your facility?

2 MR. STATTEL: Well, so this kind of goes

3 back to the original development of the ISG. It

4 really was trying to address specific technology,

5 digital technology, and the viewpoint at that time was

6 that we're really concerned about software and we want

7 to make sure that software configuration management is

8 maintained. We had cyber security concerns that we

9 felt needed to be addressed and that's closely tied to

10 that.

11 So you are correct. The emphasis is on

12 software, but I would also point out that we're

13 referring to IEEE Standard 603 and there is a matrix

14 included. Chapter D.6 includes IEEE-603 which is

15 technology neutral.

16 So the idea of the hardware configuration

17 management, essentially we didn't - we kind of felt

18 that was out of scope for this particular guide other

19 than the fact that the 603 core requirements, because

20 that's the true regulatory requirements, they were

21 still included as part of that.

22 And also keep in mind this ISG is intended

23 to be used along with, not in lieu of, Chapter 7, our

24 standard review plan.

25 MEMBER SKILLMAN: Yes, sir.

1 MR. STATTEL: So we also, I would also
2 refer back to Chapter 7 which has guidance in this
3 area as well.
4 MEMBER SKILLMAN: I was just thinking of
5 the case where you have an analog system that -
6 MR. STATTEL: I mean -
7 MEMBER SKILLMAN: For having, you know, if
8 someone says, "We're going to keep this," and it's all
9 kinds of wind-up and wind-down RC circuits and that
10 type of thing, and then you've got some digital over
11 here, and if they're communicating with each other -
12 MR. STATTEL: Right.
13 MEMBER SKILLMAN: - the digital stuff is
14 virtually instantaneous and the analog stuff takes as
15 much time as the magnets require.
16 MR. STATTEL: And there's crossover too
17 because that in FPGA systems, really configuration
18 management is a hardware configuration management
19 issue because you're moving hardware around when you
20 install an APROM or when you install an FPGA. So in
21 our evaluations, we try to understand the processes
22 for maintaining configuration management.
23 We typically have application specific
24 action items for the licensees to have some way of
25 ensuring that what was tested and deemed acceptable at

1 the end of factory test is what is in fact being
2 installed in the plant, so they have the processes
3 available.
4 MEMBER SKILLMAN: Then I would simply say
5 that the introduction kind of provides the licensee
6 with the idea this is about safety-related digital
7 instrumentation and control equipment, when in reality
8 it's really about safety-related digital
9 instrumentation and control equipment modifications
10 mostly having to do with software.
11 MR. STATTEL: That's true. It's a
12 document where, you know, it has a lot of potential to
13 have a much larger scope. We've had this come up in
14 some of our other comments we've received in areas
15 such as human factors engineering, safety systems. So
16 there are implications, right?
17 So we like to say that, you know, issuing
18 this ISG really improves our efficiency in performing
19 evaluations of these systems, but the reality of it is
20 there are things that are outside the scope of this
21 ISG that we don't know what that's going to be and it
22 could go to other review areas. It could be
23 problematic in other areas.
24 So the other thing you'll notice is if, or
25 you may have noticed, is in the old tables, we had

1 actually some time frames for Tier 1, alternate, or
2 Tier 1, Tier 2, Tier 3 reviews, so we had estimate
3 time frames, that they would be completed in a certain
4 amount of time, and phase two submittals are submitted
5 six months prior to the issue of the license
6 amendment.
7 We consciously chose to eliminate those
8 time frames because those are the types of things that
9 would easily be blown if there's facets of the design
10 that are not covered by this ISG.
11 MEMBER SKILLMAN: Fair enough. I would
12 just make one last point and it was communicated
13 earlier. When a licensee embarks on a license
14 amendment to accomplish this change, this is normally
15 an activity that takes two or three fuel cycles, so
16 this is a four, five, six, eight-year marathon for
17 these licensees.
18 And I searched through the ISG for time,
19 T-I-M-E, and there isn't anything in there that
20 recognizes that part of the defense perhaps for your
21 alternate path needs to recognize or at least is based
22 upon the recognition that it takes a long time for
23 this to mature to where it is actually implemented in
24 hardware.
25 And that kind of gives certification to

1 your comment that you've never seen one that doesn't
2 get changed in the course of time because it does.
3 People learn and they change, but it would seem that -
4 I don't know if that needs to be included.
5 Maybe it's intuitive to all of the
6 individuals that work in this part of the technology,
7 but to those who don't, it might be an ah-ha when they
8 realize this isn't something that happens by going out
9 to a vendor and buying a super wham thing to plug in.
10 This is a very disciplined, long ordeal.
11 It's very complicated. It's very
12 expensive, and it has all of the elements of Appendix
13 B to 10 CFR 50, configuration management,
14 configuration control, and without all of those
15 pieces, this really doesn't occur.
16 MR. STATTEL: Well, your point is well
17 taken, and I've had the same experience at Diablo
18 Canyon, for example. That evaluation period lasted
19 five years. So in today's day and age, we like to
20 measure things by how long it takes to perform the
21 activities, but in reality, it's not like we were full
22 bore spending 100 percent of our time.
23 We actually had a two-year period where we
24 weren't evaluating anything because the development
25 was in process, so we were waiting on phase two

1 document developments, right? And this is not
2 uncommon for these systems.
3 So you are absolutely correct. These are
4 long-term projects primarily that we're dealing with.
5 The calendar or the timeline that Samir showed, that's
6 calendar time. And when you see that the alternate
7 review process is a lot smaller calendar time, that
8 does not necessarily mean that it's any more or less
9 resources expended during that period of time. It's
10 just that calendar time, we're issuing the license
11 amendment at that earlier stage.
12 MEMBER SKILLMAN: Thank you.
13 MR. STATTEL: But again, you know, our
14 decision was to remove the time references from the
15 document, so we made a choice to do that. Any effort
16 to add them back in, I would - it could have - it
17 could give the wrong impression. That would be my
18 concern.
19 CHAIRMAN BROWN: Okay, we want to move
20 onto the next slides? I think we've got four more to
21 complete.
22 MS. ZHANG: So I will take it over. My
23 name is Deanna Zhang and I'm going to be talking about
24 the fundamental design principles as well as the
25 attribute of simplicity.

1 Before I begin, I just want to highlight
2 that we did receive, we did look at ACRS's
3 recommendation for revision one of the ISG, and one of
4 them being that Section B should be revised to include
5 a discussion that while process is important, it's not
6 a substitute for a detailed review of the hardware and
7 software architecture to ensure that they meet the
8 fundamental principles identified in the discussion.
9 Now, that was included. It was included
10 at the end of the introduction section.
11 In addition, at the Phase 0 meeting, there
12 is a discussion of how the fundamental design
13 principles are met by this new proposed change in the
14 design, and I want to go back to also in - I know Rich
15 talked about this a little bit - in Section D.1 which
16 talks about the plant system description which -
17 CHAIRMAN BROWN: Which section did you
18 say?
19 MS. ZHANG: Section D.1 which is the -
20 CHAIRMAN BROWN: The system description?
21 MS. ZHANG: Yes, the system description
22 which applies to Tier 1, 2, and 3. It says in D.1.1,
23 it says, "The documentation and description should be
24 on two levels. First, the individual channels or
25 divisions should be described, including the signal

1 flows between the various digital equipment, IMs.
2 "Second, the overall system should be
3 described with particular emphasis on additional
4 hardware items not included in the description of the
5 channels or divisions such as motors, communications
6 with workstations or non-safety related systems,
7 bypass functions, and diverse actuation systems," and
8 if you look at that description, it's really talking
9 about the new architecture that you're proposing.
10 MEMBER KIRCHNER: So may I ask a question
11 just to clarify the heading of this slide? I would
12 presume you would exercise a review that would check
13 each of these fundamental design principles whether
14 you were Tier 1, 2, 3, or any other method of
15 reviewing, so I presume you don't mean to limit these
16 design principles.
17 This is why I brought up architecture
18 earlier. I would assume going in, if it's an existing
19 design, and hopefully they already have satisfied all
20 four, and if it's a new design, then you would be
21 looking at the architecture to make sure that it does
22 that.
23 And then after whatever platform component
24 system was changed out, one would then go back again
25 and make sure nothing was done, like as Dick was

1 saying, and changing any hardware configuration such
2 that you obviated or lost, you know, you couldn't
3 satisfactorily address each of these four points.
4 Isn't that what you do, you know, when you actually do
5 the review?
6 MS. ZHANG: Yes, and, well, you know, I
7 know that for the alternative review process, we
8 really emphasize the system architecture and how it
9 meets the fundamental design principles, but we also
10 do it in reality for any of the tiers.
11 I think what Rich was trying to say
12 earlier was we get all the design outputs, so those
13 design outputs should demonstrate how the architecture
14 meets the design principles, how everything is laid
15 out.
16 It may not be organized as they would do
17 it for the alternate review process because for the
18 alternate review process, you're not getting the
19 design outputs, so the information has to be extracted
20 and pulled together to demonstrate, you know, the
21 different parts of the architecture, and maybe -
22 So it can be provided earlier in the
23 development process, but if you do it using Tier 1, 2,
24 and 3 processes, you might get an earlier
25 architecture, you know, as the first submittal.

1 Later on as you get detailed design
2 outputs, you may get more design information that
3 shows details of the architecture, including
4 implementation of the different functions using
5 different software blocks, so that level I would
6 expect to get in a phase two submittal.
7 MEMBER KIRCHNER: I'm just reflecting on
8 just the literal reading of this would almost imply
9 that you're not doing this for Tier 1, 2, and 3. I
10 don't think that's what you mean to imply.
11 MR. STATTEL: That's not our intent.
12 MEMBER KIRCHNER: Yeah, and secondly, I'm
13 just reemphasizing what Charlie said earlier. When it
14 comes to our review, for example, this, I think, would
15 be the high-level matrix that we would go through to
16 ensure that whatever system comes in front of us or
17 architecture, that it does indeed satisfy these design
18 principles.
19 MS. ZHANG: Yeah, and we received the
20 comment, and we will go back and look at our ISG to
21 see how it could be, how we could better incorporate
22 the system architecture to address that in all tiers
23 as well as the alternate -
24 CHAIRMAN BROWN: I was aware of D.1 and I
25 had read that, but it was, what, three sentences,

1 whereas D.2 was far more explicit in terms of some of
2 the characteristics. So D.1 was only, it is required
3 for all the Tier 1, 2, and 3, as well as the alternate
4 review process, and obviously D.2 is required for the
5 alternate review process.
6 And I'm not trying to dictate. It's - I'm
7 just really trying to make the point that when you get
8 to us, the higher level, that's the only thing we've
9 really had to grab onto to convince the members that
10 in fact we're implementing a new, more complex reactor
11 trip system and/or safeguard system with the
12 accompanying vulnerabilities that software bring to
13 the picture, the possibility -
14 And I'm not talking about software that
15 fails. I don't want to get into a discussion of
16 software failing. I'm still trying to figure out how
17 software fails. It always does what you say it's
18 going to do unless a gamma ray flips a bit somewhere,
19 but the design issue may be an issue, but whatever.
20 That's a subject for another thing, but
21 just that we end up with a complete review of the Tier
22 1, type 2 and 3 things and that includes, and
23 architecture, and this covered that, but it was pretty
24 much squished is what I would say, so.
25 MS. ZHANG: I don't think it was our

intention to just squish it. I -

CHAIRMAN BROWN: Do not take that as an accusation.

MS. ZHANG: Yeah.

CHAIRMAN BROWN: I know it was not your intention, okay.

MS. ZHANG: So we'll go back and take a look at how we can better incorporate the different parts of the system architecture to apply to the different processes.

CHAIRMAN BROWN: Yeah, and I do understand that you incorporated our comments, those particular comments.

MS. ZHANG: So for this slide, I'm just going to go over how the four fundamental design principles were integrated into the system architecture. This section was in the alternate review process.

And also, you know, I want to highlight that these are the same fundamental design principles that we're reviewing as part of the NuScale review. It's also documented in the NuScale DSRS, so just to bring some background as far as, that this is not something new.

So we would expect that the licensee

1 provides the necessary information to demonstrate how
2 these four fundamental design principles of
3 independent, redundancy, deterministic behavior, and
4 diversity and defense-in-depth have been met in the
5 design as well as the overall I&C architecture itself.
6 CHAIRMAN BROWN: Okay, before - were you
7 going to flip a slide now or were you going to say
8 something else?
9 MS. ZHANG: No, I was going to go through
10 each of the four.
11 CHAIRMAN BROWN: Oh.
12 MS. ZHANG: I don't have to.
13 CHAIRMAN BROWN: Okay, no, I just - I'll
14 let you go ahead and finish, and then I'll say what I
15 was going to say.
16 MS. ZHANG: Okay, so for the fundamental
17 design principle of redundancy, the system
18 architecture section specifies that the staff should
19 verify that the new architecture and system design has
20 sufficient redundancy, so this includes verifying that
21 the single failure criterion, reliability, as well as
22 requirements for maintenance bypass have been
23 addressed by the design.
24 For the fundamental design principle of
25 independence, the system architecture section

1 specifies that the staff should verify that the design
2 has sufficient physical, electrical, data
3 communications independence, as well as functional
4 independence in the new architecture.
5 The staff should verify that any new
6 connections internal to the safety systems, including
7 cross-divisional interfaces, connections to human
8 systems interfaces, other plant systems, connections
9 between safety-related systems, and connections
10 between safety related and non-safety systems have
11 been properly identified.
12 For the fundamental design principle of
13 determinism, this system architecture section
14 specifies that the staff should verify that the design
15 exhibits deterministic behavior and that reviewers
16 should verify that the new architecture ensures input
17 signals and system characteristics result in output
18 signals to ensure no relationships among system states
19 and responses to those states, and that the system
20 produces the same outputs where given setup input
21 signals and the sequence of inputs within well-defined
22 response time limits, in other words, that the design
23 exhibits predictable and repeatable behavior.
24 And information should be provided on how
25 the design prevents software failures from affected

1 the watchdog timer timing and timeout. This
2 information should address hardware and software
3 malfunction coverage for the watchdog timers,
4 including a description of the annunciation and the
5 effects of the plant during and after reset of the
6 watchdog timer or initiated by the expiring watchdog
7 timer.
8 For the fundamental design principle of
9 diversity and defense-in-depth, the staff should
10 verify that the licensee has demonstrated via a D.3
11 evaluation that the use and application of D.3 in the
12 new architecture ensures that safety is maintained in
13 the event of a postulated common cause failure.
14 CHAIRMAN BROWN: Now you're going to
15 switch slides?
16 MS. ZHANG: Yeah.
17 CHAIRMAN BROWN: Before you do that, one
18 of the things I guess I noticed that was absent and
19 that we've always covered extensively, during at least
20 the new designs as well as Diablo Canyon, was control
21 of access relative to external.
22 I'm not talking cyber security here. I'm
23 talking just about communication directionality in
24 terms of network connection to outside sources, and I
25 notice that's not addressed anywhere within the ISG,

1 and did I miss that or -

2 I know there's a control of access

3 paragraph in IEEE-603, but that just says control of

4 access, and we tried to amplify that when we made the

5 proposed rule change which, you know, was one of the

6 exceptions, I think, that was included, at least from

7 our standpoint. You all may not have incorporated it,

8 but that was at least in our letter somewhat.

9 So is there any - how have you - what's

10 your thought process on how you're going to address

11 what we've successfully accomplished on all of the new

12 plant designs? And I think Diablo Canyon was okay

13 also. I'm trying to remember that detail.

14 MS. ZHANG: So for the - we do do a SDOE

15 review which covers our control of access from IEEE-

16 603. As part of that, Samir, if you want to -

17 CHAIRMAN BROWN: Yeah, but that's control

18 of access to how you change a PROM or something like

19 that, or change the software that's being processed by

20 the platform, and that's the way I read the SDOE

21 approach. If you're going to make a software change,

22 you have to have control of how somebody implements or

23 can get into the platform to change that software.

24 MR. DARBALI: It also talks about the

25 platform's ability for remote access, so that is

1 addressed at the platform and application level, but
2 then there's also the communication section which
3 addresses one-way bidirectional communication. Is
4 that what you're getting at?
5 CHAIRMAN BROWN: Yeah, but normally that
6 is not necessarily described relative to outside the
7 plant type of stuff. When you talk about remote
8 access, it's normally relative to maintenance work
9 stations which have access -
10 MR. DARBALI: Right.
11 CHAIRMAN BROWN: - to the trip system
12 processing and/or the safeguards processing, or the
13 information flow to the main control room type of
14 processing. I don't remember all of the little
15 details, but that's what my memory is telling me.
16 So, and I'm most worried about almost all
17 of these new designs incorporate networking for
18 processing once it comes out of the system, the
19 divisions and everything. It gets into a network,
20 then it gets distributed.
21 MR. DARBALI: So -
22 CHAIRMAN BROWN: It's an architecture
23 issue.
24 MR. DARBALI: You're talking about access
25 from outside the plant, but you also -

1 CHAIRMAN BROWN: Yes, the ability, the
2 connection of a network that has all the plant ESFAS
3 and reactor trip system data on it, and it's now
4 communicated outside the plant.
5 MR. DARBALI: But you also said you're not
6 referring to cyber security.
7 CHAIRMAN BROWN: No, it's just a way of
8 sending unit directionally outside to anybody that
9 wants to get it. That's just to the corporate offices
10 or to the admin offices, or whoever that is, okay.
11 What they do with it is one, but if it's only
12 communicated only one way, you don't have to worry
13 about cyber security if it's air gapped. You only
14 have to - the internal malicious -
15 MR. DARBALI: Right.
16 CHAIRMAN BROWN: - stuff is the only thing
17 you have to, fundamentally the only thing you have to
18 deal with.
19 MR. DARBALI: But as far as reliability,
20 your concern is also if it's bidirectional.
21 CHAIRMAN BROWN: Very much so.
22 MR. DARBALI: So -
23 CHAIRMAN BROWN: And we've excluded that
24 and prevented that, all the licensees that have come
25 forth so far, and incorporated single transmittal line

1 only type of stuff external to the plant, and I saw no
2 reference to control of access relative to that in
3 terms of how any new designs would be developed, or
4 new upgrades would be developed.
5 MS. ZHANG: As you know, Charlie, we
6 discussed this a lot as part of the 603 rulemaking,
7 including discussions with OGC. We thought of this as
8 more of a look that we needed to take from an overall
9 I&C regulatory framework because this is beyond just
10 the safety and non-safety I&C system looking at
11 independence perspective, but also looking at the
12 overall I&C architecture and how it interfaces with
13 the outside world.
14 So from that perspective, we thought that
15 we needed to, you know, with input from OGC, we
16 thought that we needed to take a look at this from
17 looking at our regulatory framework, how to improve
18 the overall regulatory framework so that it does allow
19 the staff to have the ability to look at both security
20 as well as safety issues.
21 So that will be discussed and looked at as
22 part of MP 4B, and I'm looking at Luis there, and he's
23 giving me the thumbs that he will be presenting that.
24 CHAIRMAN BROWN: You're spouting the - I
25 won't use the terminology. You've done very well at

1 repeating the line we've heard for the last seven
2 years. Go ahead.
3 MS. ZHANG: But it is included as part of
4 our integrated action plan. As part of the Appendix
5 A, there is an item to address that.
6 CHAIRMAN BROWN: Yet I continue to
7 maintain that if you don't provide an architecture
8 where you can protect yourself from external access,
9 then you can have all the cyber security plans you
10 want and they won't do any good, and if you wait until
11 after - it's always been argued that it's a
12 programmatic issue under 7.34, or 31, or whatever the
13 number is, 70.34 or something -
14 MR. DARBALI: 73.54.
15 CHAIRMAN BROWN: Pardon?
16 MR. DARBALI: 73.54.
17 CHAIRMAN BROWN: 73.54, thank you very
18 much, 73.54. My memory is not that good. And you can
19 have all the great language you want to and all the
20 great systems - is that upstairs?
21 Yeah, so I'd just make the point again,
22 it's up to - it's your all's bailiwick to ensure our
23 architectures have the capability to handle these
24 situations, and it doesn't do any good to all of a
25 sudden have a bidirectional ethernet connection to

1 YouTube that you're going to cyber research and be
2 caught in the same hacking situation that everybody
3 keeps reporting these days as they continue to get
4 hacked because you're always behind the hackers.
5 You're always reacting to them. You will never be
6 able to protect the plant, and if they ever take over
7 control of the network, you're had.
8 MS. ZHANG: So right now, working within
9 our current framework, we've been trying to address it
10 on a case by case basis. That's why it was all -
11 CHAIRMAN BROWN: And we will continue to
12 do that in each and every meeting we have as long as
13 I'm here anyway. It might have to happen when I
14 retire, okay? Rich is looking forward to that. I'm
15 just teasing you, Rich. No, I love it. Rich and I
16 have gone back and forth many, many times. I love our
17 discussions with Deanna. So anyway, you've said what
18 you were going to say and what I expected you to say,
19 so we can move on.
20 MS. ZHANG: So, next slide. So in
21 addition to the four fundamental design principles,
22 the system architecture section also includes a review
23 of guidance for the attribute simplicity in the design
24 which is also consistent with the NuScale Chapter 7
25 safety review.

1 Since this principle, and it's a very
2 subjective principle. There's nothing absolute to
3 measure. We look at it as a balance act in terms of
4 how much simplicity there is versus what are the
5 benefits if you were to add additional complexity, and
6 those features, what safety benefits it provides you.
7 So for example, a self-testing feature,
8 you know, is it necessary for the safety function,
9 probably not, but it does add reliability, ability to
10 detect failures, to failsafe based on that failure
11 detection, and to enunciate it to the operator, but it
12 does add complexity to the design, but we look at the
13 tradeoffs and we believe that the benefit does
14 outweigh the complexity that it does add.
15 But we also look at if you were to add
16 additional complexity and it does provide benefit, how
17 does it impact the overall I&C architecture and the
18 fundamental design principles, independence, does it,
19 you know, challenge your independence? Does it
20 challenge your overall diversity and defense-in-depth
21 as well as your deterministic operations? So we did
22 include that as part of the design change.
23 CONSULTANT HECHT: Can I ask a question?
24 Because it seems to me that if complexity is basically
25 you know it when you see it, it becomes very difficult

1 to make a regulatory determination which is going to
2 cost somebody some money, and aren't there other ways
3 of expressing that complexity in terms of criteria so
4 that you don't have to put on this thing called
5 simplicity which can lead to controversy?
6 You gave the example of redundancy.
7 Presumably that adds complexity because you put more
8 lines, more boxes on your architecture, but on the
9 other hand, I can abstract that away through something
10 like, you know, calling it a single line diagram and
11 it's not there.
12 So can't you say, "Well, this introduces
13 more vulnerabilities," or, "This introduces more
14 single points of failure or more common cause failure
15 points, or makes it more difficult to review," or
16 something like that?
17 MS. ZHANG: Yeah, I think overall in the
18 design, we have to look at all of the potential
19 hazards within the design, right? So single failure
20 is a hazard. You want to ensure that your
21 architecture is protected against single failure.
22 Now, are there other ways of addressing
23 single failure rather than putting in additional
24 equipment? That is something I think we need to
25 explore as more of looking at it from a research

1 perspective. I don't know of it existing otherwise.
2 You know, have we done anything that looks at more
3 specific criteria?
4 You know, this is what you would need to
5 do in terms of maybe reliability to demonstrate that
6 you're not subject to the single failure in terms of
7 having software reliability or system reliability that
8 you would say, "I don't need to address single failure
9 and I could just have one."
10 CHAIRMAN BROWN: Let me interrupt because
11 in my own mind, we're going to have redundancy whether
12 we - on the trip systems and safeguard systems. In my
13 own mind, the biggest source of complexity in all of
14 this stuff is the platform software.
15 It is - any time you have, I don't know,
16 500,000 lines of code that you have to program in and
17 make sure, and all the little testing nuances, you
18 know, triggering a test signal that has to reset in
19 two milliseconds so you don't trip your output breaker
20 relay and everything else, that introduces complexity
21 based on how you test your, the self-test features
22 that you're talking about.
23 I guess, and I won't cite the platform,
24 but one talks about every two milliseconds, it goes
25 out and triggers something to happen and then it

1 resets it very quickly so that it doesn't happen, but
2 it senses that it was going to happen if you can
3 understand with that dialogue I just mentioned.
4 MR. STATTEL: So we've been grappling with
5 this issue for a number of years.
6 CHAIRMAN BROWN: Yes.
7 MR. STATTEL: The truth of the matter is
8 it's not a one-sided argument. Complexity, adding
9 complexity is not always bad. There is such a thing
10 as necessary complexity. There is such a thing as
11 regulated complexity.
12 When we look at these systems and we look
13 at these diagrams, the detailed logic that's
14 implemented in these systems, at a glance, at first
15 glance, they may look unnecessarily complex, but
16 inevitably when we get down into actually looking at
17 the logic and we kind of discover the reason why
18 those, that complexity was added, by and large it's
19 because of meeting a regulatory requirement.
20 So an example would be, you know, when we
21 think of a typical safety function, you think, "Oh,
22 well, that should be a really simple system. You just
23 process an analog input signal. You ran it through a
24 comparator, and you send an output out. Why would you
25 need anything more than that? That's as simple as can

1 be," but the reality of it is that system would not be
2 acceptable because it doesn't meet the regulatory
3 requirements.
4 So the regulatory requirements would
5 dictate that that system would have to be testable,
6 online testable, so you have to add logic to support
7 testing online. It would have to, if it had a bypass
8 function, you would have to annunciate that bypass
9 condition to the operators. That adds logic.
10 So all of these things, all of the
11 requirements, I mean, you can go through IEEE-603 and
12 look at each requirement, single failure criteria,
13 maintenance bypass, operation bypass, reenabling
14 safety functions, all of those things add complexity
15 and all of those things end up adding function blocks,
16 adding logic, adding comparators to these diagrams.
17 So it's easy to get an impression when you
18 look at one of these safety systems that that's more
19 complex than it needs to be, but the reality of it is
20 a lot of that complexity, at least in our experience,
21 in our reviews, a lot of that complexity is driven by
22 the regulation itself. So we're kind of pushing both
23 ends of the rope here, right?
24 We clearly have guidance to the vendors
25 and to the licensees, "Don't make these systems more

1 complex than they need to be," right? "If you're
2 adding complexity in order to save the operator from
3 doing channel checks, then that might be more complex
4 than it needs to be," and we do question those types
5 of functions in systems.
6 But when it comes to diagnostics
7 functions, failure detections, these new digital
8 systems are so much better at detecting failures and
9 preventing latent failures from occurring in these
10 systems than the analog systems were, there are clear
11 benefits to that and it's undeniable, so the guidance
12 is what it is.
13 CONSULTANT HECHT: I guess I would observe
14 that, what you call simplicity at the architectural
15 level, I would distinguish from simplicity at the
16 implementation level, but we don’t -- both
17 definitions, if we haven’t -- or both perceptions, if
18 we haven’t really defined what the difference between
19 an architectural simplicity and an implementation
20 simplicity, or complexity, we can’t do that.
21 And the other thing is, of course, what
22 looks architecturally, or even simple from the
23 perspective of implementation of either the vendor or
24 the operator saying, we just have this black box and
25 we just use this black box called, for example, Linux,

1 and it looks real simple to me, but in fact, is
2 internally complex. We don't necessarily have a way
3 of measuring that.
4 So, I guess, we have -- everybody has a
5 common interest of not making things more complex than
6 they need to be, but what is this telling you? The
7 example that you gave of the additional functions
8 there, to simplify operations, you might consider that
9 to be unneeded functionality, which maybe you want to
10 state that way, but I'm not sure that simplicity is
11 the right concept.
12 MS. ZHANG: I think what we want to promote
13 is for the licensee or the designers to really think
14 about some design choices they're making. If there is
15 a way to not introduce unnecessary complexity, that
16 they consider it, whether from an architectural
17 perspective or even from the platform they're
18 selecting.
19 CONSULTANT HECHT: Then, maybe, shouldn't
20 there be a section on design decision justification as
21 opposed to calling it complexity?
22 MS. ZHANG: And, again, we are trying to
23 work within the purviews of our regulatory framework.
24 And we're looking at it from a safety perspective and
25 this is guidance for us to look at it, to make a

1 safety determination.

2 There are decisions that are made that are

3 not for safety reasons and we can't, as regulators,

4 prohibit such a design. However, we do want to

5 advocate, in this case, for the designers to think

6 about --

7 CONSULTANT HECHT: Okay.

8 MS. ZHANG: -- looking at their design and

9 reducing unnecessary complexity.

10 CONSULTANT HECHT: All right.

11 CHAIRMAN BROWN: We're going to go on.

12 CONSULTANT HECHT: Yes.

13 CHAIRMAN BROWN: We're running behind, so

14 I'm going to help catch us up a little bit. And then,

15 I'll say what we're going to do in another five

16 minutes.

17 MS. ZHANG: So, that's my slides. And I'm

18 going to pass it over to Mike to talk about the

19 licensing oversight.

20 MR. WATERS: Yes, I'll go through this

21 really quick. This table, we talked about all this

22 this morning, it's just a higher level comparison of

23 the tiered process and alternate review process and

24 all the features of it.

25 I won't go through every line item here,

1 but for the tiered process, as Rich noted, there's a
2 two-phase process that provides flexibility to a
3 licensee and an ability to make design changes as a
4 part of the license review process up to
5 implementation. We traditionally make a compliance
6 finding at the factory acceptance testing stage.
7 All the review process is one submittal,
8 with potential license conditions. This provides the
9 flexibility, as the team noted, to a licensee
10 receiving an earlier NRC approval of the design to
11 help inform and refer expenditure resources to
12 actually prepare and develop the detailed design.
13 In both cases, once the license is issued,
14 when it arrives at the site, primarily for site
15 installation to be subject to regional inspection.
16 The alternate review process, we believe
17 some of the implementation and test activities after
18 license is issued would be subject to vendor
19 inspection. And, again, we need to work out some of
20 the programmatic details of that down the road, but
21 that's the key difference
22 And we would expect both our quality
23 assurance experts and our I&C experts to be part of
24 that process. To move on, last slide, these are the
25 next steps. Obviously, we appreciate our time here

1 this morning.

2 We plan to brief the full Committee on

3 June 6, I think I got that date correct. We also plan

4 to have what we're calling table top exercise with

5 industry on June 13 and 14.

6 Practically, the idea is to walk through

7 our past review of Diablo Canyon, primarily, and some

8 of Hope Creek, to kind of test out how this alternate

9 review process will play out with this draft ISG.

10 Once we do that, we'll make some final changes to the

11 draft, from that and any comments from the

12 Subcommittee, and plan to issue the draft for formal

13 public comment in July of 2018.

14 Finally, looking ahead, we are very eager

15 to engage utilities in pre-application meetings. We

16 understand that a LAR submittal from a lead-plant

17 using the alternate review process is currently

18 expected in 2019 time frame.

19 Pre-application meetings are very

20 important to align on expectations for what will be

21 submitted. We address some of the questions, for

22 example, of how will we tailor the guidance in the

23 Enclosure B, what would B look like, and it's very

24 important to do that.

25 I know that Charlie, offline, that at some

1 point, these are great guidance, we've done a great
2 job, and we really want to have a lead-plant to lead
3 and exercise it throughout the review process.
4 And finally, my team reminds me, more
5 often than not, that ISGs are in fact Interim Staff
6 Guidance, and at some point, we'll make a strategic
7 decision to incorporate it into the Standard Review
8 Plan down the road, along with other potential
9 regulatory changes.
10 With that, I will thank the team. We did
11 take some really good notes, Samir and myself, and I
12 was going to summarize them, but I won't do them in
13 interest of time.
14 We talked about the architecture, the
15 configuration control, the NQA 1 question, the
16 application design principles, alternate review
17 process. We had a Figure 8 I guess -- conversation
18 and the simplicity.
19 And I think, at a minimum -- we've heard
20 some really good comments. At a minimum, we're going
21 to go back and we need to clarify some things in the
22 ISG, in particular, the architecture and the table.
23 And to the extent practicable, we'll
24 consider these comments in -- tomorrow, we'll start
25 working on the ISG probably, and we'll do our best to

1 communicate to Christina before the full Committee
2 meeting what we're doing and providing any other
3 responses to questions you may have before and after
4 the full Subcommittee meeting, up to the issuance in
5 July.
6 CHAIRMAN BROWN: Okay.
7 MR. WATERS: I think that's all I have.
8 CHAIRMAN BROWN: All right. We'll -- I
9 have to make some type of a decision here. We've got
10 some time, we had half an hour set aside for some
11 audience folks who are attending the meeting to make
12 some comments.
13 And I'm -- instead of waiting until after
14 lunch, I'm going to go ahead and defer lunch and let
15 them make their comments now, so we've got a connect
16 between this discussion and them.
17 And we'll go over your other type stuff,
18 we'll talk about possible things -- what to do in the
19 full Committee a little bit at the end of the day, so
20 you'll have a little bit of focus on what to address
21 the full Committee, if anybody's got any suggestions
22 at that time, in addition to my own.
23 So, right now, I'm going to open the --
24 we're not going to do the phone line yet, we're going
25 to do that second. But if there's anybody in the

1 audience, I think there are a few folks that want to
2 make some comments.
3 MR. REMER: Yes, thank you.
4 CHAIRMAN BROWN: All right.
5 MR. REMER: Yes, good morning. Jason
6 Remer, I represent NEI. I'm also the coordinator for
7 the Digital I&C working group. Been working together
8 with the NRC on modernizing the digital infrastructure
9 here.
10 We really appreciate the NRC's
11 consideration in this ISG. It will really meet a need
12 for more efficient reviews. We have a strong need to
13 modernize our digital systems out there, not just
14 control systems, but safety systems.
15 We've got, essentially, safety-related
16 World War II vintage systems at work today, right?
17 This very minute, 99 plants, maybe not 99, maybe 92
18 plants, are using World War II vintage safety systems,
19 while their control systems for power production are
20 mostly Revision 2 or 3 digital systems, with all the
21 feedwater, turbine, generator, all that stuff.
22 You'll hear more about that from our
23 colleagues from industry. So, a real need to
24 modernize this process. And one big step is to get
25 our regulatory process more streamlined.

1 And we really appreciate this, it's been
2 a model process, working together with the industry,
3 hearing our needs, while of course, recognizing the
4 need to maintain safety. We believe switching to
5 digital systems will improve safety and improve
6 efficiency.
7 I'm involved in also a second license
8 renewal, basically, operations out to 80 years. SLR
9 will allow major modifications to go forward at power
10 plants, because if you've got another 20-year horizon,
11 you break free a lot of money to spend on upgrading
12 your plant.
13 So, we hope the utilities decide with SLR
14 to replace their analog safety systems with digital
15 control systems. That will not happen unless we
16 streamline the regulatory process, I can tell you.
17 The CNOs want to communicate that strongly, that until
18 we change the process, they will stay analog.
19 I know that's a ridiculous decision, but
20 that's what will happen. So, I'm really happy to see
21 this process going forward, I think it's the right
22 thing to do, and I think it will work. Again, it's a
23 model process.
24 I'll close out by just asking the
25 question, the whole world has gone to digital

1 processes and systems, including the other large light
2 water reactors around the world, they're either all
3 digital or they're going digital.
4 All the major risk-significant industries
5 are all digital. You drove here in a digital-powered
6 automobile, you flew here in a digital-monitored
7 airplane. And so, why not us? This is our time to do
8 this. We want to do it, we hope to be able to do it.
9 And, frankly, we're fighting for our lives
10 at nuclear power stations, as you know what's going on
11 out there. Safety has improved dramatically, look at
12 our safety performance over the years. It's time for
13 efficiency to catch up. Thanks very much. John?
14 MR. CONNELLY: Good afternoon. John
15 Connelly, I'm with Exelon. Gordon, you posed a
16 question, Charlie, you kind of amped on to it, and
17 Mike alluded to it earlier in the day, are there
18 people waiting in the wings to do these projects?
19 Kind of a Field of Dreams thing, if you build it, they
20 will come.
21 I'd like to provide a more direct response
22 to that question. So, and I'm speaking for Exelon
23 here, we've invested very heavily in digital
24 technology. Very heavily. Turbine control systems,
25 digital feedwater systems, open phase detection,

1 protective relay, ASCs, the list goes on and on and
2 on.
3 That's measured in hundreds of millions,
4 if not billions of dollars. We've invested very, very
5 heavily in non-safety-related digital upgrades. The
6 question is, why?
7 Well, first and foremost among them is
8 that we see precipitous drops in initiating events by
9 going to the digital domain. I mean, we see 80, 85,
10 90 percent reductions in SCRAM rates by going to
11 digital. So, there's a tremendous business imperative
12 that drives that.
13 Jason alluded to this, we're under
14 economic pressures that we've never seen before,
15 between shale gas, subsidies renewables, a flat growth
16 of electrical demand. We're under tremendous pressure
17 to make these plants much more efficient, more safe,
18 and more economically viable.
19 So, do we have a project specifically
20 queued up ready to go? The answer is, not really, but
21 the same principles that have been driving us to
22 invest heavily in digital technology for the non-
23 safety side of the house exists in the safety side of
24 the house at the same time.
25 We've been precluded from doing that

1 because of the risks that attach to it. But, frankly,
2 speaking from a licensee's perspective, those risks
3 are falling away.
4 Once we have this ISG in place and we have
5 a stable path forward where we can make those kind of
6 investments and proceed forward with those, that's
7 going to open up a floodgate. That'll open up any
8 questions that you have for me.
9 CHAIRMAN BROWN: We'll finish.
10 MR. CONNELLY: Okay.
11 CHAIRMAN BROWN: If anybody has any
12 questions, you can go ahead and ask them, I'm open,
13 I'm letting this be kind of free running.
14 MR. HERB: Thank you for letting me speak.
15 My name is Ray Herb, I'm with Southern Nuclear. And
16 we currently have one of the plants being developed
17 right now that utilizes very heavily on digital
18 protection systems.
19 And we appreciate the NRC's allowing us to
20 consider some of our inputs when they developed this
21 new alternate review process. We see the alternate
22 review process as vital for implementing our upgrades
23 to digital protection systems that we are currently
24 still being planning for the rest of our fleet to
25 complement our Vogtle 3 and 4 designs.

1 I'm not saying we're putting in Common Q,
2 but I'm saying we're in the initial planning and
3 scoping phases for that development process. And I
4 couldn't get approval to even go there without some
5 assurance that this alternate review process was going
6 to be in place.
7 And so, based on the fact that this
8 process that they've developed with input from us to
9 address some of our concerns, specifically with the
10 earlier approval of the LAR, we are going forward.
11 Now, does that mean we're going to be pre-
12 application in 2019? We have a lot of other pressures
13 going on right now. We have to get Vogtle 3 and 4
14 done. And so, when some capital dollars get freed up,
15 we will be submitting a Phase 0 based on that.
16 But I'm spending money today in
17 determining that scope. And so, it is happening, it's
18 just a matter of time. These projects, as I think
19 somebody said, it takes seven to ten years from the
20 planning phases all the way through.
21 I mean, the new alternate review process,
22 it allows us to get our ducks in a row early, with a
23 nice architecture, with a very set level of
24 requirements that are set, that are inspected to. And
25 then, we take it from there, as I think Rich had said

earlier, some of that risk now comes on us.

We have to make sure that we stay within that approved application that the NRC has reviewed. And then, there's an additional burden of inspections that we're willing to accept going forward.

And we have to also evaluate any potential changes that come after a review has been done, or after this LAR is submitted, underneath a 50.59 process, to determine whether or not they break the plane to go back to a resubmittal of the LAR or we can do it within our own design processes.

And so, because of that, because the new alternate review process requires an additional inspection element that wasn't there. We have a little bit of concern that after this project is done, that we need to probably raise that piece as well.

Whatever additional inspection guidance is needed for inspectors for the alternate review process, not for the regular ISU process that I think we've got a lot of stuff already out there, but we're not quite sure where that is.

It's just a concern that I would like to see us, once this is done, once we get the alternate review process in, we start to look at that piece too, work with maybe some workshops or something like that.

1 So, thank you.

2 CHAIRMAN BROWN: All right, thank you. Is

3 the phone open?

4 MS. ANTONESCU: Yes.

5 CHAIRMAN BROWN: Would someone on the phone

6 line -- oh, I'm sorry. Ken?

7 MR. SCAROLA: Thank you. Ken Scarola,

8 Nuclear Automation Engineering. I wasn't actually

9 planning on commenting on this section.

10 CHAIRMAN BROWN: I know.

11 MR. SCAROLA: So, my notes are cryptic.

12 (Laughter.)

13 MR. SCAROLA: I was planning on commenting

14 later this afternoon. And, please, I don't want

15 anyone to construe anything that I say as an attempt

16 to hold up this ISG in any way. We need this ISG, we

17 need it as fast as possible, we need to start

18 modernizing our digital safety systems. But I still

19 have comments.

20 This ISG was generated in 2011. And let

21 me remind you, it's Interim Staff Guidance. And when

22 the Commissioners responded to SECY-15-0106, which was

23 the birth of this whole digital action plan, they

24 basically said, revamp the I&C regulatory

25 infrastructure.

1 Not patch it, revamp it. And when you
2 revamp it, make sure that your regulatory criteria for
3 new plants and operating plants is the same, there's
4 no reason for it to be different.
5 So, I have a simple question. We're now
6 seven years later, isn't it time we looked at the SRP
7 and fixed it and stopped patching Interim Staff
8 Guidance? Simple question.
9 And with that, I have to ask, who at the
10 NRC is responsible for looking to the long-term and
11 making sure that we do things in the manner that gives
12 the industry viability for the long-term, instead of
13 patches for the short-term? We've got to get out of
14 this mode.
15 Now, some people have told me, well,
16 there's a big difference between this ISG and the SRP,
17 because the ISG has tiers. Well, now, Rich, you said
18 it yourself, the biggest difference in the tiers is
19 whether you reference a pre-approved platform or not.
20 But you said it, every platform, Topic
21 Report, is different, they're all over the map. So,
22 nobody can come in and say, I'm in Tier 1. There's
23 always, I'm in Tier 1, but I'm in Tier 2 minus. And,
24 very frankly, we've been doing this tier approach for
25 as long as I've been in this industry, which is 43

1 years.

2 Any time there has ever been a licensing

3 action with the NRC, the first thing we always do is

4 what you call Phase 0, we come in and we say, look,

5 this is what we're doing and on this plant, it's the

6 same as what we did before, with the following

7 changes.

8 And we sit down with the NRC and we make

9 a list of what's really changing, so that we can then

10 define what has to be submitted. There's nothing new

11 here.

12 We ought to be doing this in the SRP and

13 making it generic, not just saying, well, operating

14 plants are different than new plants. They're all the

15 same, there is always a reference.

16 So, I don't see anything new about the

17 tier process, very frankly, I think it complicates

18 things, because no one is every clearly in any single

19 tier.

20 My preference would be, here's all the

21 things that are important to a regional review, now

22 come in in Phase 0 and make your case of things that

23 you don't want to submit, because you have a prior

24 reference.

25 And I think we would be much better served

1 by that, than trying to shoehorn -- very frankly, the
2 tier process was invented by Bill Kemper, back when
3 this whole thing came up. And it was a marketing ploy
4 to show -- in an attempt to show licensees that, hey,
5 if you're in Tier 1, look, it's easy. Well, it's
6 never worked and it won't work.
7 One technical comment. On Slide 15, we
8 have this big gap in the middle of the slide where we
9 don't intend to review processes. And I'm floored by
10 this.
11 In the middle of the slide, there's a box
12 missing that in the other review says application
13 software design implementation test plans and
14 processes. Well, I think anyone who has been in this
15 industry knows that you can't judge the output product
16 without judging the processes that lead to the output
17 product.
18 I mean, this is fundamental computer
19 systems design from day one. Any complex design
20 process, whether it's software development, human
21 factors engineering, you can't judge the product
22 without understanding the process. So, I'm kind of
23 shocked that that box is missing.
24 Last comment, I'll get to my cryptic
25 notes. With this whole slide on simplicity. I'm

1 sorry, what is it in 10 CFR 50, 10 CFR 52, that gives
2 you the authority to regulate simplicity?
3 If we regulated simplicity, there would
4 never be core protection calculators in many operating
5 plants today. They are extremely complex, top of the
6 line DNBR calculators, flow projected DNBR trips.
7 If we regulated simplicity, we would never
8 have rate-limited variable set-point for reactor
9 coolant pump flow trips. These are complex analog
10 things. So, and I can go on and on and on.
11 There are numerous complex things, using
12 rod position inside the protection system, it's crazy,
13 it's complicated. But, you know what?, it gives us
14 margin. Using in-core detectors inside the protection
15 system, it's crazy, it's so complicated. But it gives
16 us operating margin.
17 So, I don't think there's anything that
18 gives you the authority to attempt to regulate
19 simplicity. I think simplicity gets regulated by the
20 market. And I think you ought to just let it happen
21 that way. Thanks for listening.
22 CHAIRMAN BROWN: Thank you, all. Now, we
23 will -- the phone is open. Can somebody on the phone
24 line say something so I can make sure that the phone
25 line is in fact open, if anybody's there?

1 Hi. Thank you very much. Would you like
2 -- anybody out there would like to make a comment,
3 please state your name, where you're from, who you're
4 from? And you're online if you would like to say
5 something or have some comment on the morning's
6 activities.
7 Hearing none, I will -- we will recess.
8 I'll make one observation first. No, I think we've
9 covered everything. We'll come back at 1:15, after
10 lunch. We'll recess at this point.
11 (Whereupon, the above-entitled matter went
12 off the record at 12:13 p.m. and resumed at 1:18 p.m.)
13 CHAIRMAN BROWN: The Subcommittee is back
14 in session. We are going to less at least two who had
15 to leave. But I think we have a quorum with Member
16 Ballinger and Member Vesna. So, I think we can go
17 ahead and proceed on with the common cause failure
18 discussion. You said Joy was going to join us, Vesna?
19 Thank you.
20 MR. GUTIERREZ: Good afternoon. My name is
21 Mauricio Gutierrez, I'm from the Office of Research.
22 Here at the table to brief you this afternoon on IAP
23 Modernization Plan #1, Protection Against Common Cause
24 Failure is Dinesh Taneja, from the Office of NRO, and
25 Mike Waters, from NRR. Another key member on our

team, Rossnyev Alvarado, is out today.

So, the information we'll present to you today is an update on the status of our activities related to protecting DI&C systems and components from common cause failure concerns.

We are not seeking a formal letter or formal comments at this time. We do, however, appreciate any comments and insights you offer us today and we will consider them as we proceed with our work. Samir, next slide, please.

So, you saw this slide in the morning, and it just recaps the IAP Modernization Plan. We'll be focusing on the three activities listed, that are bolded on this slide. Please proceed to the next slide.

This presents our agenda with a little bit more detail on the activities, it gives their titles. MP #1A is the RIS 2002-22, Supplement 1, Clarification on Endorsement of Nuclear Energy Institute Guidance in Designing Digital Upgrades in Instrumentation and Controls Systems.

MP #1B refers to the review of NEI 16-16, Guidance for Addressing Common Cause Failure. MP #1C is implementing the Commission's policy on protection against CCF in digital I&C systems. And we'll provide

1 more detail on each of these items during this
2 presentation.
3 Before we dive into the details for each
4 activity, which will include purpose, scope, status,
5 and next steps, we would like to provide you with some
6 overarching background and context information for
7 these activities. Next slide, please.
8 So, microprocessor-based safety systems
9 were first introduced in the 1980s. Since then, the
10 NRC staff has recognized that digital I&C technology
11 can provide advantages in reliability and
12 functionality, but we also recognize that it also
13 creates the potential for a new software vulnerability
14 due to CCF on the systems in which functions are
15 performed by identical software executed in identical
16 hardware.
17 In particular, the staff is concerned with
18 the potential that a latent systemic fault could
19 result in a CCF because of increased resource sharing
20 and the potential for unspecified interactions among
21 systems or cause unanalyzed plant conditions.
22 In 1993, the staff prepared a SECY
23 discussing our concerns to the Commission. The
24 Commission approved in part and disapproved in part
25 the staff's recommendations in the SRM to SECY-93-087,

1 item II.Q.

2 The title for SRM to SECY-93-087 was

3 Policy, Technical, and Licensing Issues Pertaining to

4 Evolutionary and Advanced Light Water Reactor Designs.

5 Item II.Q was titled Defense Against Common Mode

6 Failures in Digital Instrumentation and Control

7 Systems.

8 The staff implemented the Commission

9 policy into BTP 7-19, Guidance for Evaluation of

10 Diversity and Defense-in-Depth in Digital-Based

11 Instrumentation and Control System Review

12 Responsibilities.

13 CHAIRMAN BROWN: Can I interrupt?

14 MR. GUTIERREZ: Yes.

15 CHAIRMAN BROWN: If you don't mind?

16 Anybody else answered it? I'm gathering out of this,

17 since this is the background, and I looked at the next

18 slide, that fundamentally -- and correct me if I'm

19 wrong, okay? -- that the belief is that diversity and

20 defense-in-depth is your primary guard against CCF in

21 software-based or computer-based systems.

22 Is that a reasonable -- that's what I take

23 away from the comments and your very clear

24 clarification of the 93-087 II.Q thing. So, is that

25 -- Mike's shaking his head up and down and nobody else

1 is saying anything.

2 MR. WATERS: I believe the answer is yes,

3 but with the asterisk that, of course, you can

4 demonstrate, -- I guess part of the diversity and

5 defense-in-depth, I guess, it's true, you can

6 demonstrate the plant can cope with a failure, right?,

7 and the consequences are acceptable.

8 Or as other means, such in terms of

9 diversity to demonstrate that. But that's the primary

10 way to demonstrate this. And this is why we're

11 concerned about common cause failure.

12 CHAIRMAN BROWN: I guess I would just make

13 just an observation, and this is just my own

14 perspective and nobody else's, is that, if I was

15 dealing with computer-based systems in what I call

16 control systems, such as a feedwater pump controller,

17 you've got to make decisions.

18 If it breaks, the pump stops, and how much

19 stuff do you put in to back it up? Do you have two

20 systems in parallel, such that one of them detects if

21 the other one doesn't? It's now no longer working,

22 but it's got all the data and it can rapidly switch

23 over control of itself, et cetera, et cetera.

24 There's a lot of different ways to think

25 about that, it adds complexity. But also, if you

1 think about it, the plant analysis that gets done
2 accounts for failures of those pumps to operate and
3 your systems, aside from the pump controller, takes
4 over to protect or take the corrective actions for
5 it.
6 So, I -- and when it comes to arc reactor
7 trip systems and safeguard systems, you've got four
8 channels, you've got redundancy. And I don't mean to
9 speak out of school, but I will, in that redundancy in
10 itself, even though you've used possibly the same
11 software, the same processor, the same platform, the
12 same configuration in each division, you say, well,
13 gee whiz, you could have a single common failure.
14 And the most likely common failure is in
15 the voting units, if you're using them, not in the
16 independent four different processing units, which all
17 have independent data being fed into them. So, it's
18 -- so, redundancy in itself is another means of
19 protecting yourself against common cause failures.
20 MR. WATERS: Yes, let me clarify and maybe
21 --
22 CHAIRMAN BROWN: So, that's why I asked the
23 question, I got the flavor that it's all defense-in-
24 depth and you've got to have another system --
25 MR. WATERS: I think we'll get to, when we

1 start about the principles, I want to clarify, and
2 Dinesh can correct me if I'm wrong, for RPS and ESFAS,
3 our position is that diversity and defense-in-depth is
4 needed. And there's diversity requirements within
5 some of the GDCs and as part of the licensing basis.
6 CHAIRMAN BROWN: I'm not disagreeing with
7 it --
8 MR. WATERS: Right. There's other safety-
9 related equipment where there may not be diversity
10 requirements and there may be means to employ defense-
11 in-depth, including operator actions and other coping
12 measures and consequence analysis to demonstrate that
13 that hazard is acceptable.
14 So, I just want to clarify that before --
15 the risk-significant systems like RPS and ESFAS, for
16 the most part, the answer, I think is, yes. And I
17 think Dinesh will get to that when we talk about the
18 principles.
19 CHAIRMAN BROWN: Okay. Just wanted to make
20 sure I understood the thought process.
21 MR. GUTIERREZ: The last bullet on this
22 slide here is the SRM to SECY-16-0070, and that's the
23 Integrated Strategy to Modernize the Nuclear
24 Regulatory Commission's Digital Instrumentation and
25 Control Regulatory Infrastructure. And that's what

1 our work falls under.

2 CHAIRMAN BROWN: Correct me if -- that's

3 the SRM that followed the attempted rulemaking?

4 MR. GUTIERREZ: Yes.

5 CHAIRMAN BROWN: Where we had to

6 recalibrate back to an integrated --

7 MR. GUTIERREZ: Yes.

8 CHAIRMAN BROWN: -- overall framework?

9 MR. THOMAS: Yes, it is.

10 CHAIRMAN BROWN: Okay, that's what I

11 thought, but I wanted to make sure. Okay.

12 MR. GUTIERREZ: Next slide, please. So,

13 the technical issues challenging consistent

14 application of NRC position by both the staff and

15 industry on defense against common cause failure in

16 digital I&C systems include: The evolution of digital

17 technology and industry standards. The evolved scope

18 of applicability of our position.

19 Addressing CCF concerns when performing

20 upgrades. Determining the amount of emphasis on CCF

21 concerns during system design. Determining the

22 likelihood of a CCF in digital I&C systems.

23 Determining the diversity needed.

24 We also face challenges in determining the

25 need for diverse actuation systems or use of certain

1 design attributes. I think Mike spoke a little bit
2 about operator action, but we also recognize that
3 diversity can add complexity.
4 Another challenge is performing the D3
5 analysis for all types of safety I&C systems under a
6 graded approach. And last, what we have on this slide
7 is, addressing CCF concerns in the context of specific
8 10 CFR evaluation criteria.
9 I'd like to point out that these issues
10 are not unique to the U.S. nuclear industry. Although
11 there are differences in the regulatory structures and
12 oversight in other countries and other industries,
13 there is a recognition that CCF is a significant
14 safety concern for digital systems in safety-critical
15 applications.
16 With the use or replacement of digital
17 systems, this has created an increase in dependence on
18 software in safety systems, which consequently, has
19 increased the safety significance of CCF caused by
20 software.
21 For example, the effect of systematic
22 failures that can lead to a loss of safety in many
23 ways, such as unwanted interactions and another is a
24 safety function is not provided when it's needed.
25 Please note that, although we have encountered these

1 issues, the NRC has been able to proceed with
2 reviewing and accepting licensing applications.
3 One example that you're familiar with is
4 the Diablo Canyon Process Protection System upgrade.
5 For this application, the staff determined that there
6 is adequate diversity within the plant design such
7 that plant responses to design-basis events,
8 concurrent with a potential common cause failure due
9 to software in the process protection system, meet the
10 acceptance criteria in BTP 7-19.
11 If it's okay to proceed, I'd like to turn
12 the presentation over to Mike Waters and he will
13 provide you with details on the activity MP #1A on the
14 RIS 2002-22, Supplement 1.
15 MR. WATERS: Good afternoon, again. So,
16 this activity is one of our first products to address
17 CCF challenges with respect to 50.59 licensing issues.
18 We intend in a couple weeks to issue the final
19 revision, or finalize Supplement 1 to RIS 2002-22.
20 Last year, Dave Rahn provided a very
21 detailed briefing on the RIS to this time. And
22 Wendell Morton, as well, provided a brief on 50.59.
23 The key message is, fundamentally believe the same
24 concepts and principles back then remain within this
25 current version of the RIS.

1 However, the details and the structure of
2 the RIS may have changed as a result of stakeholder
3 feedback and other considerations. We did provide the
4 Subcommittee a version of the RIS that was issued for
5 public comment back in March.
6 We are still in the process of finalizing
7 our response from the public comments, including legal
8 reviews. So, the challenge this afternoon for us to
9 talk about some of these detailed issues today.
10 For those who weren't present at the
11 briefing last May, 2017, the RIS Supplement provides
12 a clarification to our previous endorsement of NEI 01-
13 01. And the RIS specifically clarifies approaches for
14 performing qualitative assessments for determining
15 that CCF is sufficiently low.
16 A 50.59 determination within that context
17 and qualitative findings that are needed for 50.59 to
18 make an upgrade without prior NRC approval. In short,
19 NRC still considers latent software defects to be a
20 credible source of CCF.
21 However, the consideration of design
22 attributes, design processes, and operational
23 experience can be used to justify that the likelihood
24 of a CCF malfunction is much less than other types of
25 malfunctions that may be considered in the existing

1 safety analysis and the licensing basis. And, again,
2 I'm making -- within the context of the 50.59
3 approach.
4 The current RIS Supplement focuses on
5 three areas, a discussion of how the sufficiently low
6 finding specifically addresses the criteria of 10 CFR
7 50.59.
8 Discusses the qualitative assessment of
9 design attributes, design processes, and the operating
10 experience. And then, describes supporting failure
11 analysis and defense-in-depth analysis that could be
12 used to support the qualitative assessment.
13 Finally, it's important to know that the
14 RIS was targeted to address digital upgrades at the
15 beginning for auxiliary safety-support systems, which
16 have been identified as a high priority upgrade needed
17 by industry. It was not initially designed for major
18 upgrades of reactor protection systems and engineering
19 safety features.
20 This morning, you heard about ISG-06 and
21 industry has indicated, we expect those major upgrades
22 to be coming for a License Amendment Review process
23 under the ISG-06, just to clarify.
24 CHAIRMAN BROWN: So, there's -- yes, I read
25 that in the Supplement. So, there is no thought

1 process that says somebody is going to try to do a
2 50.59 on arc reactor trip system and safeguards
3 upgrades?
4 MR. WATERS: Let me ask Dave to handle --
5 CHAIRMAN BROWN: It says that this does not
6 apply.
7 MR. WATERS: There's a little nuance, but
8 I want them to clarify this.
9 MR. RAHN: Yes. So, what we -- oh, sorry.
10 CHAIRMAN BROWN: State your name also.
11 MR. RAHN: This is David Rahn, from the
12 Office of NRR. Can you hear that? Okay. So, in the
13 RIS, what we tried to do is to parse out what aspects
14 of different highly safety-significant systems could
15 be attempted for modification.
16 But to the -- but basically, you're
17 largely correct, the basics of the internal signal
18 processing, bistables, voting logic, all that, all
19 those aspects of RPS and ESFAS systems, are considered
20 really out of the scope of the intent of the guidance
21 that's provided in this Supplement.
22 That's not to say someone can't attempt to
23 do something like this using a simplistic replacement
24 method, but it's highly unlikely that it would
25 actually make it all the way through the 50.59

criteria when you do that.

So, what we did do, though, is we opened the door for someone to potentially replace a sensor that feeds the RPS logic, or maybe a power supply that feeds one division or two divisions of the RPS and ESFAS system. So, some of those auxiliary supporting things that are typically outside the cabinets that house most of the signal processing and logic.

And they're further delineated with another clause that says, we're expecting that there are no inter-connectivity among these things that are being added or replaced.

And if there are some inter-connectivities, there's some additional guidance to go to to figure out what to do to minimize the impact of a potential hazard due to that inter-connectivity.

CHAIRMAN BROWN: Well, the nuance that you just brought up relative to replacing a power supply --

MR. RAHN: Yes.

CHAIRMAN BROWN: -- or a sensor that feeds like a pressure detector and/or whatever other sensor you may pick --

MR. RAHN: Yes.

CHAIRMAN BROWN: -- if it's a different

1 type or style, what have you, that certainly did not
2 come out in this. The way I read this was that it was
3 virtually anything connected with the arc reactor trip
4 and --
5 MR. RAHN: Yes. So --
6 CHAIRMAN BROWN: -- ESFAS would be
7 prohibited.
8 MR. RAHN: You're probably looking at the
9 version that we sent --
10 CHAIRMAN BROWN: Well, I don't know what
11 version --
12 MR. RAHN: -- in March, I think.
13 CHAIRMAN BROWN: -- there's no date on
14 this.
15 MR. RAHN: Yes.
16 CHAIRMAN BROWN: Okay.
17 MR. RAHN: So, there was a version --
18 CHAIRMAN BROWN: There's an ML number on
19 it, but that's all.
20 MR. RAHN: And, again, language has changed
21 a little bit.
22 MS. ANTONESCU: The last week of February,
23 they had that version up.
24 CHAIRMAN BROWN: Well, I don't -- this one
25 actually had an ML number. The date was February 16,

2018.

MR. MORTON: Charlie, this is Wendell Morton, NRC.

CHAIRMAN BROWN: Yes.

MR. MORTON: So, the original RIS, and the reason why we're trying to get that nuance is the original RIS basically took RPS and ESFAS off the table.

CHAIRMAN BROWN: Not the Supplement, the initial?

MR. MORTON: Not the Supplement --

CHAIRMAN BROWN: Yes.

MR. MORTON: -- the original main one. So, part of the effort to put that nuance in there, to say that the staff does find that there are some systems being replaced to be acceptable.

As Dave was alluding to, those things, transmitters, power supply centers, et cetera, without affecting the specific logic or decision-making portions of the systems.

Now, that clarification is being more refined in the version that's currently in-house, it's been refined from that one.

CHAIRMAN BROWN: It's not in this one?

MR. MORTON: Yes, it's been refined from

1 that version that you have right there.

2 CHAIRMAN BROWN: You mean, it was in this

3 one, but it's being more refined? Because I didn't

4 see that.

5 MR. MORTON: It's clarifying that point

6 that you just raised.

7 CHAIRMAN BROWN: I didn't even see it

8 mentioned as these other things could have possibly

9 slipped in in this particular version, in this

10 February issued version. I totally missed it if it

11 was. I did read every page.

12 MR. MORTON: Yes, subsequent to that

13 version.

14 CHAIRMAN BROWN: I was awake most of the

15 time.

16 (Laughter.)

17 MR. MORTON: I don't doubt that.

18 MR. WATERS: Yes. So, as I was mentioning,

19 you are looking at an older version and it is

20 evolving. I will note that, we have scheduled a

21 public meeting next week to talk about the current

22 draft, because we're on the verge of releasing a new

23 version today. It's not out yet.

24 And what we can do is, once it's released,

25 we can, it'll be after the meeting of course, we can

1 feedback to Christina, to highlight that portion that
2 Wendell and Dave were talking about to make it crystal
3 clear to you.
4 The version you're looking at, the wording
5 has indeed changed, we just can't stop public --
6 MS. ANTONESCU: We used the latest public
7 --
8 MR. WATERS: Right --
9 MS. ANTONESCU: -- version available.
10 MR. WATERS: -- the latest public version.
11 CHAIRMAN BROWN: Okay. Well, when we talk
12 about this, whichever next meeting we talk about this,
13 with the full Committee, that nuance ought to be --
14 MR. WATERS: Yes, we'll --
15 CHAIRMAN BROWN: -- discussed.
16 MR. MORTON: Yes.
17 CHAIRMAN BROWN: I think the upcoming
18 meeting in June is primarily to make sure we get the
19 ISG-06 --
20 MR. WATERS: Right.
21 CHAIRMAN BROWN: -- that's the primary
22 focus of that meeting.
23 MR. WATERS: Right, and --
24 CHAIRMAN BROWN: I haven't seen an agenda
25 yet for the June --

1 MS. ANTONESCU: 20th.

2 CHAIRMAN BROWN: -- no, for the June, for

3 the full Committee, we haven't set that up yet.

4 MS. ANTONESCU: Oh, no.

5 MR. WATERS: So, timing is a challenge,

6 because we're dedicated to get the RIS issued by May

7 31. So, we'll have the final RIS by then as well.

8 And --

9 CHAIRMAN BROWN: Oh, you're going to issue

10 this by May --

11 MR. WATERS: Yes.

12 CHAIRMAN BROWN: -- permanently?

13 MR. WATERS: Yes.

14 MR. MORTON: Yes.

15 CHAIRMAN BROWN: That's interesting. Well,

16 it's too late then, they've issued it May 31, it's

17 already out. Well, send us a copy.

18 MR. WATERS: Absolutely.

19 CHAIRMAN BROWN: And I'll see if we ad-lib

20 it in the June meeting.

21 MR. WATERS: Well, and I plan to talk about

22 it -- the next phase of the 50.59 issues will be

23 resuming our review of a separate NEI document called

24 Appendix D 96-07.

25 Right now, today, we anticipate that we

1 will incorporate some of the -- we've asked -- it's
2 NEI's document, but some of the features and concepts
3 in this RIS will be incorporated into that Appendix D.
4 We've not had a discussion with NEI yet on
5 that, but that may be another opportunity to discuss
6 some of these issues regarding the applicability of
7 qualitative assessment.
8 CHAIRMAN BROWN: Okay. The term
9 sufficiently low, there's another term in the
10 Supplement, I'm trying to find it, I know I had it
11 underlined, but it seemed like the likelihood
12 thresholds were sufficiently low, or whatever they
13 were, were fundamentally based on qualitative
14 assessments by engineering evaluations. Which seems
15 to be bass-ackwards.
16 If you're going to make an assessment of
17 not requiring a License Amendment, based on
18 qualitative stuff, as opposed to a technical
19 engineering evaluation, and then, following that up
20 with a qualitative assessment of that evaluation --
21 MR. WATERS: Yes, I'll let --
22 CHAIRMAN BROWN: -- that's --
23 MR. WATERS: I'll let Wendell chime in for
24 details.
25 CHAIRMAN BROWN: I might be getting ahead

1 of you, I don't know.

2 MR. WATERS: Well, the version last year,

3 it kind of intermingled the qualitative assessments

4 issues with some technical evaluation issues.

5 The 50.59 criteria, as promulgated by the

6 Commission, allows the use of qualitative engineering

7 judgments to make some of the findings within the

8 specific criteria for 50.59, such as: does the

9 likelihood of a malfunction increase, there's a new

10 type of malfunction?

11 With that said, we all recognize that

12 before we even get to that licensee and that

13 determination, there will be some supporting

14 engineering analysis to help provide that licensing

15 person that basis.

16 But in this newest version of RIS, we're

17 very careful to kind of separate those two elements.

18 And I'll let Wendell chime in with any more.

19 MR. MORTON: Yes. So, basically, and I'm

20 going to -- the qualitative assessment, it's based on

21 the technical engineering product in place. So, it's

22 not just a qualitative assessment of what someone

23 thinks, it's based upon the product that's already

24 been designed.

25 So, if you have an engineering design

1 change package and you have a certain amount of design
2 features, you have design processes used, whatever
3 operating experience you have used as part of your
4 design package, you take that information and you fill
5 in the details in terms of the qualitative assessment
6 factors and categories.
7 So, if you have a particular design, you
8 have a particular CCF vulnerability identified. As
9 part of the design package, as part of the qualitative
10 assessment, you would be looking at if you have
11 particular design features in place to address said
12 vulnerability.
13 That's part of the assessment. But the
14 assessment takes place after the design, not prior to
15 it. So, it's not based on -- it is based on the
16 design and the technical work first, and then you do
17 your qualitative assessment in order to support the
18 licensing decision. And then, the sufficiently low
19 term --
20 CHAIRMAN BROWN: By the licensee?
21 MR. MORTON: By the licensee.
22 CHAIRMAN BROWN: Okay. It was difficult to
23 glean this out of the Supplement. I'm sorry to say
24 that, but with just 17 pages of stuff, it was hard to
25 derive that conclusion.

1 MR. WATERS: No, we appreciate that. And
2 that's some of the commentary we got when we issued
3 for public comment, we actually issued twice for
4 public comment. My personal observation, 50.59 is a
5 unique regulation.
6 There are some challenges, I'm an
7 engineer, I overview licensing, and that's been part
8 of the challenge that Dave and Wendell are working on
9 to explain it.
10 CHAIRMAN BROWN: Go ahead.
11 MR. WATERS: Slide 7, again, I believe we
12 discussed some of these last year. These are
13 examples. This is an example, there's more examples
14 of actual RIS qualitative factors that can be used to
15 lead to a CCF sufficiently low determination, which
16 would therefore move the criteria for 50.59.
17 We believe the use of design attributes to
18 probably be the most significant factor in addressing
19 potential CCF issues. Again, there's nothing binding
20 in this list for the licensee to use, but these design
21 attributes could include inherent diversity, things
22 like automated self-testing and watchdog timers.
23 We also recognize the use of standards and
24 industry practices, specifically to improve the
25 quality and reliability of digital components. And

1 how operating experience can be used to demonstrate
2 the performance and reliability of the digital design.
3 CHAIRMAN BROWN: Why is it an assessment of
4 that design attribute? Why doesn't that fall under
5 the category of an engineering evaluation? I mean, if
6 you've got redundancy and you've got watchdog timers
7 to control this to make sure it processes and if
8 you've got self-checking that does certain things,
9 don't those --
10 MR. WATERS: I'll let Dave give you the
11 answer. I think, from reality, it will be both
12 evaluated as part of the engineering evaluation
13 package that the licensee does to design and build the
14 system.
15 But at the end of the day, for the
16 qualitative assessment that one has to justify that I
17 have met the 50.59 criteria, again, they'll have to
18 address these, that I have these things. So, I think
19 it will be addressed both, but I will let Dave chime
20 in to make sure --
21 MR. RAHN: Yes.
22 MR. WATERS: -- I didn't miss anything.
23 MR. RAHN: Thank you. Yes, again, this is
24 David Rahn. So, I can see where you are getting the
25 impression that all we are doing is a qualitative

1 assessment, because the flow of the document talks
2 about that first.
3 But in reality, every design modification
4 has to go through an engineering evaluation process,
5 which is a very rigorous process. It starts with a
6 failure analysis, either FMEAs or other types of --
7 there's newer ways of evaluating some of these. But
8 then, there's also a defense-in-depth analysis of
9 this.
10 In some cases, there may be needs for
11 evaluating the potential effects of these failures.
12 And in all cases, all these engineering evaluations
13 are completed prior to the performance of any
14 qualitative assessment.
15 So, the qualitative assessment then weighs
16 the results of all these engineering evaluations,
17 along with what one knows about the potential
18 operations of the system, due to its operating
19 experience and the methods by which it was developed,
20 what kind of quality was put into it.
21 And the aggregate of all those things are
22 what goes into the decision-making in this qualitative
23 assessment, which then helps you support a decision as
24 to whether there is a sufficiently low likelihood of
25 a failure, which enables you to answer the most

1 critical 50.59 questions.

2 MEMBER BALLINGER: Tell me how any of these

3 are qualitative.

4 MR. RAHN: So, there is a potential -- what

5 was the question?

6 MEMBER BALLINGER: How are any of those --

7 MR. RAHN: Yes, so --

8 MEMBER BALLINGER: -- qualitative --

9 MR. RAHN: -- at some point in time --

10 MEMBER BALLINGER: How are they

11 qualitative?

12 MR. RAHN: At some point in time, there's

13 always an unknown unknown regarding the software,

14 whether there are potential latent failures that may

15 be embedded in that software.

16 MEMBER BALLINGER: Well --

17 MR. RAHN: And the qualitative judgment

18 you're making is more associated with the whole

19 package, the design attributes that you put into it

20 and what you may or may not know about whether there's

21 any embedded software errors in the system.

22 MEMBER BALLINGER: Okay. I understand

23 that, but independence is not qualitative. It either

24 is or isn't.

25 MR. RAHN: That's something that --

1 MEMBER BALLINGER: Same for all the others.
2 MR. RAHN: -- you evaluate. You evaluate
3 that first, it's an engineering judgment. It's not a
4 judgment, it's a determination that you made based on
5 the design attributes that you've included in the
6 system.
7 MR. WATERS: Next slide?
8 CHAIRMAN BROWN: I guess.
9 MR. WATERS: So, in summary, the initial
10 draft was issued for public comment last July 2017.
11 We issued a second draft for public comment this past
12 March. We had approximately 60 public comments from
13 seven commenters.
14 And as I noted at the beginning, we are
15 actively resolving these comments and we're looking to
16 finalize the RIS, we intend to issue it by May 31,
17 2018.
18 One thing to note is, once we issue the
19 RIS, our work is not done. We intend to conduct
20 inspector training on digital upgrades performed under
21 50.59 with this RIS. And we hope to follow up with
22 workshops with industry to discuss additional uses of
23 this RIS for the specific types of upgrades they're
24 looking at.
25 Also, we intend to update BTP 7-19 in the

1 future, that is not part of this RIS. BTP 7-19 is
2 staff guidance specifically for evaluating common
3 cause failure in License Amendment Requests before the
4 NRC.
5 However, we do expect to incorporate some
6 of the concepts and lessons from that RIS into a
7 future update making BTP 7-19 applicable to all the
8 range of safety systems that we may look at. With
9 that, I'll turn it back over to Mauricio.
10 CHAIRMAN BROWN: Is NEI 16-16 involved in
11 this 50.59 process? I thought that was supposed to be
12 given to us at one time and it addresses, that's the
13 industry, I guess, paper on CCF, which I guess that's
14 still in transition?
15 MR. WATERS: I don't want to steal
16 Mauricio's -- that's what he's going to talk about
17 next. Right now, we're not looking at NEI 16-16,
18 we've been asked to halt our review on that.
19 CHAIRMAN BROWN: Yes, I understand that.
20 MR. WATERS: I think, conceptually, when it
21 was delivered and we were working on the RIS in
22 parallel, it became kind of intuitively that the RIS
23 focuses on design attributes and design quality
24 processes.
25 Again, I think they were thinking 16-16

1 would help define what are acceptable design
2 attributes in more detail in a systematic manner that
3 would complement that. But I just told you what
4 Mauricio is going to tell you. So, I'll turn it over
5 to him and he can elaborate some more.
6 MR. TANEJA: Yes. What you heard, you said
7 you heard previously, NEI 01-01, we had some concerns
8 with the way it was being used by the industry. And
9 one of the solution that NEI proposed was that they
10 were going to take back NEI 01-01 and replace it with
11 Appendix D to 96-07, which is the 50.59 criteria, and
12 a technical companion document.
13 And NEI 16-16 was intended for that
14 purpose initially. That's really probably what you
15 heard back then. And I guess it's been evolving.
16 Let's put it this way --
17 CHAIRMAN BROWN: I'd forgotten all that.
18 MR. TANEJA: Okay. But that's probably
19 what you heard. So, it was initially intended to be
20 separate out the technical into a separate document
21 and put the regulatory information in Appendix D.
22 MR. THOMAS: Yes. Let me -- this is Brian
23 Thomas. Let me just chime in a little bit.
24 CHAIRMAN BROWN: Could you use the mic?
25 MR. THOMAS: You mentioned the CCF guide.

1 CHAIRMAN BROWN: Could you give you -- oh,
2 you gave your name, thank you. I'm trying to --
3 MR. THOMAS: Yes. But you --
4 CHAIRMAN BROWN: -- I'm moving slowly right
5 now.
6 MR. THOMAS: You mentioned the EPRI CCF
7 Guide. The EPRI CCF Guide was communicated to us as
8 being the basis, if you will, document that they were
9 planning to use as the basis to develop NEI 16-16.
10 So, Dinesh is correct, 16-16 is evolving.
11 We've heard different information, if you
12 will, from NEI, in terms of what's the construct of
13 16-16? But you are correct, the CCF Guide, the EPRI
14 document that was published, was the one that was
15 referred to as an underpinning, if you will, baseline
16 information that would be captured in 16-16.
17 CHAIRMAN BROWN: So, it's still pending?
18 It's pending also then, it's not an EPRI document yet?
19 MR. THOMAS: No, they issued a CCF Guide,
20 EPRI did.
21 CHAIRMAN BROWN: That's the 2005 --
22 MR. THOMAS: Yes, the --
23 CHAIRMAN BROWN: -- 2005 --
24 MR. THOMAS: Yes, the 3258 --
25 CHAIRMAN BROWN: -- 326, all those numbers?

1 MR. THOMAS: Yes, some odd number, yes.
2 That was the CCF Guide. And it was indicated that
3 that would be used as the baseline for the development
4 of 16-16.
5 But 16-16, as Dinesh said, is still
6 evolving. And that was part of our focus, was to help
7 get some clarification as to the purpose and scope of
8 that document.
9 CHAIRMAN BROWN: It just seems to me, the
10 whole CCF issue is eating you guys alive, so you try
11 to define how the world will cope with it and by the
12 time you read the RIS, but the time you look at 01-01,
13 and by the time you look at the old, some version of
14 16-16, whatever, the EPRI documents, et cetera, that
15 there’s more papers than you can shake a stick at.
16 MR. WATERS: I guess the challenge then of
17 course is a diversity of type of I&C systems, not just
18 RPS and ESFAS. And then there's the 50.59 allowances
19 to make changes, NRC approval, then our normal law
20 review processes. And it creates a multidimensional
21 problem, so you're -- it is eating me alive, but I've
22 gained weight over the time, so I'm not sure if it's
23 working, but I'll let Mauricio finish up any of the
24 NEI 16-16 known facts.
25 MR. GUTIERREZ: Okay. So I'll maybe

1 repeat some of the stuff that's been said and add a
2 little more detail to the conversation here.
3 So NEI 16-16 is guidance for addressing
4 digital common cause failure, and NEI is developing
5 this document to support industry's response to NRC's
6 activities on protection against CCF and digital I&C
7 systems. This document, the NEI 16-16, intends to
8 provide technical guidance on addressing CCF for
9 compliance to deterministic licensing criteria and NRC
10 policies and positions articulated in documents such
11 as SRM to SECY 93-087 and BTP 7-19.
12 The draft of the document was first
13 provided to us in December of 2016 with the
14 understanding that an NRC endorsement would be sought
15 when the document was more fully developed. The
16 guidance in NEI 16-16 includes an appendix with a
17 defense of measures, or attributes as it's called in
18 other places, that can be credited in addition to
19 those in current staff guidance, specifically guidance
20 in SRP BTP 7-19; includes two criteria which if
21 satisfied can be used to eliminate from further
22 consideration the potential for software CCF based on
23 a demonstration that adequate internal diversity
24 exists or based on assurance that the systems are
25 sufficiently simple that all possible logic failure

1 paths can be tested for and shown to be non-existent.
2 And was stated earlier, NEI 16-16 is based
3 on the EPRI technical report on bullet three on this
4 slide, which is often referred to as the CCF Guide.
5 We'll note that EPRI has not requested a review or
6 endorsement of this topical report. That's separate
7 from the NEI 16-16 document.
8 CHAIRMAN BROWN: So fundamentally the only
9 guidance right now is 01-01 plus the supplement with
10 RIS 2002-22, and now then with the supplement? That
11 will be the existing guidance that licensees have?
12 MR. TANEJA: Well, the NEI 01-01 is hard
13 to do a change under the 50.59 rule for digital
14 upgrades. So it really doesn't specifically go into
15 the CCF concerns alone. 01-01 is how do you do a
16 digital upgrade in a plant using the 50.59 process?
17 So the RIS that endorsed --
18 CHAIRMAN BROWN: That's a screening
19 process now, right?
20 MR. TANEJA: Well, screening and
21 evaluation.
22 CHAIRMAN BROWN: No, I know, but it's
23 really screening to determine whether you need to do
24 an LAR or an amendment --
25 (Simultaneous speaking.)

1 MR. TANEJA: Exactly. Exactly. So that's
2 what the intent of the 01-01 is. And I think we
3 endorse it using the RIS. And what we are trying to
4 do is provide a supplement to clarify how you really
5 do those. Answering those 50.59 questions you have to
6 understand your design, digital I&C design so you can
7 answer those questions in earnest. And I think we are
8 helping the engineer or the licensing person to
9 earnestly answer those questions by providing the
10 supplement.
11 So it's not exclusively CCF. CCF was the
12 main concern that was causing problems answering those
13 questions. So the intent was take the regulatory part
14 out of 01-01, put it in Appendix D, take the technical
15 part of it out of and come up with a separate
16 technical document. And 16-16 is intended for that
17 purpose which essentially becomes a CCF, dealing with
18 CCFs, software CCFs. Correct me.
19 MR. WATERS: No, I mean -- and just to
20 reiterate what Dinesh said, if you can't tell by now,
21 we're looking at -- we have to look at two buckets:
22 what are -- what's the licensing guidance and what's
23 the technical guidance? The licensing right now we
24 have is the RIS supplement which clarifies endorsement
25 of 01-01. The technical guidance is -- I guess on the

1 street there is EPRI guidance right now for
2 dependability for digital I&C system CCF, and the NEI
3 16-16, which they are asking us to endorse at some
4 point in the future, however, that's on hold
5 indefinitely to my understanding at such time that I
6 guess EPRI revises their approach.
7 CHAIRMAN BROWN: Is the -- that EPRI
8 document, is that a CCF document also?
9 MR. GUTIERREZ: Yes, the EPRI document
10 here, the TR --
11 CHAIRMAN BROWN: All the numbers --
12 MR. GUTIERREZ: -- that's --
13 CHAIRMAN BROWN: -- 33 -- ending in 322?
14 MR. GUTIERREZ: Yes, that's referred to as
15 the CCF Guide.
16 CHAIRMAN BROWN: Okay.
17 MR. AUSTIN: Rob Austin with EPRI, if I
18 may? So just to clarify our guide a little bit and
19 its purpose and its future. So just wanted to be
20 clear. This is -- it's a regulatory agnostic
21 technical process, so it's deliberately silent on
22 licensing. EPRI is a non-profit public interest
23 research group. It's a technical guide, a technical
24 engineering guide. It addresses CCF from many sources
25 as informed by our studies and operating experience,

1 not just software.

2 And I think we've talked about this to

3 this Committee about that guide when it was still in

4 draft form a couple years ago. It's a combination.

5 It really provides an approach to combine mitigating

6 measures, coping measures as well as the defensive

7 measures, which are now called preventive or limiting

8 measures, Ps and Ls, with the guide.

9 Now 16-16; and Jason Remer can speak more

10 to that, but that's a separate guide. It's

11 independent. It uses a section, a list of defensive

12 measures from the EPRI Guide. Just lifted it out of

13 the EPRI Guide, dropped it into 16-16.

14 Now the EPRI Guide has a process with

15 risk-informed hazards analysis as an engineering

16 process. Again, it's independent of licensing. So we

17 are revising it, but it's not going to be a major

18 change. Really what changes we're making, that will

19 start later this year and then wrap up next year.

20 What we want to do is incorporate process

21 improvements, bring it in tighter with our digital

22 engineering guide, which across the U.S. industry

23 plants are adopting as how they do digital mods. So

24 we want to work in those considerations seamlessly

25 into the mod process and the design process including

1 interactions between utilities and vendors.

2 Want to bring in -- we're continuing our

3 research in assistance engineering and hazards

4 analysis, so we have some refinements that we want to

5 bring into the guide, kind of crisp up how you can

6 address hazards. And finally we want to make the Ps

7 and Ls more performance-based, less prescriptive.

8 CHAIRMAN BROWN: Ps and Ls?

9 MR. AUSTIN: Sorry. Preventive and

10 limiting measures, defensive measures. Sorry.

11 Nothing like a new term. It's probably not on

12 Mauricio's list of acronyms either, so -- but we want

13 to make those --

14 CHAIRMAN BROWN: What was it again?

15 MR. AUSTIN: Ps and Ls?

16 CHAIRMAN BROWN: Yes, shows my retention

17 capability.

18 MR. AUSTIN: Yes. Preventive and limiting

19 measures.

20 CHAIRMAN BROWN: And limiting measures.

21 MR. AUSTIN: So in short, a preventive --

22 there's a -- a preventive measure would -- and this is

23 high-level. A preventive measure can reduce the

24 likelihood of an event occurring, a mitigation measure

25 -- mitigative measure reduces the impact if it does

occur, and a limiting measure sometimes kind of falls in the middle. Some of that's in the eye of the beholder.

So I want to note, too, though as we go through and you look at the EPRI Guide, it's not all about software common-cause failure. Again, it's based upon the EPRI operating experience failures we consider, sources of failure from multiple sources as informed by our operating experience studies. That's why, although it's known as the EPRI CCF Guide, you don't see CCF in the title.

Just point out the OE studies by EPRI, both in the U.S. and abroad, have shown that the prevalence of software common-cause failure is low. when we've looked at risk impacts of the CCF if it does occur for existing reactor designs the ones we've looked at it's expected to be low-risk significance, low increase in core damage frequency.

So we're really focused with our research on making sure that it's effective and efficient systems engineering processes. Taking CCF into account would also be taking into account the other sources of failure and problems that the operating experience has shown. So -- but we are revising the guide, but it's not a radical revision.

1 CHAIRMAN BROWN: It's going to have a new
2 number?
3 MR. AUSTIN: It will have a new number,
4 but it will still be long.
5 (Laughter.)
6 MR. AUSTIN: I'm going to go check though.
7 I believe ADAMS numbers are longer.
8 (Laughter.)
9 CHAIRMAN BROWN: Thank you.
10 MR. AUSTIN: Let me know if there are any
11 questions on the EPRI Guide or --
12 CHAIRMAN BROWN: Oh, yes, there's --
13 MR. AUSTIN: -- if that was at all helpful
14 or --
15 CHAIRMAN BROWN: No, it all depends on
16 what the definition of "helpful" is.
17 (Laughter.)
18 MR. AUSTIN: Thank you.
19 CHAIRMAN BROWN: Yes.
20 MR. GUTIERREZ: Okay. So continuing on,
21 as stated earlier, NEI provided their first draft of
22 NEI 16-16 for potential endorsement later on in
23 December 2016. The second draft was provided to NRC
24 in May 2017. NRC and NEI held several joint meetings
25 to resolve comments on both draft 1 and draft 2 of NEI

16-16. In February 2018 NEI requested that NRC pause review of the document to free up resources for the RIS 2002-22 Supplement 1 effort and to allow EPRI to revise their CCF Guide. No further work has been done on NEI 16-16 by the staff since we were asked to pause the review, but we will reengage when engaged by NEI.

If it's okay to proceed, let's move to the next slide.

MEMBER REMPE: I had a question that I should have asked a minute ago, but this EPRI Guide, is it free or is it --

MR. GUTIERREZ: No.

MR. TANEJA: Very expensive.

(Laughter.)

MEMBER REMPE: Yes, so you guys are endorsing something that --

MR. TANEJA: No.

MEMBER REMPE: Okay.

MR. GUTIERREZ: So the document that we're considering for endorsement is NEI 16-16 --

MEMBER REMPE: Right.

MR. GUTIERREZ: -- which uses a portion that's pulled out from the EPRI CCF Guide.

MEMBER REMPE: And that's clearly pulled

1 out, so it's available --

2 MR. GUTIERREZ: Yes.

3 MEMBER REMPE: -- for free to somebody?

4 MR. GUTIERREZ: Yes.

5 MEMBER REMPE: Okay. Thank you for that

6 clarification.

7 MR. GUTIERREZ: That appendix is available

8 in draft 2 of NEI 16-16.

9 MEMBER REMPE: Thank you.

10 MR. AUSTIN: The -- and by the -- the EPRI

11 Guide, I don't think it's free. We didn't make it

12 free and public. We did price it attractively,

13 similarly priced to a standard. I believe NRC has a

14 copy somewhere, so --

15 MEMBER REMPE: I just was curious because

16 we've had that issue before in other areas where staff

17 would endorse something relying on an EPRI document.

18 And I think that's kind of taboo from what my

19 impression was before. So thank you for the

20 clarification.

21 MEMBER BALLINGER: Three hundred bucks.

22 MEMBER REMPE: That's not bad. It's not

23 300K.

24 (Laughter.)

25 CHAIRMAN BROWN: Why is that attractive?

1 MEMBER REMPE: After you buy a new sweater
2 you can buy the EPRI document.
3 (Laughter.)
4 CHAIRMAN BROWN: That's why I don't have
5 a copy of it.
6 MEMBER REMPE: Sorry.
7 MR. GUTIERREZ: So now I'd like to provide
8 a status update on the activity for implementing the
9 Commission policy.
10 The staff will update guidance documents
11 to ensure that the Commission policy in SRM to SECY-
12 93-087 continues to be consistently applied and
13 addresses evolving digital I&C technologies.
14 The staff is not proposing nor requesting
15 a change to Commission policy. It may be we may gain
16 more information when it's taken in the holistic
17 context of activity MP 4B and we consider any feedback
18 from the Transformation Team output.
19 The staff is developing a Commission
20 Information SECY on future improvement efforts in
21 addressing CCF.
22 Next slide. So I'd like to turn it over
23 to Dinesh Taneja.
24 MR. TANEJA: This is Dinesh. Thank you,
25 Mauricio.

1 So due to the evolving nature of digital
2 I&C technologies and their implementation in new and
3 operating reactors, safety review -- staff review of
4 guidance BTP 7-19 has been updated a number of times
5 to address acceptable means for protecting against
6 potential digital I&C common-cause concerns. The last
7 significant update to BTP 7-19 captured the Interim
8 Staff Guidance on CCF that was developed during 2006-
9 2007 time frame in coordination with NEI and other
10 stakeholders.
11 Staff evaluated all of the BTP 7-19
12 updates and took into consideration issues raised by
13 the licensees, NRC inspectors, technical reviewers and
14 other stakeholders in implementing digital I&C designs
15 in accordance with the SRM to SECY-93-087 and is
16 proposing five points that are listed on this slide in
17 updating the staff guidance for consistent application
18 of the Commission policy moving forward.
19 So we still expect licensees and
20 applicants of test and research reactors, operating
21 reactors and new reactors to continue to address
22 potential software CCF concerns. Like Mauricio
23 mentioned, Commission policy on the software CCF
24 should continue to remain in place without any
25 modifications. And a D3 analysis is required to be

1 performed for RPS and ESFAS to address CCF concerns.
2 So this analysis can either be a best
3 estimate that is using realistic assumptions or a
4 design-basis analysis as is appropriate and also allow
5 graded approach for D3 analysis for less safety-
6 critical systems. Examples would be like in control
7 room HVAC chillers. They are considered safety-
8 related, but they are not as critical as RPS or ESFAS.
9 So there's some graded approach allowed in that area
10 when we do the D3 analysis.
11 Clarify the use of alternate means to
12 address CCF concerns. That is that a CCF concern can
13 be addressed by both safety and non-safety systems of
14 sufficient quality to perform the necessary function
15 in a realistic manner for the associated event under
16 consideration.
17 And then allow use of certain design
18 attributes to address CCF concerns. Currently the BTP
19 7-19 has two measures given in there which eliminates
20 the CCF from consideration. One is the demonstrated
21 diversity. The other is the adequate testing. And
22 it's simple enough where we can test it -- essentially
23 100 percent testing to assure that there is no
24 potential CCF concerns in that software. So what we
25 are looking into is to -- enlarging that attributes to

1 consider some other technical areas that may be
2 considered to alleviate that concern.
3 So these are the five points that we are
4 proposing to take into consideration in writing this
5 Information SECY paper and applying the SRM to the
6 SECY 93-087 consistently across operating reactors,
7 new reactors, new designs, digital upgrades. So it's
8 across the board.
9 CHAIRMAN BROWN: What do you mean by 100
10 percent testing?
11 MR. TANEJA: Well, that's what we say in
12 BTP 7-19 that --
13 CHAIRMAN BROWN: I know, but what is it?
14 MR. TANEJA: Design is simple enough where
15 you can test it thoroughly and adequately to say that
16 there are no latent defects in this piece of device.
17 So if that is the case, then you don't have to worry
18 about CCF. That's what we say in BTP 7-19. And so
19 the interpretation of that has been out there and it's
20 been interpreted differently by different people.
21 Hey, is it simple enough? Is it too complex? There
22 are so many lines of code. Can you test all these
23 stages? And so we're going to work on that to get
24 that --
25 CHAIRMAN BROWN: Do you test every line of

1 code for every bit combination in a field that could
2 come in? And if you've got a 32 or 64-bit processing
3 system, I think if you do the combination or whatever
4 it is of that, you're talking several million
5 combinations of which the only way to test that would
6 be a high-speed computer that would spit out bits for
7 a year-and-a-half and get halfway through. I'm
8 exaggerating obviously to make a point.
9 MR. TANEJA: Right. Point well-taken.
10 CHAIRMAN BROWN: So 100 percent testing is
11 virtually impossible.
12 MR. TANEJA: Yes.
13 MR. WATERS: I think we recognize it as a
14 very limited practical applicability for what we're
15 seeing, but we -- when we wrote BTP 7-19, we left that
16 option if there was something very simple as a
17 potential option, but we understand it has very
18 limited applicability to what's being done out in
19 the --
20 (Simultaneous speaking.)
21 CHAIRMAN BROWN: That's why you should use
22 6800's 8-bit processors and have a custom code which
23 only has 2,000 lines of code and you might get there.
24 MR. TANEJA: Well --
25 CHAIRMAN BROWN: That's just an example of

1 being able to --

2 MR. TANEJA: -- the exhaustive testing can

3 be done on relatively simple systems. I think that

4 was the position there. So you don't have to worry

5 about doing a D3 analysis and say, hey, I can treat

6 this thing like I would an analog or another device

7 where I have a predictable performance.

8 CHAIRMAN BROWN: It would never be

9 considered if you get 100 percent test a reactor trip

10 system or a safeguards system.

11 MR. TANEJA: Well, that's why we said that

12 we do need a D3 analysis for the reactor trip --

13 (Simultaneous speaking.)

14 CHAIRMAN BROWN: Yes, I got that. That's

15 why I --

16 (Simultaneous speaking.)

17 MR. TANEJA: So, that's really where we

18 are saying that, yes, no, those --

19 CHAIRMAN BROWN: You're defaulting to

20 another approach effectively to -- so you look at

21 defense --

22 MR. TANEJA: Consequences of a high risk.

23 CHAIRMAN BROWN: -- diversity of defense-

24 in-depth.

25 MR. TANEJA: Where are the consequences of

1 high risk? Yes, we want that level of defense-in-
2 depth.
3 CHAIRMAN BROWN: Okay.
4 MR. TANEJA: So let me turn it back to
5 Mauricio.
6 MR. GUTIERREZ: Okay. So our next steps
7 on the MP 1C activity here. We're going to hold
8 stakeholder interactions. We have a meeting planned,
9 a public meeting planned for next week. We're going
10 to apply the staff clarifications in all activities
11 for regulatory guidance and endorsement activities.
12 So we want to issue RIS 2002-22 supplement for 50.59.
13 And as Mike mentioned, we're aiming for the end of
14 this month to issue the final on that.
15 We're going to continue the review of NEI
16 96-07 Appendix D for 50.59. And our primary mechanism
17 I guess for MP 1C is to update BTP 7-19. And we will
18 review future industry guidance, NEI 16-16, when we
19 are reengaged. And we will -- intend to provide our
20 Info SECY to the Commission in August of 2018, later
21 this year.
22 CHAIRMAN BROWN: On CCF?
23 MR. GUTIERREZ: Yes, this is CCF.
24 CHAIRMAN BROWN: We're going to get to see
25 -- you're going to plan on seeing -- showing that to

1 us?

2 MR. GUTIERREZ: So --

3 MR. WATERS: The answer was we weren't

4 planning on that. It was an information paper, not a

5 policy paper for policy decision. We were essentially

6 going to provide the Commission an update very similar

7 to what you hear a presentation in a SECY inform form

8 is our current plans.

9 CHAIRMAN BROWN: Going to give us a copy?

10 (Laughter.)

11 MR. WATERS: I'll get back to you. I

12 don't think I can commit to that.

13 CHAIRMAN BROWN: I think a good answer --

14 (Laughter.)

15 CHAIRMAN BROWN: I think a good answer is

16 yes.

17 (Laughter.)

18 MR. GUTIERREZ: Next slide. So more

19 broadly the activities and path forward on CCF that we

20 have described support broader agency activities.

21 This includes the work being performed on advanced

22 reactor framework and research being undertaken. We

23 list three projects that are in -- we're developing

24 right now: a project on risk-informed approaches where

25 we will try to assess graded regulatory approaches

1 using PRA risk insights and develop tools and/or
2 guidance for digital I&C risk-informed reviews. The
3 embedded digital devices and evolving technologies
4 project will assess safety implications of EDDs, the
5 embedded digital devices in I&C equipment. They'll
6 assess emerging technologies and develop a technical
7 basis and/or recommendations for guidance for
8 regulating EDDs and emerging technologies.
9 CHAIRMAN BROWN: What do you mean by
10 "embedded digital devices" in this circumstance? How
11 do you define that?
12 MR. GUTIERREZ: So they are devices --
13 CHAIRMAN BROWN: In a microprocessor
14 there's an embedded digital device inside your
15 platform, so --
16 MR. GUTIERREZ: Yes, and I don't think we
17 would consider that an embedded digital device, but we
18 would say it's some other device that stands alone
19 that has its own internal digital components that it
20 requires to operate.
21 CHAIRMAN BROWN: I just lost the bubble on
22 that.
23 MR. TANEJA: An example would be is like
24 an electrical switch gear or even a circuit breaker.
25 Traditionally they have like thermomagnetic over-

1 current protection.

2 CHAIRMAN BROWN: Okay. I understand what

3 you're saying.

4 MR. TANEJA: Or they have digital -- maybe

5 they are simple functions. What do they call them?

6 Dedicated functional features. And that's all they

7 do. But now they use those instead of using the old

8 typical thermal --

9 CHAIRMAN BROWN: Thermal overloads?

10 MR. TANEJA: Overloads or thermal

11 overload-type devices, which is -- and you know that's

12 one example. But now we are seeing them almost in

13 everything. You have them in your washing machine,

14 you have them in --

15 CHAIRMAN BROWN: No, I don't. I've got

16 a --

17 (Simultaneous speaking.)

18 MR. TANEJA: Well, you still have the old

19 -- but see --

20 (Laughter.)

21 MEMBER REMPE: -- by hand.

22 MR. TANEJA: But --

23 CHAIRMAN BROWN: I've got a washboard.

24 MR. TANEJA: I would -- oh, a washboard?

25 Okay.

1 CHAIRMAN BROWN: I'm not sure you even
2 know what a washboard is. You're too young.
3 (Laughter.)
4 MR. TANEJA: Yes, I've seen one. I've
5 never used one.
6 (Laughter.)
7 CHAIRMAN BROWN: I actually used one with
8 my grandmother when I was seven years old, so I know
9 what a washboard is.
10 MEMBER REMPE: Could you elaborate what
11 you're doing for the advanced reactor framework
12 effort? Are you just talking about NuScale? Are you
13 talking about --
14 MR. TANEJA: No, beyond that.
15 MEMBER REMPE: Beyond that? So the non-
16 LWRs? Do they have enough of a design you can really
17 do much in that area?
18 MR. TANEJA: Well, see, we have the
19 evolution with the DSRS that we came up with to do the
20 NuScale review.
21 MEMBER REMPE: Yes.
22 MR. TANEJA: We'll be coming in front of
23 you soon enough with our I&C review for the NuScale
24 design. And so far what I can say is that that review
25 that be performed in accordance with DSRS was

1 significantly much more efficient than the reviews
2 that we performed using the SRP. So there is
3 demonstratedly gain of experience that was utilized in
4 doing that.
5 So now we have in front of us the
6 challenge to get ready for reviewing advanced reactor
7 designs, which are non-light water. They are from
8 miniature reactors to small reactors. There's all
9 variations thereof. So we've been working on coming
10 up with this review framework which is essentially
11 technology-neutral and not only from the reactor
12 technology point of view, but also from the I&C point
13 of view. And that really just focuses on looking at
14 a performance-based way of reviewing that thing.
15 So we've started looking at that thing.
16 Last couple of months we've been kind of brainstorming
17 in that area. So hopefully it's soon enough we can
18 probably show you what we are thinking.
19 MR. BETANCOURT: This is Luis Betancourt.
20 We actually met with the advanced reactor community in
21 a public meeting two weeks ago, but we gave a
22 presentation of this initiative that Dinesh is talking
23 about. Those slides are publicly available and we're
24 happy to show those to you. But the whole idea is
25 that we're evolving in the guidance that we want to be

ready when these non-light water reactors come in, because right now the only thing that they have is the SRP, which is system-based. The DSRS has actually changed that from a system-based fundamental design principle, and we want to have that available when those applications come in. So that's basically -- we just want to be prepared when they come in.

MEMBER REMPE: Yes, I would appreciate a copy of the slides and I think it should go to more than the Subcommittee. I know Dennis would probably like to see it --

MR. BETANCOURT: Sure.

MEMBER REMPE: -- and perhaps Mike. So --

MR. BETANCOURT: Yes, we want --

MEMBER REMPE: -- send it to Christina, and then we'll get it around, please.

MR. BETANCOURT: Sure.

MEMBER REMPE: Thank you.

MR. BETANCOURT: Yes.

CHAIRMAN BROWN: DSRS, we know what that is. If I didn't know any better -- design-specific? I didn't know whether Vesna knows or not. Design-specific review --

MR. TANEJA: Standard.

CHAIRMAN BROWN: Standard? Oh, thank you

1 for the word "standard."

2 MR. GUTIERREZ: And the last sub-bullet we

3 have there for our developing research project is the

4 technical basis for common-cause failure. We will

5 assess insights on latent design error hazards and

6 uncertainties, technical approaches for addressing

7 hazards and international approaches for addressing

8 common-cause failure. And we're looking to develop

9 the technical basis for future guidance and framework

10 development.

11 And that concludes our presentation.

12 Thank you for your attention and your insights. Are

13 there any questions?

14 CONSULTANT HECHT: I have a question.

15 Getting back to the definition of an "embedded digital

16 device," I think the last time this issue was

17 discussed John Stetkar brought up the issue of

18 chillers, of replacement of the chillers with those

19 digital components, and I assume that you're

20 attempting to address that problem by separate

21 guidance for these embedded digital devices. Is --

22 MR. WATERS: Well, I wouldn't say this is

23 about our review of the chillers per se. It's more

24 about the fact that embedded digital devices are being

25 implemented in the plant. There are some examples.

1 There's been an evolution and she's
2 learned some lessons, we've learned some lessons.
3 First and foremost was awareness that some of the
4 component replacements -- they were -- I know one
5 example, there was a part for part, but that the
6 vendor had put in a -- embedded his device without
7 anyone's awareness, and then there was an issue. So
8 I think industry is involved in the past understanding
9 of that.
10 But the primary thing is recognizing that
11 imbedded design technologies is not a new technology,
12 but it's being implemented in the plant and we want to
13 focus on that and where -- as well as evolving
14 technology to help inform any future infrastructure
15 needs maybe for licensing or maybe for inspection
16 guidance, maybe for commercial grade dedication. So
17 it's more of a broader look. I just want to clarify
18 it's not about specifically a chiller per se. It's a
19 little bit more of a broader holistic look.
20 MR. REBSTOCK: I'm Paul Rebstock from the
21 Office of Research. We're just getting into that EDD.
22 And the definition -- it started out with the idea --
23 like somebody mentioned, the microprocessor in a -- or
24 digital technology embedded in a -- the valve actuator
25 or a circuit breaker or something. But we also

1 realize that it gets bigger than that. Like you --
2 Mike mentioned a chiller where you might have a PLC on
3 board on the chiller. Or you might have a device
4 that's in the -- that has traditionally been not
5 digital, but it's digital controls on a skid. And
6 then we realized, too, that you could go further than
7 that even. And some of those digital controls have
8 communications off of the skid.
9 So we're looking at it from a rather broad
10 standpoint like that of all kinds of digital stuff
11 that shows up where the objective was you didn't go
12 out to something digital. You went out to buy a
13 washing machine, but it has all this digital stuff in
14 it. Or you went out to buy a control room chiller and
15 it has all this digital stuff in it. And so the
16 research that -- what we're looking at is what is all
17 that stuff? What are the possibilities? How should
18 we classify it and what should do about it? And
19 that's really where we're going.
20 So the term has morphed into something
21 considerably bigger than the little microprocessor
22 inside a tiny relay instead of using a pneumatic
23 piston that it started out with. It's kind of broad
24 now.
25 CONSULTANT HECHT: Right, because there

are no -- I guess every vendor is approaching their design problem differently with very cheap microprocessors and very cheap communications devices as a solution and --

MR. REBSTOCK: And part of the problem is they don't always tell you. So you may buy this -- you may buy something and find out -- without knowing that there's something in there --

CONSULTANT HECHT: Yes.

MR. REBSTOCK: -- that you should have worried about.

CONSULTANT HECHT: Okay. Well, that's good that you're looking at it.

MR. REBSTOCK: So that's -- yes, it's kind of a broad scope. That's what we're doing.

CONSULTANT HECHT: Yes.

MR. REBSTOCK: Right? Thank you.

MR. TANEJA: So recently, I think it was a couple of years ago, there was an IE notice that was issued on a timing relay. So the timing relay -- the replacement relay was bought, same exact model number, same look, same everything, form, fit, function, but it did not work. So when they investigated that, what they found out that they replaced a part in that timing relay with a CPLD. But it was susceptible to

1 the EMC environment, so when they put it in that ENC
2 environment killed it. It would not work.
3 So really what happened -- form, fit,
4 function the relay did exactly the same thing because
5 change of that embedded digital component caused it to
6 not work in the given situation where the previous
7 discrete device did perfectly fine.
8 So you are coming up with these type of
9 examples over and over again where you're not even
10 aware of -- typically when you write a purchase order
11 you attach bunch of additional requirements depending
12 on what you're buying. Oh, I meet EQ qualification.
13 So there is an addendum to your purchase order. Give
14 me something that meets this. I need seismic testing
15 done. Another addendum to that.
16 And if there is digital, there is probably
17 an addendum that says give me an EMC testing or give
18 me XYZ testing with it. But if you're specifying a
19 washing machine and you don't expect something, you
20 probably will never ask for that and you'll never get
21 it. And I think those are the areas that are probably
22 getting into now.
23 CHAIRMAN BROWN: You're going to get us
24 that SRM, correct? I mean, that SECY.
25 MR. WATERS: I'll have to get back to you,

1 Charlie. I'm not authorized to make that decision
2 here at the table.
3 CHAIRMAN BROWN: I figured. I just wanted
4 to reemphasize it.
5 (Laughter.)
6 MR. WATERS: Unless something changes
7 there will be more detail in the Info SECY, but the
8 structure and content we present to you and we're
9 going to engage stakeholders next week, so --
10 CHAIRMAN BROWN: I didn't expect it
11 immediately, just -- you're going to give it to them
12 in August. But the Committee is obviously very
13 interested in CCF for this since we have been getting
14 our brains beat out with these meetings --
15 MR. WATERS: Yes.
16 CHAIRMAN BROWN: -- as well as the design
17 approvals that we review. So it would be useful to
18 see what you're telling the Commission about CCF.
19 MR. THOMAS: So Brian Thomas again. Let
20 me chime in here. I feel compelled to.
21 So this is a proposed Information SECY --
22 CHAIRMAN BROWN: Yes.
23 MR. THOMAS: -- that would go up. And I
24 like the way you phrased it earlier. You said you're
25 being eaten alive by CCF. Well, basically it's a SECY

1 that says, yes, CCF is challenging. It's fraught with
2 challenges/concerns coming from all sides, coming from
3 the staff and reflecting also what we're getting from
4 industry. So it's not going to address solutions on
5 anything. That's not the intent of this. It's just
6 to say, hey, these are all the various aspects of CCF
7 that's been bubbling up different concerns, concerns
8 with what's in the SRM 93-087, concerns in terms of
9 what's been -- what industry is experiencing or how
10 they've expressed their challenges, concerns we've
11 embarked upon in involvement of the RIS and so forth.
12 So just recognize this is just an
13 information and we would direct it to make it very
14 short and sheet. So it's an information paper that
15 just goes up that says, Commission, these are some of
16 the things that the staff is wrestling with.
17 MR. WATERS: Yes, and just to reiterate,
18 to add on it, that's -- I think Brian heard us
19 correctly. It's an information status where we're at.
20 And it doesn't stop there. We had obviously -- when
21 we're proceeding with work on BTP 7-19, we would
22 expect to engage the ACRS on that. Down the road if
23 we resume our endorsement or review of future NEI 16-
24 16, we would expect to engage the ACRS on those
25 tentative aspects as well, as well as these research

1 products. As we progress on that; we're just in the
2 very formative stages, we expect to engage the ACRS as
3 well. So we'll get back to you on your question.
4 CHAIRMAN BROWN: Yes, it just sounds like
5 you're going to tell them it's hard.
6 MR. TANEJA: Well, see --
7 CHAIRMAN BROWN: Which comes across. And
8 I'm struggling a little bit. You say how hard it is,
9 but yet we're approving designs, we're going forward
10 with overall concepts and architectures which address
11 the issue of CCF and everything else, and we're not --
12 it's not like we're not doing -- not we -- you are not
13 proceeding on with getting plants licensed. And you
14 will -- or amendments licensed, which you will
15 continue to do in spite of the fact that you don't
16 have a -- you've got all these hard things to deal
17 with. So I mean --
18 MR. BENNER: So I think -- this is Eric
19 Benner. And that's a good encapsulation, so we'll
20 take that a note for our outline. But I think the
21 context of this paper is the Commission in their
22 previous SRM explicitly said, hey, is there something
23 in that SRM 93-087 that needs to be changed and/or is
24 impeding your ability to support digital upgrades?
25 And so we've concluded that while hard

1 there is nothing in that SRM guidance that is impeding
2 our ability to move forward with, like you say,
3 various licensing activities, whether it's initial
4 licenses for new reactors and amendments for existing
5 reactors.
6 So that's sort of our status on it today,
7 but we talked a little bit about we have this MP --
8 this Modernization Plan 4B which is more clean sheet
9 of paper. And when we get into truly looking at a
10 more clean sheet of paper how we might have a
11 framework for licensing digital, that might be the
12 appropriate time to revisit the previous guidance from
13 the Commission on this issue to say there may be
14 benefit to changing that guidance to support a new
15 regulatory paradigm.
16 CHAIRMAN BROWN: But the guidance doesn't
17 prohibit you from doing it now. That's what I heard
18 you say. You're still doing licensing. You're still
19 approving designs.
20 MR. BENNER: It's still -- but it's not
21 impeding us from actually doing those licensing. But
22 the clean sheet of paper isn't about doing licensing.
23 It's about is there a better way to do licensing? And
24 it may be that the SRM from the Commission does
25 provide an impediment to a better way to do licensing.

1 CHAIRMAN BROWN: I could be real -- what's
2 the term for skeptic? There's another term. I can't
3 remember what it is. Maybe you ought to just
4 recommend that you leave the clean sheet of paper
5 clean. I'm just -- I've been listening to this now
6 for 10 years and it's kind of been the same, same,
7 same thing we do, yet we continue to license. Diablo
8 Canyon. New designs. Plant upgrades. So apparently
9 the SRM is not impeding you. You just have to look at
10 it from a common sense approach. The designs look
11 satisfactory from a common cause failure standpoint.
12 MR. WATERS: And I wholeheartedly -- we
13 wholeheartedly agree that we have a proven approach
14 for licensing those major designs and we also believe
15 there's multiple ways to make a safety case for a
16 digital upgrade. And you heard industry speak of
17 their needs. We're considering more efficient ways to
18 address common-cause failures, not -- there's RPS and
19 ESFAS. We alluded to some -- how do you make upgrades
20 on a 50.59 where it's not going to come to us, where
21 we're not going to do a full BTP 7-19 review? There's
22 also questions I think related to -- we have to make
23 a decision to reverse actuation. Is it needed or not?
24 Can it be risk-informed?
25 So there is a proven approach. We agree.

1 We're just trying to improve it, make it more
2 efficient and look at different ways we can make a
3 safety case or the variety of digital upgrades that
4 may be out there under 50.59 or a LAR that comes into
5 us.
6 CHAIRMAN BROWN: Let me step back a
7 minute. I mean, I hate -- we've got some time and
8 that's why I'm spending some time right now just
9 discussing the issue. Okay? Hopefully I won't forget
10 it, but if it's in the transcript, I can always go
11 back and reclaim my brains, or memories.
12 I'm recalling one of the projects we
13 reviewed where the defense -- the D3 analysis was
14 performed and they looked at that against all the
15 reactor accident analyses. And there was a
16 consideration made that if the operator could take
17 action within 30 minutes or 45 minutes or -- I think
18 it was 30 minutes, then for those particular accident
19 scenarios you didn't need a diverse actuating system.
20 You could depend on the operator.
21 And there were a half a dozen, I don't
22 know, or more where you couldn't confirm the 30-minute
23 operation and therefore you employed a diverse set of
24 instrumentation to account for that, which is a
25 perfectly reasonable way of doing it. It's an

1 approach. Thirty minutes is kind of a universal
2 number for operator actions for the most part. I'm
3 sure there's exceptions somewhere.
4 So I'm struggling with the use of
5 resources that you all are doing when we've already --
6 when you all have already -- not me, but collectively
7 I guess -- but the staff and the NRC has figured out
8 a way to look at these plants and use common sense
9 approaches to defining that, yes, this is a
10 satisfactory way of doing it. Why -- and if the SRM
11 satisfactorily encompasses what you all have been
12 doing; because you're all not violating the Commission
13 policy at this time, then why try to mouse-milk this
14 any farther?
15 I wish I could speak for my old program of
16 22 years when we started installing these systems in
17 1981 and are now on about the third or fourth
18 generation for the systems, yet they are not
19 configured in a manner -- we have some, but not all.
20 But yet if you look at the operating experience, it's
21 -- I mean, the digital-based systems are just so
22 superior in terms of online reliability. Once we
23 learned how to measure things with microprocessors, I
24 should -- and I'll have to admit the first system I
25 installed did not exactly perform the way we

1 envisioned it.

2 Fortunately, we had processes or

3 procedures in place to ensure that we wouldn't get

4 trapped. And then we fixed it and incorporated it.

5 But the common-cause failure issue has not been the

6 software. As long as you do a reasonable development

7 process with oversight of the vendor processes and not

8 let spaghetti code get developed to implement it, it

9 works extremely well, not like your computer at home

10 which all of a sudden locks up on you at all.

11 I'm just making the observation that if

12 you want to be innovative and thoughtful, I would

13 think that you would try to take into account the

14 experience and the various diverse systems, different

15 types of systems and lay out a game plan that doesn't

16 just drain you over the next three or four or more

17 years, or turn into a research program that goes on

18 forever.

19 MR. WATERS: Yes.

20 CHAIRMAN BROWN: Maybe I'm speaking out of

21 school, but that's --

22 MR. WATERS: No, and I --

23 CHAIRMAN BROWN: That is my perspective,

24 by the way. That is not the Committee perspective

25 that you might --

1 MR. WATERS: And my perspective -- I think
2 we would generally agree with that. I mean, as Dinesh
3 talked about the principles, I'd expect for the major
4 upgrade that comes in on the revised ISG process, they
5 -- we would expect the full D3 analysis, which you're
6 familiar with for those type of systems. And, yes,
7 there's 30 minutes. I don't know if that's etched in
8 stone, but we consider that.
9 But again, just to reiterate, one
10 challenge is -- BTP 7-19 technically covers all safety
11 systems. And the question is is that type of D3
12 approach appropriate for those things that have less
13 risk significance, for lack of better words.
14 CHAIRMAN BROWN: Yes, but you can do that
15 independent of a massive --
16 MR. WATERS: We agree, but there's
17 questions of exactly what does that look like? That's
18 something we want to address in BTP 7-19, the
19 applicability of the various types of systems.
20 There's things we want to fix as well.
21 CHAIRMAN BROWN: Well, there's a -- but
22 that's a specific place you go address it as opposed
23 to an overarching world enhancing approach. I just --
24 I'm only tossing this stuff out because we have an
25 opportunity to chat about it, which we don't

1 frequently have.

2 MR. TANEJA: So the challenges that came

3 in when we looked at the challenges is the new

4 reactors -- it's a brand new design and they follow

5 the SRM word by word. Do a D3 analysis using best

6 estimate. Determine whether you need -- whether you

7 can cope with the failure. If not, you need defensive

8 measures. And that practice has worked very well on

9 new reactors.

10 So the policies language was really

11 intended for advanced and new reactors, however, the

12 digital upgrades or digital technology that's used in

13 upgrades is essentially the same as what's being used

14 in new reactors. So the D3 concern is the same.

15 Now some of these upgrades are piecemeal.

16 They're making a minor little change, but it's a

17 digital update. Some is a little bit larger, but the

18 licensee is using the guidance in BTP 7-19. Our

19 inspectors are using that guidance in 7-19. We as

20 technical reviewers are using that guidance, 7-19.

21 And we -- what we heard is that

22 everybody's got their own little twist and approach on

23 how they use that thing, and that's created a number

24 of issues where it's keeping the digital upgrades from

25 not moving forward because they're saying, ah, this

1 thing is an impediment. I can't do any work under
2 that. I don't have a best estimate analysis. Why do
3 I need to do a whole analysis to do this minor change?
4 So those five principles that we laid out is
5 essentially to get everybody on the same page. And
6 with this BTP 7-19 update we are hoping that we all
7 can speak the same language. I think we are making a
8 very reasonable discussion here and I hope everybody
9 in the industry can hear that. And that's what we're
10 trying to get communicated in this next update to BTP
11 7-19.
12 CHAIRMAN BROWN: If they say there's an
13 impediment and it's not really applicable to their
14 thing, you should be able to say, okay, you're the
15 regulator.
16 MR. TANEJA: Well, that's -- the way we're
17 going to communicate is by updating the BTP 7-19. I
18 think that's really where we're going.
19 CHAIRMAN BROWN: I wouldn't even say that
20 you have to revise BTP 7-19 every time. That's why
21 you're the regulator. I used to -- I hate to say
22 this, I had specs for all my equipment and I would
23 like to say I always met the spec for every piece of
24 equipment that I ever delivered. That is not true.
25 I accepted stuff that didn't meet the spec because it

1 was good enough for the application we were using it.
2 You could call that we over-specified. So what? We
3 got part way there, but we -- it was good enough. So
4 we accepted it. So I --
5 MR. THOMAS: Mr. Chairman?
6 CHAIRMAN BROWN: Yes, Brian. I'm sorry.
7 MR. THOMAS: Oh, sorry. So I think you
8 nailed it. There are a couple of different camps, if
9 you would, if I can use that word, even within the
10 staff. Okay? So, and given that, that's why this is
11 only an Information SECY, to say we have some
12 challenges here and we're looking into it.
13 CHAIRMAN BROWN: Why don't you tell them
14 it's good enough?
15 MR. THOMAS: Well, the --
16 (Laughter.)
17 MR. THOMAS: What we have -- the way we
18 are approaching it is to say, well, BTP 7-19 may be a
19 point of -- maybe the -- what needs further
20 clarification, which is what Dinesh is getting at.
21 And so, from the standpoint of scope and being
22 overwhelmed by our efforts, our approach is to just
23 send up this Information SECY and then also deal with
24 the clarification of BTP 7-19. Speaking for myself on
25 the steering committee, we don't see that as -- view

1 that as an overwhelming task even though this whole
2 CCF issue -- as you said, it does have a lot of
3 tentacles, it seems like it, and it keeps going on and
4 on. And it could --
5 CHAIRMAN BROWN: They're never going to go
6 away.
7 MR. THOMAS: -- we can get wrapped up in
8 this thing. Hopefully through the clarification of
9 BTP 7-19, and we do that in the near term on a
10 short/midterm basis, we'll kind of put some things to
11 rest and also see what else we uncover as we go
12 through some of these other guidance documents that
13 we're dealing with you on and looking at enhancing.
14 But that's the approach for right now. It's -- we're
15 not taking on the world of CCF right now. We're just
16 trying to -- because it is different camps and
17 different thoughts and so forth, let's just do
18 something about it in terms of providing some
19 clarification on BTP 7-19.
20 CHAIRMAN BROWN: Well --
21 MR. THOMAS: But I truly appreciate the
22 comments.
23 (Laughter.)
24 MR. THOMAS: There are some folks that are
25 in the same camp as you're reflecting here today. And

1 so --

2 CHAIRMAN BROWN: Well, the only way to

3 direct it is to meet it head on and go try. You never

4 try, don't shoot it -- somewhere the line you ought to

5 go shoot this pig. I just -- I really think you're

6 spending a lot of effort. And you've already got a

7 successful process to get where you want to go.

8 You're delivering product. And where there's an

9 impediment you look at that specific item and you fix

10 that, but don't try to generalize it to an overall

11 encompassing thing. You'll never get there.

12 It's like cyber security. You're always

13 going to be behind the hackers. You will always be

14 reactive. You will never beat them at their game no

15 matter how good you think you are. Can't revise your

16 stuff fast enough until after somebody's figured out,

17 ah, we got hacked. There's another fix. That's just

18 the way it goes.

19 So, all right. Full Committee meeting,

20 it's going to be fundamentally ISG-06. We'll have

21 what, an hour-and-a-half roughly?

22 MS. ANTONESCU: Yes.

23 CHAIRMAN BROWN: Some of your -- I tried

24 to give this some thought while we were sitting here.

25 I wanted to use your slides to make -- clear that one.

1 MR. DARBALI: The ISG slides?

2 CHAIRMAN BROWN: Yes, the ISG slides. You
3 had 31 -- actually 23 slides, I think. Is that right?
4 I've forgotten where you hit the backups. It was
5 around slide 24 or 25, if I'm not mistaken. Okay.
6 And 25 was questions. So we don't need that one. The
7 backup slides were 25 and 26. Questions. Next steps,
8 24.

9 If you go back up to the beginning. You
10 ought to do a -- the one or two slides on how this
11 fits within the IAP part of the thing. In other
12 words, the Commission direction slide. I think that
13 was slide 4. Yes, slide 4. And there's a slide 3.
14 Just get rid of the -- is there any -- do really need
15 even slide 3?

16 MR. DARBALI: I don't think so.

17 CHAIRMAN BROWN: Yes, slide 4 would seem
18 to me you need. That was the modernization. Then
19 your Modernization Plan, slide 5, just to give it some
20 overall context and say what you're not going to talk
21 about because that's not in place. And then go into
22 the ISG-06. There's the purpose. That would be slide
23 8. Slide 9 gives some differentiation. It says this
24 is part of the plan, although those are the goals.
25 You've got -- yes, you got to say a little bit --

1 what's the difference between Rev. 1 and Rev. 2. And
2 I think that's in your slide 11 and 12 and 13, 14.
3 Oh, and you talk about the feedback
4 because this was revisions due to lessons learned.
5 And then do the slides on ISG-06. And the alternate
6 review process, the table that looks like it. And
7 then up through about slide -- either 22 or 23. Looks
8 like about 14 slides. That ought to be coverable in
9 the hour-and-a-half -- functions of questions.
10 You ought to cover the -- make sure you
11 get the architecture question in.
12 MR. DARBALI: Sure.
13 CHAIRMAN BROWN: I had another -- oh, a
14 little bit of a discussion like we had on how is the
15 decision made as to what -- whether you do a tier 1-3,
16 2-3 or the Alternate Review Plan -- Alternate Review
17 Process. And your -- some of your words explain the
18 difference between the two of them.
19 And if -- when you're talking about the
20 architecture part you ought to make it clear that even
21 though your tier 1, 2 and 3 -- I don't know what
22 changes you will have made or intend to make, although
23 I would throw the architecture thing in there. I'm
24 not so sure how you intend to implement that, but it
25 ought to be clear from the -- that figure C-1 and C-2.

1 And you ought to try to integrate those in where you
2 show where the D number -- I mean, the -- how you get
3 like Phase 1 and here's these things that encompasses
4 these types of actions. And whether it's tier 1, or
5 2-3, whatever they are. I think those -- that plus
6 the enclosure that you need to show, and try to
7 integrate those to show that you're covering the
8 waterfront here.
9 There was some good discussion in the back
10 and forth we had up in the beginning. I don't
11 remember all the words that were there, but Richard
12 had a bunch. Go find a transcript. Can we get --
13 We ought to rush it because we've got the
14 meeting on June the 6th or 7th, whatever day it is.
15 MR. WATERS: Yes, some of the items we
16 kept was the architecture of course. A good
17 discussion with Mr. Skillman on --
18 CHAIRMAN BROWN: Oh, the response
19 ownership?
20 MR. WATERS: Ownership, right.
21 Ownership --
22 CHAIRMAN BROWN: Ownership. Yes,
23 that's --
24 MR. WATERS: -- and understanding from the
25 beginning of the life cycle. And I'll -- we'll take

1 a look at the ISG, if anything needs to be clarified
2 there, but we'll provide some information how we --
3 we'll address that.
4 CHAIRMAN BROWN: Dick had another comment
5 later in the meeting on -- where's my page?
6 (Pause.)
7 MR. WATERS: You had a comment regarding
8 the ISG does not talk about hardware --
9 CHAIRMAN BROWN: Yes, hardware
10 configuration, whatever it is.
11 MR. GUTIERREZ: -- configuration.
12 CHAIRMAN BROWN: I know Rich had a
13 response. We'll take a look at that and provide some
14 more discussion on that as well. Not going to -- I
15 mean, we'll update ISG, but we'll take a look hard at
16 that comment and tell you how we're going to address
17 that.
18 CHAIRMAN BROWN: And the point of the ISG
19 being used in conjunction with the SRP, not
20 independent of --
21 MR. WATERS: Yes.
22 CHAIRMAN BROWN: -- the SRP.
23 MR. WATERS: Yes.
24 CHAIRMAN BROWN: So I'm kind of looking
25 for the high-level concept relative to architectures

1 and what's getting covered under each of the tiers,
2 why -- how they're selected. I didn't really think
3 about you all agreeing with the licensee or applicant,
4 or whoever it was. I thought you all got to the LAR
5 and figured out what you would do, but in fact what
6 you've said, if I'm correct, was that the license
7 provides some input to you on what they would like to
8 see in order -- how they want to proceed with their
9 development of their design --
10 MR. WATERS: Yes.
11 CHAIRMAN BROWN: -- which is just fine.
12 If there's anything to be added, for Phase
13 0 since that's kind of the pre-LAR -- might be one
14 slide that just says, hey, we go over all this with
15 them before they start. And it doesn't have to be
16 extensive, but just -- it's just not like you leap
17 into this thing without any pre-meetings to make sure
18 everybody's on the same page.
19 MR. WATERS: Yes, that leads to --
20 CHAIRMAN BROWN: We didn't really cover
21 that. I -- we understood that.
22 MR. WATERS: Yes, right. We'll highlight
23 that. And that leads of course to what enclosure
24 review we're going to cover, what we're going to
25 provide. There's a tier process. We'll have to

1 review process. So we can definitely highlight that
2 better for the Full Committee.
3 CHAIRMAN BROWN: Okay. And the -- yes,
4 the enclosure I think you need -- you definitely need
5 to use that because it shows you what is -- not only
6 what process-wise you're going to do in terms of
7 scale, but it shows you the content -- technical
8 aspects that you're going to be developing for each
9 one. Is that clear enough?
10 MR. WATERS: I believe it's clear.
11 CHAIRMAN BROWN: Probably 15, 16, 14
12 slides, somewhere in that ballpark.
13 MR. WATERS: That makes sense to us. And
14 we'll begin working on that and we'll communicate with
15 Christina to clarify any small points and --
16 MS. ANTONESCU: You can send a draft.
17 CHAIRMAN BROWN: Yes, if you want to send
18 us a draft, we can -- at some point, I'll --
19 MR. WATERS: I'll --
20 CHAIRMAN BROWN: -- I will be around,
21 maybe.
22 MR. WATERS: Oh, yes. We'll be happy to
23 send you a draft iteration before we finalize it, of
24 course. We want to make sure we provide -- fully
25 inform the Full Committee to your expectations.

1 CHAIRMAN BROWN: Yes, we've only got about
2 -- what's today? It's the 17th. So it's about three
3 weeks, two-and-a-half weeks.
4 MR. WATERS: Yes, so we got to get on it
5 next week. So we'll do that.
6 CHAIRMAN BROWN: Yes, there may be a
7 circumstance where I'm not here; I'm not anticipating
8 that, from a medical procedure standpoint. But Dennis
9 will take charge if I'm not here. Unfortunately, he
10 wasn't able to make this meeting. I'm not
11 anticipating that happening, but Christina will know
12 what's going on and will be able to fill in what we
13 need to do. And in any event, I might be able to look
14 at the slides anyway in a draft form even if I --
15 somebody has to carry them out to me. Okay?
16 MR. WATERS: Sure. We're happy to do
17 that.
18 CHAIRMAN BROWN: Oh, got one more thing
19 here. Ken, did you cover yourself this morning?
20 (No audible response.)
21 CHAIRMAN BROWN: Okay. We will transition
22 now into the public comment in the audience. Anybody
23 else other than Ken have anything else to say on the
24 second round here?
25 Oh, hey, not bad. Great idea. Thank you

very much. I forgot about that. It's 3:00. We will recess for 15 minutes.

(Whereupon, the above-entitled matter went off the record at 3:00 p.m. and resumed at 3:21 p.m.)

CHAIRMAN BROWN: We're back in order again. Meeting is back in session.

MR. ARCHAMBO: We ready?

CHAIRMAN BROWN: Yes, go ahead.

MR. ARCHAMBO: All right. I'm Neil Archambo. I work for Duke Energy. I am a design engineer, a reactor design engineer. We've put in a number of digital systems. I also do a lot of 50.59 evaluations and screens, and so I am down in the trenches. So I'll give you perspective hopefully of what's going on in the industry and where we're finding the hard spots.

I kind of got a little bit lost at the end of the last session. I almost thought I heard that the existing guidance is okay, and I hope that's not what I heard because that's not what we feel out in the industry. We're having issues.

Now about a year ago I and a few of my esteemed colleagues sat in front of this Committee and we -- to give a little bit of presentation of what was going on in the industry. And one of the

1 modifications I talked about at that time, you might
2 remember, is the upgrade to the diesel generator
3 voltage regulators. We wanted to replace our motor-
4 operated potentiometers with some digital reference
5 adjusters. I don't know if you recall that one.
6 The problem with the existing guidance for
7 that particular modification is, as we talked about,
8 BTP 7-19. We said that you got two options. Well,
9 you got three options really: You got -- you can do
10 100 percent testing, which we've established, yes,
11 software, that's not possible, correct? You can use
12 diversity. Or your third option is you could assume
13 you have a CCF. I guess that's an option. You could
14 just assume you have a CCF and see if the plant still
15 functions like it's supposed to, provided you don't
16 violate your licensing basis.
17 So really with the digital reference
18 adjuster we established there were 17 lines of code
19 and we established that that could not be 100 percent
20 tested. So our option in that case is to use
21 diversity. So what does that mean? That means I use
22 two different -- either two different digital
23 reference adjusters on my diesels or I use one motor-
24 operated potentiometer and one digital reference
25 adjuster. That would be diversity. That works, but

1 that's not the route we wanted to take.

2 So what happened with that particular

3 modification, because of the regulatory uncertainty at

4 that particular plant, we did not install the digital

5 reference adjusters. We chose instead to keep the

6 motor-operated potentiometers. And that's what's out

7 there today as we speak.

8 And on top of that, just to give a little

9 bit of background on that modification, the engineer

10 that was in charge of that, the vendor had come to him

11 and said, look, it's an analog voltage regulator, but

12 we got this digital reference adjuster we highly

13 recommend. So the engineer, being eager, said that

14 sounds like a good idea. So we had a commercial grade

15 dedicated with the digital reference adjuster.

16 And when it come to the plant, the folks

17 who are involved in a lot of these things and know

18 about the regulatory uncertainty, said -- up to our

19 senior management, said we're not putting that thing

20 in because of the regulatory uncertainty. We don't

21 know if the NRC inspector is going to come and tell us

22 our diesels aren't operable because we have digital

23 components of the same type on both trains.

24 So the end of that story was we paid $2

25 million to send that equipment back to have it

1 rededicated with the motor-operated potentiometers.
2 That's what's happening out in the industry. That's
3 one example of many.
4 Now we have upgraded a lot of our non-
5 safety systems with digital equipment over the years,
6 probably for the last 25 years, and I can tell you
7 that what we've noticed; and I think you've heard a
8 few people say, is it's been nothing but performance
9 improvements. In reliability and safety our plants
10 are operated better than ever. What utilities want to
11 do is apply these digital -- this digital equipment to
12 our safety-related systems, but we don't have the
13 infrastructure to do that yet. That's where we've
14 having problems.
15 And the guidance out there that we have
16 today doesn't lend itself well to us putting this
17 equipment in our safety-related systems. So as it
18 stands right now very few utilities are doing safety-
19 related digital upgrades. Now we feel as an industry
20 that would certainly help safety and the reliability
21 of our plants to install these digital upgrades.
22 I've been involved in a lot of digital
23 upgrades over the years and I can tell you that in no
24 cases I've ever seen that we installed a digital piece
25 of equipment and we decided -- we said -- we didn't go

1 back and say, you know what, that analog stuff worked
2 a lot better. We're going to take that digital stuff
3 out and put analog stuff back in. That's never
4 happened. And in my career; and I've been in the
5 industry about 31 years, I've yet to see a software
6 common-cause failure. I'm not saying they don't
7 exist. And maybe somebody else has seen one. I
8 haven't. And we've got a lot of digital equipment out
9 in that plant.
10 So it begs the question are we putting too
11 much emphasis on this issue? Perhaps we're putting
12 way too much emphasis on this issue and the outcome is
13 is our plants are using a lot older analog equipment.
14 We're not realizing the safety benefits that we could
15 just because we think that it's a possibility to have
16 a common-cause failure.
17 I think EPRI has done some research that
18 kind of supports that evidence that there's not a
19 whole lot of stuff out there that -- we have a lot of
20 other failures, but software common-cause failure just
21 hasn't been one of the number one items that we've had
22 to deal with in the industry.
23 So I'll just leave you with the fact that
24 the existing guidance is not there. We hope this RIS
25 will allow us to do safety-related digital upgrades

1 with a level of regulatory certainty. That's the goal
2 of it. We'll see. It's supposed to come out today,
3 the next revision. And we're cautiously optimistic
4 with that. And we think Appendix D to 96-07 will help
5 us as well, and hopefully this revision to the ISG
6 process will help us get some of the projects -- the
7 safety-related projects going.
8 There's a number of industries, or a
9 number of utilities that are going to have to do
10 reactor protection system upgrades, digital reactor
11 protection system upgrades, but until we get that
12 process streamlined enough to where it's financially
13 feasible to do that, you're probably not going to see
14 a whole lot of them.
15 We go back to the Oconee. I work for Duke
16 Energy. We're still kind of licking our wounds on the
17 Oconee project. So we're going to have to see some of
18 these other utilities step up, try out this new
19 process. And if they have some really good success,
20 we'll be right on board. We got some of our plants
21 that would -- that are going to be in need of
22 upgrading these reactor protection systems.
23 Right now what I'm hearing from my senior
24 management is see if there's an analog system
25 available. We don't need to be going down that road.

1 That's crazy. We need to be upgrading our plants with
2 the latest state-of-the-art like every other industry
3 has done.
4 Any questions? Comments?
5 CHAIRMAN BROWN: No, we don't comment. We
6 don't discuss the comments from the public.
7 MR. ARCHAMBO: No comments or questions.
8 Understood.
9 CHAIRMAN BROWN: Yes, we can't go back and
10 forth here.
11 MR. CONNELLY: I'm John Connelly. I work
12 for Exelon.
13 What we've been talking about here today
14 is really two extreme edges, or bookends, if you will.
15 On one side we've got ISG-06, what we need to be able
16 to do in RPS or an ESFAS, a big -- a high-impact
17 modification.
18 On the other end of the spectrum is the
19 RIS. The question was posed this morning are there
20 shovel-ready people sitting there waiting to come
21 forward with a license amendment through the ISG?
22 Addressed that earlier. The RIS is the other end of
23 the spectrum. And there are tons of shovel-ready
24 modifications ready to go. Neil alluded to some of
25 them. Voltage reference adjusters, chillers, digital

1 relays. I mean, there are a lot of things that we
2 would like to modernize under the RIS. That's
3 probably going to be -- I'm just taking an educated
4 guess here, 80-90 percent of the modifications or
5 modernizations that we want to do are going to fall
6 under the purview of the RIS. That makes the RIS
7 critically important.
8 We're pinning a lot of our modernization
9 initiatives on this RIS coming out in a state in which
10 we can use it. To be blunt, the speed with which we
11 get it out doesn't matter as much as getting it in a
12 state that we can actually pick it up and apply it in
13 a way that allows us to move forward with
14 modernizations.
15 So what I've heard this morning is the
16 intent was to get this issued on the 30th of this
17 month. So just a quick envelope thing here. That
18 basically leaves us four days to review it and five
19 days for any comment resolution that may occur. So
20 that seems to me as an artificially compressed
21 timeline. We want it out, but we're very interested
22 in making sure that all the comments that we've
23 provided, and there have been hundreds of them along
24 the way -- that all of those comments that are picked
25 up in such a way as that there's no ambiguity and we

1 don't feel a sense of risk in terms of inspection
2 findings down the road.
3 I guess the comment I would make is we
4 need to make sure that we've allocated the right
5 amount of time and the right amount of rigor and going
6 through the right process and reviews to make sure
7 that we get something that we can ultimately use,
8 because this is critically important to us moving
9 forward with modernization. That's my comment.
10 CHAIRMAN BROWN: Thank you.
11 MS. ANTONESCU: The line is open. The
12 phone.
13 MR. REMER: Good afternoon. Jason Remer,
14 Director of Life Extension and New Technology at NIE.
15 Thanks for the meeting today.
16 I think the Modernization Plan is a really
17 good step in the right direction. I was involved way
18 back in the 603 scenario and it was clear that that
19 wasn't a unified approach. It had a lot of non-
20 concurrences and a lot of people didn't agree with the
21 way that was going forward anyway. But I think the
22 Modernization Plan developed -- I think we put it out
23 in -- May 31, 2016. So that's been almost two years.
24 Good strategy, good effort, but -- a lot
25 of good work, two years, really no product so far that

1 we can use. Two years. We started the RIS with an
2 effort to do a quick turnout and so we could upgrade
3 some safety-related low-significant digital systems.
4 And that was going to be a quick turn. We were going
5 to get it out in six months or so.
6 We hope that the RIS coming out today will
7 be useable. We really hope we -- we have worked
8 together with the NRC and have made our comments
9 known. The problem with the previous version is it
10 actually caused us issues with the non-safety mods
11 that we're doing right now. And we felt if it would
12 have gone out, it would have actually hindered the
13 non-safety mods. And so we can't go backwards where
14 we're at. We're already stuck right now as an
15 industry. We're hoping this Modernization Plan can
16 help us go forward.
17 ISG-06 is a wonderful effort and I think
18 it's going to help us on the major mod side, which
19 we'll see. I don't think people will be too
20 interested in doing digital safety-related mods for
21 big ones if they see we can't do minor mods for
22 safety-related equipment like chillers.
23 That's our poster child. The chiller.
24 We've got companies out there right now that have an
25 analog chiller and a digital chiller control because

1 they're afraid of putting two digital controls on
2 there because there's uncertainty. They're afraid of
3 the inspectors coming out and inspecting them and
4 giving them a fine and saying you didn't do it right
5 because there are so many interpretations of what's
6 right.
7 We got breakers, relays, transmitters,
8 controllers of all sorts that we could upgrade. Like
9 I said before, we're using World War II equipment
10 right now for the safety functions, many of them.
11 Works fine. You just can't get parts anymore. I
12 don't know if you've seen an AGASTAT timing relay.
13 It's a diaphragm device. And we use thousands of them
14 at the plant. There's still many of them out there.
15 But the digital replacement is so much better. We're
16 ready to do that.
17 So I would suggest to you, I would propose
18 to you that the longer we wait on doing these mods,
19 the safety improvements we're not taking advantage of.
20 In other words, in time we're kind of going down in
21 safety rather than going up. So I would like to
22 suggest that the NRC help us lean forward so we can
23 totally modernize our nuclear plants. We need this.
24 We need this not just for safety. We need it for
25 economics. We think technology is a way ahead as far

1 as helping us operate or plants more efficiently.
2 So thanks for the opportunity to speak and
3 I'll leave these comments with you.
4 CHAIRMAN BROWN: Anyone else in the
5 audience?
6 MS. ANTONESCU: Yes, there's another one.
7 CHAIRMAN BROWN: Oh, Ken? Sorry about
8 that.
9 MR. SCAROLA: Thank you. Ken Scarola,
10 Neighbor Automation Engineering. I'm sitting down not
11 at the microphone because I have a lot of notes on my
12 computer and I just couldn't find another way to do
13 this.
14 As I said earlier, I've been a champion
15 for digital upgrades in the nuclear power industry for
16 43 years. And by the way, Mauricio, the first digital
17 protection system was in 1978 for ANO2, not in the
18 1980s. It's probably not on your radar because I
19 think maybe it was before you were born. I don't
20 know.
21 (Laughter.)
22 MR. SCAROLA: I was also the author of the
23 defensive measures, the Ps and the Ls in the EPRI
24 document which was referred to by the staff and also
25 discussed by Rob Austin. I was also the lead author

1 for the first draft of NEI 16-16 which adopts all
2 those defensive measures.
3 I'm here because I have strong concerns
4 regarding the upcoming RIS on digital upgrades under
5 50.59, but please understand I haven't seen the latest
6 version. It's not out yet to the public. So my
7 comments reflect what I saw back in March. Maybe
8 things have changed. I don't know.
9 I completely agree with Gordon Skillman
10 that 50.59 is only a screening process to determine if
11 NRC review is needed. And in many areas NRC's
12 regulatory guidance is sufficient to conclude that NRC
13 is not -- NRC review is not needed. For example,
14 IEEE-344 gives us guidance that is sufficient to
15 conclude that there is no CCF due to an earthquake.
16 IEEE-384 gives us deterministic guidance for
17 preventing CCF due to electrical faults. Reg. Guide
18 1.180 gives us guidance to prevent CCF due to EMI
19 hazards. Reg. Guide 1.106 gives us deterministic
20 guidance for preventing CCF due to a set-point design
21 error. And I could go on and on and on. We have a
22 lot of good guidance.
23 But until there is clear regulatory
24 guidance for deterministic attributes that can be
25 credited for preventing new sources of CCF that come

1 with the digital technology and also clear guidance
2 for analyzing potential CCFs that are not prevented so
3 we can demonstrate that the malfunction results are
4 bounded by previous accidents, the industry is just
5 not ready for digital upgrades under 50.59 for systems
6 that, (1) directly initiate plant transients, or (2)
7 systems that are directly credited for accident
8 mitigation when digital integration, interconnectivity
9 or standardization are employed.
10 In essence, RIS 2002-22, Supplement 1 puts
11 the cart before the horse. We don't have sufficient
12 guidance to make the decision as to whether or not
13 regulatory review is required. If we had the
14 guidance, we could be very confident that the industry
15 would move ahead with that guidance, they would
16 execute it correctly, the inspectors would confirm
17 that and we would have safe plants. With a lack of
18 guidance what are the inspectors going to inspect to?
19 What is the industry going to use as their yardstick
20 for what are sufficient defensive measures?
21 So I feel very strongly about this, and
22 let me explain why. There should be no question that
23 the inherent attributes of digital technology, which
24 are the ability to integrate, the ability to
25 interconnect and the ability to standardize, offer a

1 tremendous benefit to this industry. It can lower our
2 operations and maintenance costs while maintaining
3 plant safety, and that is critical for our future
4 viability. We need it.
5 But there should also be no question that
6 these same inherent attributes of interconnectivity,
7 integration and standardization have the potential to
8 create new un-analyzed sources of CCF, and these
9 sources of CCF can create malfunctions that were
10 previously un-analyzed. Worse, they can threaten
11 plant safety.
12 Now I think we all understand very well
13 the issue of a design defect that affects two
14 divisions of a safety system. This is the thing we
15 talk about most often, that we have the same software
16 in both safety divisions and we get a CCF and
17 therefore the safety divisions become ineffective.
18 But we don't necessarily understand other sources of
19 CCF that are much more likely and equally detrimental
20 to the safety of the plant. And I'd like to give you
21 some examples.
22 The accident analysis for an overcooling
23 event typically most operating plants considers the
24 erroneous run out from a single feedwater pump. And
25 that was appropriate in the days of analog technology

1 because we had one analog component, one I&C component
2 controlling one feedwater pump. If we had a failure,
3 one pump would be affected. But in digital
4 implementations it's very common to control two or
5 three feedwater pumps from the same digital
6 controller. Now in digital technology we can get an
7 erroneous pump run-out command to three pumps and now
8 create a new event that was previously un-analyzed.
9 That new event challenges DNBR margin. It
10 also challenges reactor coolant system pressure limits
11 margin. So this is an un-analyzed condition. And
12 there is no regulatory guidance right now that we can
13 point to that says, yes, we're confident that when
14 licensees implement that digital feedwater system
15 they're going to prevent that new CCF.
16 Second example: The accident analysis for
17 typical power distribution anomalies considers single-
18 rod events or single-rod group events because that was
19 the big -- those were the failure modes that were
20 appropriate for the technology of the day. But now in
21 digital systems we integrate all the rods together in
22 a single digital controller. Now we can have multiple
23 asynchronous rod motion demands that now challenge
24 local power density fuel design limits in a way that
25 were previously un-analyzed. So again, we have the

1 potential for new digital CCFs and no deterministic
2 guidance from the staff to help industry ensure that
3 those are prevented.
4 With your patience I'll offer one more
5 example and then I'll get to my point.
6 Distributing control systems commonly
7 connect multiple controllers. I may distribute my
8 control functions. I may have a reactivity control
9 controller. I may have a feedwater controller. I may
10 have a temperature controller. I may have a pressure
11 controller. But we interconnect all these controllers
12 through data communication networks and very often
13 through operator workstations with soft controls.
14 Digital data communication networks can
15 have data storms that adversely affect all of those
16 functions. Operator workstations with soft controls
17 can generate erroneous soft control commands to all
18 of those functions. Now that doesn't mean that we
19 don't have ways to prevent these things. There are
20 ways and we know how to do it. That's the subject of
21 the Ps and the Ls in the EPRI document.
22 I'm getting a nod here that I have to wrap
23 up. Okay. Let me -- I thought we had until 4:30
24 today. I'm sorry.
25 CHAIRMAN BROWN: We're not going to 4:30.

1 MR. SCAROLA: Well, 15 minutes you told me
2 I could have for my part of it.
3 CHAIRMAN BROWN: You've got -- like I say,
4 you've got five more minutes.
5 MR. SCAROLA: Okay. Fine. Okay.
6 The problem I have --
7 CHAIRMAN BROWN: Make your point.
8 MR. SCAROLA: -- is that the RIS allows
9 licensees to make highly subjective qualitative
10 assessments regarding the adequacy of CCF defensive
11 measures. The only exception in the RIS is for the
12 reactor protection system logic and the engineering
13 safety feature actuation logic. But what this tells
14 me -- I get even more concerned about this because now
15 I've got to say, well, does the I&C Branch not
16 understand that there are many other things that are
17 much more safety-significant than RPS and ESFAS?
18 For example, the instrumentation and
19 manual controls that the operators much use for
20 mitigating a steam generator tube rupture event are
21 not part of RPS and ESFAS. The load sequencers that
22 we need for mitigating loss of off-site power or for
23 accidents with loss of off-site power are not part of
24 the RPS and ESFAS.
25 So I'm wondering did the staff engage

1 their safety analysts, the PRA Branch? Did the I&C
2 Branch engage the PRA folks or the Electrical Systems
3 Branch when they -- when you established the limits
4 for which this RIS is not applicable? It seems to me
5 there's a lot more that we should be concerned about.
6 Now I have no problem with qualitative
7 assessments. We make the all the time in the
8 industry. But qualitative assessments should be
9 limited to reaching a conclusion that the likelihood
10 of CCF is sufficiently low that we can analyze it as
11 a beyond-design-basis condition.
12 If we've learned anything from Fukushima
13 and other accidents, we need to be prepared for the
14 unexpected, and that's the thrust behind the SRM to
15 SECY-93-087. It says you need to be prepared for the
16 unexpected. That's the thrust behind BTP 7-19. Be
17 prepared for the unexpected. And by the way, these
18 documents are not limited to RPS and ESFAS. They
19 apply to all safety systems in the plant. And I don't
20 see how the staff has the authority through a RIS to
21 change NRC policy in SECY-93-087 or BTP 7-19. These
22 are not limited to RPS and ESFAS.
23 So let me get to my conclusion. RIS 2002-
24 22 was flawed because it did not clarify the staff's
25 position on digital CCF. This has really hurt the

1 industry and it's been a detriment to the
2 competitiveness of nuclear power. The supplement, as
3 it was written a couple of months ago, does nothing to
4 augment this lack of clarity. Even worse it leverages
5 the lack of clarity to establish qualitative
6 assessments as the basis for 50.59 digital upgrades.
7 As I said in the beginning, in many areas
8 the NRC's regulatory guidance is sufficient for
9 effective and safe 50.59 upgrades, but until there's
10 clear regulatory guidance for deterministic attributes
11 that can be credited, we're just not ready for this
12 type of self-regulation.
13 I said earlier I wasn't here to interfere
14 with ISG-06. I think we desperately need it. I am
15 here in hopes that you'll take a second look at this
16 RIS. I understand that the staff has not requested
17 the ACRS input on this RIS, but for the safety of
18 nuclear power industry I believe that's a serious
19 mistake. The ACRS should comment on it, and I hope
20 you do. Thank you.
21 CHAIRMAN BROWN: Okay. Thank you, Ken.
22 MR. AUSTIN: Charlie, I have one quick --
23 CHAIRMAN BROWN: Okay. Go ahead.
24 MR. AUSTIN: I'd just like to clarify --
25 CHAIRMAN BROWN: State your name.

1 MR. AUSTIN: I'm sorry. Rob Austin, EPRI.
2 I'd just like to clarify that Mr. Scarola was one of
3 an authorship team for the EPRI document. He was not
4 the sole author. There's many others that worked on
5 that document. Thank you.
6 CHAIRMAN BROWN: Okay. Is there -- you
7 said the line is open?
8 MS. ANTONESCU: Yes.
9 CHAIRMAN BROWN: Okay. Is there anybody
10 on the phone line that would like to make any
11 comments?
12 (No audible response.)
13 CHAIRMAN BROWN: If somebody's there,
14 would they say something?
15 Thank you for confirming once more. I
16 appreciate that.
17 Okay. I hear no one making -- wanting to
18 make other comments.
19 At this point I want to thank the staff
20 for their presentation today. Thank you for sitting
21 through our recitation at the end as we discussed CCF
22 in a somewhat diverse manner --
23 (Laughter.)
24 CHAIRMAN BROWN: -- to play a play on
25 words there. It was very, very useful. I hope to

1 have a coherent letter maybe for you available on --
2 via the Full Committee meeting this coming June. And
3 we will -- if you have any other comments you can tell
4 me that now before I adjourn.
5 MR. WATERS: On behalf of the staff and
6 the Digital I&C Steering Committee we really
7 appreciate the opportunity sincerely. We'll take your
8 feedback we heard this morning on ISG-06 and work on
9 it and as well the formal feedback we get back from
10 the ACRS meeting next month. So again appreciate it.
11 And special thanks to all of the team
12 members here in the audience who've spent a seemingly
13 long time on ISG-06 and common-cause failure, but we
14 do have a world-class staff here who take our job of
15 ensuring safety very seriously. So again thank you.
16 CHAIRMAN BROWN: Okay. I appreciate that.
17 I have neglected my members here. Ron, did you have
18 any comments?
19 MEMBER BALLINGER: It was on purpose.
20 (Laughter.)
21 CHAIRMAN BROWN: Okay. Vesna?
22 (No audible response.)
23 CHAIRMAN BROWN: Joy didn't pass on
24 anything to you? Thank goodness.
25 All right. With that I will thank you

1 again and the meeting is adjourned.

2 (Whereupon, the above-entitled matter went

3 off the record at 3:49 p.m.)

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

MP #1 Protection Against Common Cause Failure

Mauricio Gutierrez RES/DE/ICEEB
Dinesh Taneja NRO/DEI/ICE
Rossnyev Alvarado NRR/DE/EICB
Michael Waters, NRR/DE/EICB/BC

Advisory Committee on Reactor Safeguards
DI&C Subcommittee Briefing
May 17, 2018

IAP – Modernization Plans

- **Modernization Plan (MP) #1 – Protection Against Common Cause Failure**
  - **MP #1A – Regulatory Issue Summary (RIS) 2002-22, Supplement 1**
  - **MP #1B – Review of NEI 16-16**
  - **MP #1C – Implementing Commission Policy on Protection Against CCF in DI&C Systems**
- MP #2 – Considering Digital Instrumentation & Controls in Accordance with 10 CFR 50.59
- MP #3 – Acceptance of Digital Equipment (Commercial Grade Dedication)
- MP #4 – Assessment for Modernization of the Instrumentation & Controls Regulatory Infrastructure
  - MP #4A – ISG-06 Revision
  - MP #4B – Develop Strategic activities for long-term improvements to the regulatory infrastructure

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Agenda

- MP #1A – RIS 2002-22, Supplement 1, “Clarification on Endorsement of Nuclear Energy Institute (NEI) Guidance in Designing Digital Upgrades in Instrumentation and Controls Systems”
- MP #1B – Review of NEI 16-16, “Guidance for Addressing Digital Common Cause Failure”
- MP #1C – Implementing Commission policy on protection against CCF in DI&C systems

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Background on CCF in DI&C

- DI&C technology can provide advantages in reliability and functionality, but can also create the potential to introduce a software CCF
- Commission directed staff to implement position in SRM to SECY-93-087, II.Q
- Staff implemented Commission direction into staff guidance Branch Technical Position (BTP) 7-19, "Guidance for Evaluation of Diversity and Defense-in-Depth (D3) in Digital-Based Instrumentation and Control System Review Responsibilities"
- SRM to SECY-16-0070

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Technical Issues

- Evolution of digital technology and industry standards.
- Evolved scope of applicability.
- Addressing CCF concerns when performing upgrades:
  - Determining the amount of emphasis on CCF concerns during system design.
  - Determining the likelihood of a CCF.
  - Determining the diversity needed.
- Determining the need for diverse actuation systems or use of certain design attributes.
- Performing a D3 analysis for all types of safety I&C systems under a graded approach.
- Addressing CCF concerns in the context of specific 10 CFR 50.59 evaluation criteria.

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RIS 2002-22, Supplement 1 Purpose and Scope

- Clarifies NRC's previous endorsement of NEI 01-01 for 10 CFR 50.59 upgrades
- Clarifies the use of qualitative assessments used to determine that CCF is sufficiently low
- "Sufficiently low" is based on assessing design attributes, quality of the design process and operating experience
- Not applicable to major Reactor Protection System (RPS) and Engineered Safety Features Actuation System (ESFAS) upgrades

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Example RIS Qualitative Factors

- Design Attributes
  - Independence, diversity, etc.
  - Inherent design features such as automated self-testing and watchdog timers
- Quality of the Design Process
  - Use of industry consensus standards shown to be applicable
- Operating Experience
  - Relevant operating experience in similar applications, operating environment or comparable configuration to that of the proposed modification

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

RIS 2002-22, Supplement 1 Status & Next Steps

- Initial Draft Issued for public comment in July 2017
- Second draft issued for public comment in March 2018
  - Total of 7 commenters
  - Approximately 60 public comments
- Scheduled for final issuance by May 31, 2018
- Follow-up inspection training and workshops planned

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI 16-16
Purpose and Scope

- Developed in support of industry response to NRC's activities on Protection Against Common Cause Failure.
- NEI 16-16 provides engineering guidance for industry to address CCF concerns. The guidance includes defensive measures that can be credited to address CCF, in addition to those in the current NRC guidance (i.e., BTP 7-19) for both operating and new plants.
- Based in part on the design measures in EPRI Technical Report (TR)-3002005326, "Methods for Assuring Safety and Dependability when Applying DI&C Systems."

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

NEI 16-16
Status

- NEI provided second draft to NRC in May 2017
- NRC and NEI held joint meetings to discuss and resolve comments
- In February 2018, NEI requested that NRC pause review of this document
  - EPRI is revising TR-3002005326

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Implementing Commission Policy on CCF in DI&C

- The staff will update guidance documents to ensure the Commission policy in SRM to SECY-93-087 continues to be consistently applied and address evolving DI&C technologies
- The staff is not proposing nor requesting a change to Commission policy <u>at this time</u>
- The staff is developing a Commission Information SECY on future improvement efforts in addressing CCF

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Updating Guiding Principles

- Licensees and applicants should continue to address CCFs due to software
- A D3 analysis for RTS and ESFAS to address CCF concerns continues to be required. This analysis can be either a best estimate (i.e., using realistic assumptions) or a design basis analysis
- Clarify the use of a graded approach for a D3 analysis for less safety critical systems
- Clarify the use of alternate means to address CCF concerns
- Clarify the use of certain design attributes to address CCF concerns

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Next Steps

- Hold stakeholder interactions
- Apply staff clarifications in all activities for regulatory guidance and endorsement activities
  - Issue RIS 2002-22 supplement for 50.59
  - Review of NEI 96-07 Appendix D for 50.59
  - Standard Review Plan (SRP) and/or BTP 7-19 update
  - Review of future industry guidance (e.g., NEI 16-16)
- Provide Info SECY to Commission (August 2018)

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Broader Modernization Activities

- Advanced Reactor Framework
- Research is being performed to evaluate I&C aspects that offers opportunities for potential enhancements in the NRC regulatory infrastructure:
  - Risk informed approach
  - Embedded Digital Devices and Evolving Technologies
  - Technical Basis for Addressing CCF

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Questions?

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

End

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Backup Slides

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Diablo Canyon Review Summary

- The Diablo Canyon Power Plant (DCPP) PPS design includes diverse means of providing required safety functions in the event of a PPS software CCF
  - Used two I&C platforms, Tricon and Advanced Logic System (ALS)
- Performed D3 analysis assuming loss of all functions performed by the Tricon
  - Postulated software CCF for all plant accidents and Anticipated Operational Occurrences (AOO's)
  - Identified parameters for which there is no existing automatic diverse backup function
- Assigned functions to ALS
  - Confirmed that the effect of postulated CCFs of the ALS did not cause a loss of these safety functions
- Eliminated the need for operators to perform manual actions to cope with a software CCF

U.S.NRC
United States Nuclear Regulatory Commission
Protecting People and the Environment

Comments on RIS 2002-22 Supplement 1 from Ken Scarola, Nuclear Automation Engineering 2018-05-17

As I said earlier, I have been a champion for digital technology in the nuclear industry for the past 43 years. I was the author of the defensive measures, the Ps and Ls, in the EPRI document which was referred to by the Staff and discussed by Rob Austin, and I was the lead author for the first draft of NEI 16-16, which adopts those defensive measures.

I am here because I have strong concerns regarding the upcoming RIS on digital upgrades under 50.59.

Please understand that the latest version of this RIS has not been released to the public, so my comments today reflect the RIS that I reviewed in mid-March.

I completely agree with Gordan Skillman that 50.59 is only a screening process to determine if NRC review is needed. In many areas the NRC's regulatory guidance is sufficient to conclude that NRC review is not needed. For example, IEEE-344 gives us deterministic guidance for preventing CCF due to earthquakes, IEEE-384 gives us deterministic guidance for preventing CCF due to electrical faults, RG 1.180 gives us deterministic guidance for preventing CCF due to EMI hazards, RG 1.106 gives us deterministic guidance for preventing CCF due to a setpoint design error; I could go on and on, there are many more.

But until there is clear regulatory guidance for deterministic attributes that can be credited for preventing new sources of CCF that come with digital technology, and clear guidance for analyzing potential CCFs that are not prevented to demonstrate that the malfunction results are bounded by previous accident analysis, the industry is just not ready for digital upgrades under 50.59 for any systems that (1) can directly initiate plant transients or (2) are directly credited for accident mitigation, when digital integration, interconnectivity or standardization are employed. In essence, RIS 2002-22 Supplement 1 puts the cart before the horse. This doesn't mean that there is no low hanging fruit where the RIS can apply; but these are not the areas.

So let me explain why I feel very strongly about this.

There should be no question that digital technology offers the inherent capabilities of integration, interconnectivity, and standardization that can reduce nuclear power operations and maintenance costs, and improve plant performance and availability, while maintaining or even improving plant safety. However, there should also be no question that, if not correctly designed, these same inherent digital capabilities for integration, interconnectivity and standardization have the potential to create unanalyzed malfunctions that may not be bounded by previous plant analyses; thereby, creating conditions that challenge the 50.59 criteria, and even worse may threaten plant safety.

The issue of a design defect in a standard digital platform, causing a CCF of redundant safety divisions seems to be well understood throughout the industry. But I'd like to offer some examples of much more likely CCFs that are not so well understood:

1. The accident analysis for a typical overcooling event may consider flow from one main feedwater pump whose analog controller has erroneously demanded full flow. But if two

feedwater pumps are controlled by one digital controller, which is common practice in digital upgrades, a single random hardware failure within that controller may cause an erroneous demand for full flow from two feedwater pumps. Therefore, if not properly designed the new digital system has the potential to cause a new unanalyzed CCF that challenges DNBR margin and RCS pressure limits.

2. The accident analysis for a typical power distribution anomaly event may consider a single control rod deviation, or the erroneous withdrawal of one symmetrical control rod group. But if multiple control rods and multiple groups are controlled by one digital controller, which is also a common practice in digital upgrades, a single random hardware failure within that controller may cause an erroneous motion demand for multiple control groups or multiple asymmetrical control rods. Therefore, if not properly designed the new digital system has the potential to cause a new unanalyzed CCF that challenges local power density fuel design limits.

With your patience, I'll offer one more example and then I'll get to my point.

3. Distributed control systems commonly connect multiple controllers to the same digital data communication network and the same operator workstations with soft touch screen controls. Even if control functions are distributed to different controllers - for example reactivity control in one controller, pressure control in a second controller, and temperature control in a third controller - a data storm on that network or erroneous commands from that operator workstation can result in concurrent erroneous operation of all of those control functions. Even with no hardware failures, a digital design defect, such as a software coding error, could adversely affect all of those control functions concurrently.

The common industry response to these examples is 'so what, these are non-safety functions'; but this vividly illustrates a wide-spread misunderstanding. Many I&C system designers simply don't understand that most safety analyses consider only one control function or component failure at a time, such as erroneous pressure control or erroneous temperature control or an excess flow demand from one turbine bypass valve, which are the likely malfunctions with analog systems, not multiple concurrent control function failures or multiple concurrent component failures that are the likely scenarios with incorrectly designed digital systems. Therefore, if not properly designed, a new distributed digital control system has the potential to cause an unanalyzed CCF that challenges one or more critical safety functions.

There are certainly deterministic design solutions to prevent each one of these potential new unanalyzed CCFs, as there are also deterministic design solutions to prevent a CCF within a redundant safety system. But here is the problem. The RIS, as it was written a few months ago, does not require deterministic design solutions, even if it did there is no regulatory guidance for what those design attributes should be.

Regardless, the RIS allows licensees to make highly subjective qualitative assessments regarding the adequacy of the CCF defensive measures employed in a digital upgrade. This includes qualitative assessments of operating experience and design process to conclude that a CCF due to a digital software error requires no further consideration. Based on those qualitative assessments alone, and with no further analysis to determine the plant level effect of a potential digital CCF, the licensee can say "No" to the

50.59 question does the digital upgrade “Create a possibility for a malfunction of an SSC important to safety with a different result” and “No” to the 50.59 question does the digital upgrade “Create a possibility for an accident of a different type”.

The only exception in the RIS for allowing these subjective qualitative assessments is for the automatic reactor trip and engineered safety features actuation logic functions. Now I get even more concerned, because this tells me that the NRC I&C branch doesn’t understand the even greater safety significance of other safety functions, such as the instrumentation and manual controls needed to mitigate a steam generator tube rupture or the automatic load sequencers needed to mitigate a loss of offsite power. I wonder, did the I&C branch engage NRC safety analysts, NRC PRA analysts or the NRC electrical systems branch when they decided these very narrow RPS/ESFAS limitations?

I have no problem with qualitative assessments; we make them all the time in this industry. But when qualitative assessments are used alone, they should be used only to conclude that a CCF due to a design defect is significantly less likely than a single random hardware failure, and therefore can be analyzed as a beyond design basis event. Qualitative assessments should not be used as the sole basis of a conclusion that no further plant level analysis of the potential CCF is needed at all.

I hope we have learned from Fukushima Daiichi and other accidents, that we should be prepared to cope with the unexpected. Demonstrating our ability to cope with unexpected CCFs is the position taken by the commissioners in the SRM to SECY 93-087, and the consistent position of the Staff in BTP 7-19. Neither of these regulatory documents limit their applicability to RPS and ESFAS; these documents recognize the safety significance of other systems and require demonstration of coping for a CCF in other systems. To my knowledge, the Staff has no authority to change the NRC policy reflected in either of these regulatory criteria through a RIS, especially when that RIS creates a serious threat to plant safety.

As currently written in this RIS, with the exception of upgrades to the automatic actuation logic in RPS and ESFAS, licensees can employ subjective qualitative assessments of design processes and/or operating experience to consciously gloss over the potential for new unanalyzed CCF events and their threat to plant safety. As an alternative, I strongly recommend that we maintain the defense-in-depth foundation of the nuclear power industry by ensuring:

(1) That well defined deterministic design attributes are needed to reach a conclusion that CCF likelihood is “sufficiently low” to require no further consideration in the evaluation 50.59 Questions 5 and 6.

AND

(2) For digital upgrades where adequate deterministic design attributes do not exist, the RIS should require plant level analysis for evaluating potential new CCFs, to ensure that we can cope with these new malfunctions and that the plant level results are bounded by previous analyses.

If the RIS is clear on these two technical points, then digital upgrades under 50.59 will be unquestionably safe, and therefore will not need Staff review/approval. If the RIS is not clear on the requirement for deterministic attributes, then the NRC will be giving licensees the authority to make

qualitative judgements that only NRC should be making, because non-conservatism in these subjective judgements will adversely affect the defense-in-depth that is the foundation of safety in this industry.

To conclude:

RIS 2002-22 was seriously flawed, because it did not clarify the Staff's position on digital CCF. This has deterred digital upgrades, which has been a detriment to the competiveness of the nuclear industry. The RIS-2002-22 Supplement 1, as it was written a couple of months ago, does nothing to augment this lack of clarity; even worse, it leverages this lack of clarity and lack of NRC regulatory guidance to establish qualitative assessments as the basis for 50.59 digital upgrades.

As I said at the beginning - In many areas the NRC's regulatory guidance is sufficient for effective and safe 50.59 upgrades. Until there is clear regulatory guidance for deterministic attributes that can be credited for preventing new potential digital CCFs, and clear guidance for analyzing potential CCFs that are not prevented, the industry is just not ready for digital upgrades under 50.59 for any systems that (1) can initiate plant transients or (2) are directly credited for accident mitigation, when digital integration, interconnectivity or standardization are employed. Again, RIS 2002-22 Supplement 1 puts the cart before the horse.

I said earlier today, I was not here to interfere with ISG-06 in any way. I can't say that about RIS 2002-22 Supplement 1. In the commissioner's response to SECY-15-0106, they directed the Staff to fix the digital licensing infrastructure, not patch it. Although I don't like patches of any kind, unlike ISG-06 which is a safe patch, this one is not.

I understand that the Staff has not requested ACRS input on this RIS. For the safety of the nuclear power industry, I believe that is a serious mistake. The ACRS should be commenting on this RIS.

Thank you for listening.

Additional Comment on RIS 2002-22 Supplement 1 from Ken Scarola, Nuclear Automation Engineering 2018-05-18

In the ACRS DI&C subcommittee meeting, 2018-05-17, there was a discussion of embedded digital devices.

Information Notice 2016-01 describes a hidden design defect in a time delay relay with an embedded digital device. The IN states that with this defect "EDGs 3 and 4 could simultaneously have been unable to tie to their respective emergency busses." As written, RIS 2002-22 Supplement 1 would allow this digital relay to have been employed to replace analog time delay relays all over the plant, except in RPS and ESFAS actuation logic, using a qualitative assessment of operating history. Since operating history did not reveal this design defect, there would have been no consideration of a potential CCF when answering 50.59 Questions 5 and 6. As a result, there would be no licensee evaluation of coping with this CCF should it occur.

As I commented previously, qualitative assessments should be used only to establish a basis for treating a CCF due to a design defect as a beyond design basis event and demonstrating coping accordingly. Qualitative assessments should never be used alone as the basis of no further consideration of a CCF. This is defense-in-depth, as reflected in the SRM to SECY 93-087.