

Official Transcript of Proceedings
NUCLEAR REGULATORY COMMISSION

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

Docket Number: (n/a)

Location: Rockville, Maryland

Date: Thursday, November 21, 2019

Work Order No.: NRC-0681

Pages 1-245

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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23

DISCLAIMER

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS

1323 RHODE ISLAND AVE., N.W.

WASHINGTON, D.C. 20005-3701

(202) 234-4433

www.nealrgross.com

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

UNITED STATES OF AMERICA

NUCLEAR REGULATORY COMMISSION

+ + + + +

ADVISORY COMMITTEE ON REACTOR SAFEGUARDS

(ACRS)

+ + + + +

DIGITAL I&C SUBCOMMITTEE

+ + + + +

THURSDAY

NOVEMBER 21, 2019

+ + + + +

ROCKVILLE, MARYLAND

+ + + + +

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

COMMITTEE MEMBERS:

CHARLES H. BROWN, JR. Chair

RONALD G. BALLINGER, Member

DENNIS BLEY, Member

VESNA B. DIMITRIJEVIC, Member

WALTER L. KIRCHNER, Member

JOSE MARCH-LEUBA, Member

JOY L. REMPE, Member

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

ACRS CONSULTANT:

MYRON HECHT

DESIGNATED FEDERAL OFFICIAL:

CHRISTINA ANTONESCU

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

CONTENTS

Opening Remarks 4

Introductory Remarks 13

Draft BTP 7-19, Rev.8 17

Industry Perspectives on Common Cause 150

Failures (CCFs) in Digital Systems

EPRI R&D Perspectives on Digital I&C 205

Reliability and Software CCF

Public Comments 242

Closing Remarks 243

P R O C E E D I N G S

10:02 a.m.

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

4 The rules for participation in today's
5 meeting have been announced as part of the notice of
6 this meeting previously published in The Federal
7 Register. The rules for participation in all ACRS
8 meetings was announced in The Federal Register on June
9 3rd, 2019.

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

16 Portions of this meeting can be closed as
17 needed to protect proprietary information, pursuant to
18 552b(c)(4), as stated in The Federal Register notice
19 and in the public meeting notice posted to the
20 website.

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

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

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

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

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

22 MEMBER REMPE: Is that electronic?

23 (Laughter.)

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 text, barely.

2 Where was I?

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

19 CHAIRMAN BROWN: Dennis, which part of
20 719? Was that Section 3?

21 MEMBER BLEY: Yes.

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

24 MEMBER BLEY: Yes.

25 CHAIRMAN BROWN: That's item Section 3?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

8 MEMBER BLEY: Okay.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

14 MEMBER BLEY: Yes.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 CHAIRMAN BROWN: Okay. Thank you very
4 much.

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

7 (No response.)

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

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

12 CHAIRMAN BROWN: We finally got to Eric.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

25 CHAIRMAN BROWN: I'll make one other

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 terms of the framework, the five fundamental
2 principles.

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

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

20 Have at it, Wendell, Deanna.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

18 MR. MORTON: Okay.

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

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

25 We'll also talk about the means to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

10 Okay, yes, next slide.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 get into in our later slide.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 direction was in the SRM.

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

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

19 MEMBER MARCH-LEUBA: Okay.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

13 Next slide.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

5 Next slide.

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

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

21 CHAIRMAN BROWN: Would you say that again?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

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

19 MR. MORTON: Correct.

20 CHAIRMAN BROWN: Not A1?

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

24 CHAIRMAN BROWN: Change into what space?

25 MR. MORTON: Well, 50.90 space, for

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 license amendment space.

2 CHAIRMAN BROWN: License amendment?

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

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

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

9 MR. MORTON: Right.

10 MEMBER BLEY: That throws you back here.

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

17 MR. MORTON: Okay.

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

23 MR. MORTON: It does. It does.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 CHAIRMAN BROWN: That's what --

4 MS. ZHANG: Let me try to clarify.

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

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

9 So, the reason we incorporated the
10 qualitative assessment here -- we could have just
11 said, well, if you're performing a qualitative
12 assessment, that means that it's not an A1 system.
13 And that means that you're likely to do it under
14 50.59. So, why put any guidance on qualitative
15 assessment here?

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

18 MR. MORTON: Yes.

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

21 MR. MORTON: Yes.

22 CHAIRMAN BROWN: -- for the A1 systems.

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

25 MR. MORTON: Sure.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

5 (Laughter.)

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

8 MS. ZHANG: Yes.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

16 MR. BENNER: Absolutely.

17 MR. MORTON: Yes.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 it is.

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

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

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

25 MR. MORTON: Okay. Thank you for that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 input.

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

5 MEMBER BLEY: Yes, I was.

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

15 MS. ZHANG: Eliminate, mitigate --

16 CHAIRMAN BROWN: Mitigate.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 they don't.

2 MEMBER BLEY: Yes, that was my point.

3 CHAIRMAN BROWN: Okay?

4 MR. MORTON: Okay.

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

12 MS. ZHANG: I got it.

13 CHAIRMAN BROWN: -- about that also.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 do.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

13 MR. BENNER: Yes.

14 CHAIRMAN BROWN: Love that word.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 what you get back from them.

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

8 (Pause to reconnect to the public phone
9 line.)

10 CHAIRMAN BROWN: Are we okay now?

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

10 (Laughter.)

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 reiterate that point.

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

5 MR. MORTON: Yes, right.

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

11 MS. ZHANG: I think we tried.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 So, okay, go ahead.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

15 MR. MORTON: Yes.

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

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

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

22 MS. ZHANG: Thank you, Wendell.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

9 MR. MORTON: Yes.

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

17 MR. MORTON: Correct.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MR. MORTON: Right.

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

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

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

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

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

13 MR. MORTON: Correct.

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

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

18 CHAIRMAN BROWN: Yes.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

18 CHAIRMAN BROWN: Yes, thank Jose.

19 MS. ZHANG: And Jose, Member Jose.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 CHAIRMAN BROWN: It ought to be clear.
4 Can I ask, before you do that --

5 MS. ZHANG: Yes.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

7 CHAIRMAN BROWN: Everything fails.

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

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

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

14 MS. ZHANG: Yes.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

13 MR. MORTON: Uh-hum.

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

25 You can go ahead and finish your going

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

19 CHAIRMAN BROWN: Yes, but within that
20 concept, I fully understand that because I can say, in
21 1978-79, when we first tried to apply this to the
22 naval nuclear plants -- and the only processor
23 available was a Z80, 2.3 megahertz, high-powered, node
24 memory -- we went out with a set of specs. And the
25 vendors that we went to bid said, oh -- and we were

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

7 MEMBER BLEY: And right there you hit the
8 difference.

9 CHAIRMAN BROWN: That's right.

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

13 CHAIRMAN BROWN: Exactly. And we said no.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

7 (Laughter.)

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

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

12 CHAIRMAN BROWN: Yes, thank you.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

5 MEMBER BLEY: You kind of blushed past
6 50.69, which uses the same language.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

25 MEMBER MARCH-LEUBA: In that light,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

19 In addition, I just want to state that --
20 (Noise on phone line.)

21 MEMBER MARCH-LEUBA: That is your
22 feedback.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

4 Dennis?

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

7 CHAIRMAN BROWN: Yes.

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

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

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

23 (Laughter.)

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Just a thought.

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

5 (Laughter.)

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

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

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

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

18 CHAIRMAN BROWN: Or one system.

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

22 MS. ZHANG: Thank you.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

12 MR. MORTON: Yes, yes.

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

21 MS. ZHANG: Well, it depends, right?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

6 CHAIRMAN BROWN: Exactly.

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

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

15 MS. ZHANG: Yes.

16 MR. MORTON: And we took that input.

17 MS. ZHANG: Yes.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

14 I understand what you're saying --

15 MS. ZHANG: Yes.

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

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

23 MR. MORTON: Right.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

14 MS. ZHANG: Yes.

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

18 MS. ZHANG: Maybe I should go on.

19 (Laughter.)

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

9 MR. MORTON: Yes, correct.

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

12 MR. MORTON: Yes, yes.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 breaking point right now.

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

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

6 CHAIRMAN BROWN: Scott, what did you say?

7 MR. MOORE: Mr. Chairman --

8 CHAIRMAN BROWN: I can hear you, Scott.

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

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

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

21 MR. MOORE: Right.

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

25 MR. MOORE: Absolutely.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

9 CHAIRMAN BROWN: That's fine. Okay.

10 MR. MOORE: Thank you, sir.

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

15 Recess.

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

19

20

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

2 1:05 p.m.

3 CHAIRMAN BROWN: The meeting will come
4 back to order.

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

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

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

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

25 So, for the first one, means to eliminate

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

14 So, we did try to address that aspect.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

24 (Laughter.)

25 MR. REBSTOCK: Paul Rebstock, the Office

1 of Research.

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

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

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

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

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

5 MS. ZHANG: Okay. Thank you, Paul.

6 MR. REBSTOCK: Okay.

7 MS. ZHANG: Next slide. No?

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

19 MR. MORTON: Okay.

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

22 MR. MORTON: Uh-hum.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 you can still get your protective actions.

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

8 CHAIRMAN BROWN: I understand that.

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

16 CHAIRMAN BROWN: I know that.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

21 Dennis, did you want to say something
22 or --

23 MEMBER BLEY: No.

24 CHAIRMAN BROWN: Myron?

25 MR. HECHT: Yes. I'm sorry.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: No, go ahead.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

14 MR. HECHT: Okay. Thank you.

15 MS. ZHANG: Slide.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 Ultimately, we decided to leave it in
4 because, one, we wanted to provide flexibility,
5 because it may be applicable to a very simple portion
6 of the design, right? So, it might not be applicable
7 to an entire system, but maybe a component within the
8 system where you can at least eliminate that part of
9 it from the rest of the D3 assessment. So, that's the
10 reason we decided to leave it in. We got rid of the
11 100 percent testing terminology and just provided the
12 criteria associated with that testing.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: Well, there are --

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

25 MR. HECHT: What if I include a hardware

1 memory management unit?

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

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

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

14 MR. HECHT: It was not?

15 MS. ZHANG: It was not.

16 MR. HECHT: Okay.

17 CHAIRMAN BROWN: For testing?

18 MS. ZHANG: For testing.

19 CHAIRMAN BROWN: Oh, yes, I got it.

20 (Laughter.)

21 MS. ZHANG: Okay. Next slide.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

7 CHAIRMAN BROWN: It doesn't exist.

8 MS. ZHANG: Yes.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

7 MEMBER BLEY: Can I jump in with
8 something?

9 MS. ZHANG: Uh-hum.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

6 MS. ZHANG: Yes.

7 MEMBER BLEY: Then, I'm happy.

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

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

25 For manual operator action, this is an

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: I got that part.

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

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

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

20 MS. ZHANG: Yes.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: Thanks, Member Brown.

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

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

8 (Laughter.)

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

8 CHAIRMAN BROWN: What is a latent software
9 defect?

10 MS. ZHANG: A latent software defect is --

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

13 MS. ZHANG: Okay.

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

16 MR. MORTON: Well, finish your thought
17 first.

18 MS. ZHANG: Okay.

19 CHAIRMAN BROWN: I'm sorry.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 caveats as far as its quality and reliability.

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

4 CHAIRMAN BROWN: No, let me --

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

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

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

25 CHAIRMAN BROWN: Yes, but --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

15 MEMBER BLEY: -- to drive --

16 CHAIRMAN BROWN: Just one way.

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

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

25 MEMBER BLEY: At which you're normally

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 operating.

2 CHAIRMAN BROWN: At which you exceed --

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

6 CHAIRMAN BROWN: Yes.

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

9 CHAIRMAN BROWN: I don't agree with that.

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

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

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

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

25 MEMBER MARCH-LEUBA: Yes, but there is

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

16 (Laughter.)

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

25 MEMBER BLEY: You seem to be saying we've

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 (Laughter.)

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

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

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

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

11 (Laughter.)

12 But I want to bring more context now.

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

15 MR. MORTON: Maybe.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

21 CHAIRMAN BROWN: All right. Go ahead.

22 MR. MORTON: Okay.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

17 And when we reviewed the SRM, between
18 position 3 and position 4, we noticed that there are
19 essentially two separate ways you can read that,
20 whether 3 can be 4; can something that's credited for
21 performing 3 also be credited for performing position
22 4, and the other way around? So, when we looked at
23 that, we said, obviously, position 4 was very, very
24 specific. It didn't give you any flexibility.

25 CHAIRMAN BROWN: The main control room?

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

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

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

8 CHAIRMAN BROWN: You've got to bypass --

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

11 CHAIRMAN BROWN: Bypassing the --

12 MS. ZHANG: The logic.

13 CHAIRMAN BROWN: -- logic area?

14 MS. ZHANG: Yes.

15 CHAIRMAN BROWN: Yes.

16 MS. ZHANG: Not subject to whatever.

17 CHAIRMAN BROWN: Bypass the computerized
18 portion?

19 MS. ZHANG: Yes.

20 CHAIRMAN BROWN: You left that out.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

25 MR. MORTON: They're not at a particular

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 station.

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

4 MR. MORTON: Right. Yes.

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

9 CHAIRMAN BROWN: But 4 covers that.

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

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

21 MS. ZHANG: Exactly.

22 CHAIRMAN BROWN: Even though they may not
23 substitute.

24 MS. ZHANG: Exactly.

25 CHAIRMAN BROWN: That's reasonable.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MS. ZHANG: In addition, I know one of the
2 points that were identified earlier was, why is the
3 30-minute margin, why is that not in here anymore?
4 And the reason it is that way is because we're trying
5 to align with SRP Chapter 18, which recently underwent
6 a revision, where they want to take it from a more
7 holistic look, and not just at a timing aspect, but
8 also the accessibility of the equipment, the
9 reliability of the equipment, and the availability of
10 the equipment during the associated event conditions.

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

14 CHAIRMAN BROWN: I agree. Yes.

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

17 CHAIRMAN BROWN: Exactly.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

13 CHAIRMAN BROWN: Not since I've been here.

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

16 (Laughter.)

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

4 MS. ZHANG: Well, if you look at Reg Guide
5 1.62 in terms of where the manual system feeds in --

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

9 MS. ZHANG: Yes.

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

12 MS. ZHANG: Yes.

13 CHAIRMAN BROWN: 1.62 is in there.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

2 MS. ZHANG: Yes.

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

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

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

20 CHAIRMAN BROWN: Okay. That's Section
21 3 --

22 MEMBER BLEY: Mr. Brown --

23 CHAIRMAN BROWN: Oh, I'm sorry.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 you were here at that point in time --

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

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

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

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

15 CHAIRMAN BROWN: Yes.

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

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

20 (Laughter.)

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

14 MR. MORTON: Yes, comment noted.

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

17 MS. ZHANG: Thank you.

18 Next slide.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

7 Thank you, Deanna.

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

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

23 Yes?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

3 MR. MORTON: Yes.

4 CHAIRMAN BROWN: So, that was a good
5 approach.

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

9 (Laughter.)

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

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

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

20 So, is there another question on it?

21 CHAIRMAN BROWN: Yes, go ahead.

22 MR. MORTON: So, another key change we had
23 was with the spurious operation assessment. Now Rev.
24 7 did have some guidance on spurious actuation. We
25 redefined it as spurious operation to be a little more

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

2 CHAIRMAN BROWN: As opposed to what?

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

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

7 MR. MORTON: Yes.

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

10 MR. MORTON: Yes.

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

25 The other area for advanced reactors we

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

10 The other one was in Section 3.7 of the
11 Rev. 7 there was a set of words, if I can find them.
12 That's Rev. 8. I need to find Rev. 7 here. You
13 notice I've still got paper. It was, yes, Section
14 3.7, your all's response in cases in which a credible
15 postulated spurious operation caused -- I've changed
16 the word -- caused by a software CCF -- they talk
17 about coping strategy. And that was another good
18 generalized thought process that I thought part of the
19 preamble to go along with the other two. Again,
20 that's a suggestion. Obviously, our comments are
21 comments personally. They are not Subcommittee
22 comments. They're not even Committee comments until
23 we write a letter, and we won't be until after your
24 public comments, the public comment period, and we see
25 how all this plays out.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

14 MS. ZHANG: Yes.

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

17 MR. MORTON: Yes.

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

22 MR. MORTON: Cope, yes.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

7 CHAIRMAN BROWN: Okay.

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

12 CHAIRMAN BROWN: Right.

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

15 CHAIRMAN BROWN: Preambles are nice --

16 MR. MORTON: Yes.

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

20 MR. MORTON: Yes.

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

23 MR. MORTON: Okay.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 here, anyway, 24?

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

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

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

8 CHAIRMAN BROWN: Oh, okay.

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

11 CHAIRMAN BROWN: Famous last words.

12 MR. MORTON: I know.

13 (Laughter.)

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

24 MR. MORTON: Yes.

25 CHAIRMAN BROWN: I went off and read 6303,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 1994, which I think is the latest revision.

2 MR. MORTON: Yes.

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

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

18 CHAIRMAN BROWN: Yes.

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

23 CHAIRMAN BROWN: Again, that was another.

24 MR. MORTON: Yes.

25 CHAIRMAN BROWN: You took that out of the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

4 MR. MORTON: Okay.

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

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

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

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

19 CHAIRMAN BROWN: Thirty days?

20 MR. MORTON: Sixty days.

21 CHAIRMAN BROWN: Sixty days?

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

22 CHAIRMAN BROWN: Oh, okay.

23 MR. MORTON: Yes.

24 CHAIRMAN BROWN: Okay.

25 MR. MORTON: Yes, hopefully, initiating a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 public comment period ending in February of next year.

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

5 CHAIRMAN BROWN: Okay.

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

8 And then, we do anticipate two more ACRS
9 meetings. One, another Subcommittee meeting, I
10 believe we're targeting for April of next year, April
11 8th of next year. Thank you. That meeting will take
12 place after the public comment period is completed.
13 We will resolve public comments. So, we should be in
14 plenty of time for that. And the full Subcommittee
15 meeting will be, I believe, the following month in May
16 of next year.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

22 MR. MORTON: Correct.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 something, I don't think.

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

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

14 MR. MORTON: Yes.

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

20 MR. MORTON: Well, the point of --

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 will be resolving the public comments internally.

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

4 MS. ZHANG: Yes.

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

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

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

17 MS. ZHANG: August.

18 MR. MORTON: August.

19 MS. ZHANG: The 29th.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

11 (Laughter.)

12 You're chuckling, Dennis.

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

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

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

23 MR. MORTON: Yes, that's great.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

2 MR. MORTON: Okay.

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

5 (Laughter.)

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

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

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

13 MR. MORTON: A minute early.

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

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

19 So, we are recessed until 2:45.

20 (Whereupon, the foregoing matter went off
21 the record at 2:29 p.m. and went back on the record at
22 2:51 p.m.)

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

25 And we have NEI who is now going to make

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

12 Before I get started, any questions?

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

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

19 MEMBER BLEY: Okay.

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

23 MEMBER BLEY: Yes, actually more than
24 that.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 work with EPRI.

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

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

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

20 MEMBER MARCH-LEUBA: That's for analogs?

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

8 (Laughter.)

9 MR. VAUGHN: Yes.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

19 CHAIRMAN BROWN: So, these were PRA --

20 MR. VAUGHN: Yes.

21 CHAIRMAN BROWN: -- models?

22 MR. VAUGHN: Yes. Current PRA.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

4 MR. HECHT: Okay, but my question is, is
5 that 10 to the minus 4th per year or 10 to the minus
6 4th --

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

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

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

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

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

20 CHAIRMAN BROWN: This is analog systems.

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

5 CHAIRMAN BROWN: I would counter that, in
6 35 years of running of the I&C division for the
7 Naval -- well, 22 for running it and 35 in it -- I had
8 one common-cause failure which was a relay that they
9 processed the laminations, cooled them, quenched them
10 in oil, didn't bother to clean them. And when they
11 put them in service, the oil oozed out on the top of
12 the laminate; the armature came down. It took a
13 while, but they would stick. And we had one occur.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

9 MEMBER DIMITRIJEVIC: Yes.

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

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

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

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

20 MEMBER MARCH-LEUBA: Microphone.

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

23 (Laughter.)

24 MEMBER REMPE: It has to be on the record.

25 (Laughter.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

17 (Pause to reconnect to the public phone
18 line.)

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

17 MR. VAUGHN: So, what we do agree with is
18 that, going back to 100 percent testing and diversity
19 being the only two ways to eliminate CCF, we didn't
20 agree with because it was unattainable. All right.
21 We don't need to rehash the discussion, but the whole
22 100 percent testing, that was designed for simple
23 things that you could 100 percent test; whereas, if
24 someone comes in with an RPS/ESFAS, a complex system
25 where you have software, you can't test it. Well,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 latent software defect.

2 CHAIRMAN BROWN: Uh-hum.

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

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

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

7 MEMBER BLEY: Yes, I would agree with you.

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

14 MEMBER BLEY: Go ahead.

15 MR. VAUGHN: Okay.

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

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

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

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

5 And I'm hearing the phone --

6 MEMBER BLEY: Yes, try to keep going.
7 Ignore it if you can.

8 MR. VAUGHN: Okay. We lost connection?
9 Continue or?

10 CHAIRMAN BROWN: Sorry, gentlemen, our
11 high-quality, microprocessor-driven, electronic system
12 is getting confused from a common-cause failure.

13 (Laughter.)

14 (Pause to reconnect to the public phone
15 line.)

16 Is there someone on the line?

17 MEMBER MARCH-LEUBA: They need to call in.

18 CHAIRMAN BROWN: It said there's two
19 people including us.

20 If there's somebody on the line, can they
21 hear me?

22 MEMBER BLEY: They're probably silenced.

23 (Someone on the phone line speaks.)

24 CHAIRMAN BROWN: Thank you. Please mute
25 now. We appreciate that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MR. VAUGHN: All right. So, that's the
2 background and context, sort of framed the challenge
3 that we been dealing with for several years and are
4 continuing to deal with.

5 And now, I would like to turn it over at
6 a high level to provide what our path forward is from
7 a solution perspective. And I'm going to turn it over
8 to Neil Archambo from Duke Energy to lead that
9 discussion.

10 MR. ARCHAMBO: Okay. In the industry, of
11 course, up to this point, we've been dealing with
12 common-cause failure in kind of a hybrid, confusing
13 approach. We know we have to deal with common-cause
14 failure. We know that the probability of common-cause
15 failure is not zero.

16 So, what we're doing here, what we're
17 talking about here on these first principles, we want
18 to take a step back and see what constitutes a CCF --
19 where does it come from? -- and understand that.
20 Instead of throwing everything and the kitchen sink at
21 a design, step back and see where do we need to focus
22 our efforts to eliminate/mitigate common-cause
23 failures in these digital systems, primarily software.

24 So, the first principle you see up there
25 -- and software quality depends on complete correct

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 requirements, design, and implementation -- and what
2 we found when we implemented digital systems, and
3 we've had errors in those digital systems or events
4 that were caused by those digital systems, is it could
5 be usually traced back to an incomplete or incorrect
6 requirement. There was an incorrect requirement. It
7 was either missing or it was incorrect.

8 Now it doesn't matter how good your
9 software is, if the requirements that you used to
10 design that software are incorrect or missing, you're
11 probably going to experience some problem. So, we
12 realized that that's probably one of the first things
13 we have to do, is work on our requirements
14 development. And we'll talk a little bit about that
15 in the next slide, the path forward on that, how we're
16 addressing requirements development.

17 The second one is we realize that we need
18 concurrent triggering to trigger a defect. If you
19 have software and it has a defect, it has to be
20 triggered somehow in order to cause you a problem, to
21 cause you a failure. If you have a single-loop
22 controller out there with a design defect in the
23 software, and then, that defect gets triggered, you'll
24 have a signal failure, but you won't have a common-
25 cause failure. Now, if you have a couple of single-

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 loop controllers in the system and they experience the
2 same concurrent trigger, then you'll have a common-
3 cause failure. So, that's one of the guiding
4 principles that we're talking about.

5 MEMBER REMPE: Would the people on the
6 line please mute themselves? Thank you.

7 MR. ARCHAMBO: Okay. No problem.

8 And we've also recognized that the effects
9 or likelihood of a software defect can be minimized by
10 design, design attributes. It might be actually
11 software design. It might be external system design
12 attributes. So, we can apply design attributes to
13 further reduce the likelihood of a common-cause
14 failure or mitigate the effects of a common-cause
15 failure.

16 And then, we recognize that operating
17 history can also support software quality. By that,
18 we mean a lot of these platforms that are out in the
19 industry and have millions of hours of operation. And
20 EPRI -- and I suspect Matt will talk about this in a
21 little bit -- has some research on platforms that have
22 been out there and have a tremendous amount of
23 operating experience with a lack of any type of
24 software common-cause failures. So, we can capitalize
25 on that operating history. The operating history may

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 also show you a system that you want to avoid. So, it
2 works both ways.

3 The first principle, we first wanted to
4 align, put our arms around the issue, and figure out
5 what we need in design space to tackle that issue.

6 MR. HECHT: Can I ask a question with
7 respect to the operating history? Earlier this
8 morning, we heard about yet another RES attempt to do
9 some quantitative estimation of software failure
10 probabilities. And I know that the past studies have
11 been hindered primarily by the lack of relevant
12 operating experience, particularly from the nuclear
13 industry. And I think that's been a problem within
14 the NRC for a long time in attempting to address it.
15 In another life, I was also part of those efforts.

16 What do you think is the probability that
17 NEI or EPRI, or both, would be willing to share data
18 that was pretty much at this point safeguarded and
19 kept from the NRC in terms of helping to get that
20 relevant operating history and those failure modes
21 that would really enable a better attempt to address
22 that?

23 MR. ARCHAMBO: Yes, if you're talking
24 about platform software -- and I'll phone a friend,
25 Matt, perhaps -- EPRI just completed a report recently

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 on SIL certification of platforms. And I believe the
2 NRC has that report.

3 MR. HECHT: That's the report. That's not
4 the underlying data.

5 MR. ARCHAMBO: Yes. No, I'd have to ask
6 EPRI if they would be willing to share that underlying
7 data. I'm sure there might be some proprietary
8 information there. So, I'll leave that up to Matt.
9 Maybe when he gets up here --

10 CHAIRMAN BROWN: We'll ask him.

11 MR. ARCHAMBO: -- he can address that
12 question. I can't answer that one. I don't know if
13 anybody up here on the panel can.

14 MR. HECHT: Just with respect to that last
15 point, I mean, data can go a long way to addressing
16 what are largely hypothetical concerns because we
17 don't have enough --

18 MR. ARCHAMBO: Sure.

19 MR. HECHT: -- real experience.

20 MR. ARCHAMBO: Understood.

21 Any more questions on the first principles
22 that we talked about?

23 CHAIRMAN BROWN: Yes, I had one question.
24 Because I haven't seen this in probably 10 or 15 years
25 now. When the program I was in first started doing

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 our computer-based systems in 1979, one of the
2 problems we ran into was a complete lack of software
3 standards. Programming standards just did not exist;
4 quality standards did not exist. And you ended up
5 with a large amount of what I call "spaghetti code".
6 Stuff was carefully intertwined. Programmers love to
7 be fancy, and they all thought they were smarter than
8 everybody else.

9 So, we initially had to develop our own
10 set of software programming standards that we
11 utilized. But, over the years, there's been a great
12 deal of emphasis, at least from what I've read in the
13 IEEE magazines and stuff like that, on developing
14 commercial software standards. I mean, I guess
15 Carnegie-Mellon had some or somebody. I've forgotten
16 the names of all the participants.

17 Is there a good track of really high-
18 quality software standards, like you comment your code
19 extensively, so you can track line by line what you're
20 putting in and what it's supposed to be doing, as
21 opposed to what you thought it was doing, but you
22 forgot because you didn't tell yourself? I have no
23 connection with that now. It's just been so long.

24 MR. ARCHAMBO: Yes, there is actually.
25 And we've been looking at the IEC standards, primarily

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 the 61508 and the 61511, I believe. IEC 61508, Part
2 3, has a pretty significant guidance on coding
3 standards, exactly what you're talking about. It goes
4 down to the detail of commenting, how much white
5 space, how many lines per module of software code.
6 For instance, they want to keep the lines per module
7 of software below 100 lines of code; one single input,
8 one exit to a routine, things like that. So, today
9 there is good standards out there to develop software.

10 We're looking at those standards in our
11 industry to apply those to, more or less, the
12 application software that we mostly deal with. But
13 those standards do exist now. Other industries are
14 using those standards.

15 CHAIRMAN BROWN: I guess the operating
16 system coding is pretty tough to get your hands on
17 from --

18 MR. ARCHAMBO: It is.

19 CHAIRMAN BROWN: -- the various guys that
20 build the platforms.

21 MR. ARCHAMBO: Right. Now what we have to
22 rely on the platforms, for instance, the platform
23 software, is, one, it's either been pre-approved by
24 the NRC -- that means the NRC looked at it and pre-
25 approved it. And what we're trying to go for, also,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 we'll work with the NRC on, and I think we're getting
2 there, is the SIL certification, the Safety Integrity
3 Level certification. If you're not familiar with
4 that, there's four levels of SIL certification.

5 And the SIL certification is usually based
6 on the IEC standards. So, for instance, a protection
7 system may be a SIL 3-certified system, would
8 demonstrate the quality needed for a system of that
9 safety significance. So, those are the kind of things
10 we're looking at right now bringing into the industry,
11 so we can demonstrate software quality at the platform
12 level.

13 Because at the plants, clearly, we don't
14 have access to the code. We don't have that. We
15 probably wouldn't know what we were looking at. What
16 we need to focus more on at the plants is if we have
17 good application software. We have to develop -- I
18 mean platform software -- we have to develop
19 application software, and that's where we want to
20 really focus our efforts on, because that's where we
21 find in the research, in EPRI's research and
22 operational experience, that's where our failures come
23 in. It's development of the application software.
24 The platform software works fine. It's the
25 application software.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 And again, a lot of that goes back to the
2 requirements, an incomplete or missing requirement
3 that led to that application software defect. The
4 software usually does exactly what you tell it to.
5 Sometimes you didn't intend to tell it to do
6 something, and it will do it perfectly in most cases.

7 MR. HECHT: In response to your question,
8 Charlie, there is a standard called MISRA, which was
9 developed by the Motor Industry Reliability
10 Association of the United Kingdom. It's called
11 MISRA C, and there's one MISRA C++, which are widely
12 accepted now in multiple industries.

13 With respect to operating systems, the FAA
14 has accepted for use giving licenses for an integrated
15 system of real-time operating systems from several
16 vendors, including Green Hills, Wind River, and
17 several others. And they've made that source code
18 available, and they've provided what are called
19 certification packages, so that an avionics
20 manufacturer can include that software data with their
21 own application and submit it to the FAA for approval,
22 including --

23 CHAIRMAN BROWN: The source code was open?

24 MR. HECHT: To the FAA.

25 CHAIRMAN BROWN: To the FAA?

1 MR. HECHT: Yes. Including the MCAS
2 system and the 737 MAX, but, as was pointed out
3 earlier, I think that was a requirements and an
4 integration problem, as Joy pointed out.

5 CHAIRMAN BROWN: Okay. Thank you.

6 MR. ARCHAMBO: If there's no other
7 questions on that slide, I'll go to the next slide.

8 All right. So, how do we apply these
9 first principles? That's what this slide is all
10 about. Again, our research and our experience tells
11 us it goes back to requirements development. You have
12 to do your homework upfront to get those requirements
13 correct.

14 Now, up to this point, when we developed
15 requirements, it was a lot of times a lot of people
16 sitting in a room coming up with things they thought
17 would be good for the system. And there was other
18 sources where we got requirements from. We never had
19 a real systematic process for developing your
20 requirements. Well, that's changed. That's changed.
21 The nuclear industry has implemented the Digital
22 Engineering Guide from EPRI, and the Digital
23 Engineering Guide is really heavy on requirements
24 development.

25 And what we're using is a process that was

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 developed by MIT. It's called the Systems Theoretical
2 Process Approach, or STPA. And it's a system that
3 walks us through how to develop requirements. It's
4 not a haphazard approach.

5 We've had some industry workshops and it
6 is very effective. In fact, some of the issues that
7 we had where we missed requirements in designs, we
8 worked through those with a blind class of people that
9 had no idea what the problem was with that design.
10 And we were able to flesh out that requirement that
11 was missing prior to the design. So, it looks like it
12 will prove very effective in developing our
13 requirements.

14 So, we're applying that into our designs
15 now to get our requirements. Because, again, even if
16 you have the best software, the best software on the
17 market, if you have a missing or incomplete
18 requirement, you're going to have problems, and we
19 recognize that.

20 MEMBER BLEY: Can you give us a quick
21 tutorial, a couple of bullet items, on what kind of
22 application software the plants are developing
23 separate from the big system software that they're
24 installing?

25 MR. ARCHAMBO: Sure. If you take a

1 turbine control system, for instance, you'll choose a
2 platform for your turbine control systems, but, then,
3 you have to apply it, of course, to your particular
4 system.

5 One that's kind of near and dear to my
6 heart is recent. We developed the requirements for
7 that application software, and a lot of times that's
8 logic that we're building for that particular, you
9 know, to integrate that platform into our system. But
10 we like to put in a lot of redundancy, as you would
11 expect, into these systems, minimize the single points
12 of vulnerability. A lot of times we do that by having
13 three sensors feed a median select device that, then,
14 feeds that signal into our system, right? And that
15 way, if one of those sensors fails, you still have two
16 others. And instead of median select, it usually goes
17 on to an average of those two signals.

18 A lot of times people put a requirement
19 that says, if those all of those three signals go out
20 of range for whatever reason, trip the system;
21 sometimes wrong. We don't trust our sensors, so trip
22 the system. And a lot of times that's a good
23 requirement, but not always.

24 MEMBER BLEY: It's not.

25 MR. ARCHAMBO: Not always. And in a case

1 I can give you an example of, there was cooling flow
2 to a turbine, and we don't care if there's high flow,
3 right? High flow is removing the heat. That's good.
4 We're concerned about low flow. But the requirement
5 said, if these sensors go out of range, trip the
6 turbine.

7 Now we have two pumps that feed the
8 system, the cooling to the system, and only one pump
9 usually runs. And then, you like to cycle the pumps.
10 But you start off the other, the second, the redundant
11 pump, before you close down the first pump, of course,
12 when you're changing the pumps. Well, as soon as you
13 kick down the first pump, what happened? The flow
14 over-ranged on all three sensors.

15 MEMBER BLEY: So, you have a trip.

16 MR. ARCHAMBO: You have a trip. The
17 system did exactly what it was told to do, but the
18 requirement was the problem.

19 MEMBER BLEY: So, I understand you write
20 those requirements for this new control system you're
21 getting. But, then, does the vendor of the control
22 system do the coding or do you do that?

23 MR. ARCHAMBO: Generally speaking, yes.

24 MEMBER BLEY: Okay. But you feed them
25 the --

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MR. ARCHAMBO: We feed them the
2 information.

3 MEMBER BLEY: -- plant requirements?

4 MR. ARCHAMBO: That's right.

5 MEMBER BLEY: Yes.

6 MR. ARCHAMBO: Now, generally, the design
7 engineer at the plant is not going to be developing if
8 it's complex application software. We will have a
9 vendor do that. We'll work with them, of course, so
10 we'll understand and --

11 MEMBER BLEY: So, when you submit the LAR,
12 that's for the system with your requirements already
13 met?

14 MR. ARCHAMBO: Yes, but, you know, it's
15 not always with the LAR. With the turbine controls,
16 that's not an LAR.

17 MEMBER BLEY: Understand that, yes.

18 MR. ARCHAMBO: But that's just the design
19 process.

20 So, design requirements for development,
21 of course, is a big-ticket item. We recognize that.
22 We haven't done a good job of it in the past. And
23 now, we have tools that should put us on the right
24 path with requirements development.

25 We also recognize there's design

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 attributes. We know that, even with the best
2 requirements development, with the best coders out
3 there, with the best application software, we can
4 never say that it's defect-free, 100 percent defect-
5 free. We know that. We recognize that.

6 But we can apply some design attributes to
7 either further minimize the likelihood of a common-
8 cause failure or mitigate the effects of a common-
9 cause failure. For example, if we have diagnostics to
10 look at the system alarming, perhaps we can fix an
11 issue before it becomes a common-cause failure. A lot
12 of the digital systems, when they fail, we can
13 determine what state it goes to. We can put it in a
14 failsafe state. So, there's a host of design
15 attributes that we can apply to the system on top of
16 the quality of the software to help minimize and
17 mitigate the effects of a software CCF. So, we do
18 apply those now, but we'll continue to refine those
19 and apply those in our systems.

20 Now the quality of the software design
21 process, again, that goes back to your question. When
22 it comes to the platforms, we have to rely on a couple
23 of things. We have to rely on, hey, was this platform
24 either pre-approved by the NRC or was it certified by
25 another body perhaps? Was it developed by an Appendix

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 B supplier for use in a safety-related application?
2 Those are things we have to look at to meet the
3 quality requirements for software at the platform
4 level.

5 Now, if you get down to the application
6 software level, that's where you're not going to have
7 those things. You're not going to have, chances are,
8 pre-approved application software. You're not going
9 to have a SIL certification on application software.
10 So, that's where we feel we need to spend most of our
11 time, on the application software development. That's
12 our intent.

13 And then, as the slide says, division of
14 responsibilities. Another thing that we recognize,
15 that if you have complex systems, it's easy to drop
16 things without a clear division of responsibilities.
17 And that goes back to your requirements and your
18 requirements traceability, who's responsible for
19 seeing those things all the way through. And these
20 are the areas that we found that, through root-cause
21 analysis and analysis of issues, we've discovered were
22 the primary cause of issues -- lack of requirements,
23 lack of division of responsibilities, things of that
24 nature.

25 So, that's at a high level of how we want

1 to attack the software common-cause failure issue. We
2 know we can never get to 100 percent assurance that
3 we're not going to have it. That's not the idea.
4 It's to get to reasonable assurance that we've
5 protected against software common-cause failure.

6 MR. HECHT: Can I ask a question about
7 your definition of platform software?

8 MR. ARCHAMBO: Sure.

9 MR. HECHT: Is that simply the operating
10 system or would that be, for example, a ladder logic
11 interpreter or an IEC -- what is it? -- 1163-type
12 language processor that would be on top of that? That
13 would be used, for example, in PLC programming or
14 something like that.

15 MR. ARCHAMBO: Yes, that would be included
16 in the platform software. Take a PLC, for instance,
17 an Allen-Bradley PLC. When I'm talking about
18 application, it's simply the ladder logic. That's
19 what we would develop, the ladder logic. Whatever
20 comes in that box beforehand, the operating system,
21 any other systems, that would be included in the
22 platform software.

23 Does that answer your question? It
24 doesn't look like it.

25 MR. HECHT: Yes, well, I know that in the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 aerospace industry, of course, ladder logic is not
2 used. I would imagine that in the IEC 61508 world it
3 might be. But have there been SIL 3 ladder logic
4 interpreters accepted or is that only the operating
5 systems?

6 MR. ARCHAMBO: My guess is there has. And
7 Matt's shaking his head, that that is the case, that
8 they have.

9 Now, when you go to 61508, when you talk
10 about platform software and things like that, you talk
11 about full variability languages. And when we talk
12 about application software, we're talking limited
13 variability language, as I see it. That's the
14 definitions you'll find in those standards.

15 So, yes, if that answers your question.

16 MEMBER MARCH-LEUBA: When I'm here
17 thinking about what you're saying, I tend to
18 oversimplify things. People get upset about it. What
19 I hear you say is we're going to get real diversity
20 and we're going to continue to do the same thing we've
21 been doing for design, only this time we promise to do
22 it right. That's what I hear.

23 MR. ARCHAMBO: Yes, well, you know, I like
24 it. You brought it down to my eighth grade level. I
25 appreciate that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 And the answer is yes. You know,
2 diversity is a double-edged sword. There's evidence
3 to suggest that having a diverse actuation system may
4 -- may -- actually be detrimental to your core design
5 or core damage frequency.

6 The solution to putting a DAS every time
7 you have a digital system we don't feel is the correct
8 way to go. There's applications for that. But what
9 we don't want to say is anytime you have a digital
10 system and a safety system, you have to have a backup,
11 either digital or analog system. It creates
12 complexity, and there's no real evidence that it adds
13 actually any security.

14 MEMBER MARCH-LEUBA: It all depends on
15 what that CCF frequency is. If it's 10 to the minus
16 8, of course, I think the system is high on complexity
17 and it's not good. If it's 10 to the minus 2, that
18 system helps you.

19 MR. ARCHAMBO: Sure.

20 MEMBER MARCH-LEUBA: When I'm driving a
21 car, I like to have brakes in the front and brakes in
22 the back just in case.

23 MR. ARCHAMBO: But, you know, in the newer
24 cars all the brakes are electronic.

25 MEMBER MARCH-LEUBA: Oh, yes. Don't get

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 me going with --

2 MR. ARCHAMBO: And your shifter is
3 electronic. There's no linkage anymore on that
4 shifter. It's electronic.

5 MEMBER MARCH-LEUBA: When you're pushing
6 the brake, you're just informing the computer that you
7 would like to slow down.

8 MR. ARCHAMBO: Exactly. Exactly. There's
9 no backup mechanical brake system unless your
10 emergency brake is part of that system.

11 MR. HECHT: I don't think that's totally
12 true. I think that there are hydraulic lines that
13 work in addition to the automatic braking systems.

14 MEMBER BALLINGER: Not in my car.

15 (Laughter.)

16 CHAIRMAN BROWN: I can guarantee you there
17 are hydraulic braking systems in my cars because
18 they're so old.

19 (Laughter.)

20 MEMBER BALLINGER: If it's 1945, of
21 course.

22 CHAIRMAN BROWN: No, it's hydraulic. It's
23 15 years old.

24 MEMBER BLEY: We're diverting wildly.

25 MEMBER MARCH-LEUBA: So, in your

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 experience, this diversity of the application
2 software, having to have two independently-developed
3 applications running, two channels one and two
4 channels the other, is that expensive; is that
5 difficult; is that prohibited?

6 MR. ARCHAMBO: You mean to have different,
7 say, manufacturers, different vendors?

8 MEMBER MARCH-LEUBA: Yes. You say that
9 application software is where all the problems happen.

10 MR. ARCHAMBO: Right.

11 MEMBER MARCH-LEUBA: Because the others
12 you can really test better. Is it that difficult to
13 have two different lines of code that -- I mean, it
14 doesn't need to be one is Russian and the other one is
15 Japanese. I mean, it doesn't have to be that bad.

16 MR. ARCHAMBO: Yes, the short answer is
17 yes. But, to get back to the point of the
18 requirements development, you're going to develop a
19 set of requirements. And if you have two separate
20 systems, let's say two separate design teams
21 developing the application software for two separate
22 trains, they're going to use the same requirements.
23 If the requirements are incorrect --

24 MEMBER MARCH-LEUBA: Oh, no, you will have
25 to develop requirements independently. Because the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 biggest problem is going to be you're going to forget
2 a requirement. That's the likeliest --

3 CHAIRMAN BROWN: That's why you write them
4 down.

5 (Laughter.)

6 MR. ARCHAMBO: But what happens with that,
7 you know, there's a lot of issues associated with
8 that, not just the expense of building it, but the
9 expense of maintaining it also. That's where the pain
10 comes in. And then, you have to ask yourself, is it
11 really necessary?

12 Now our evidence would suggest it's not.
13 We have not seen a significant amount of common-cause
14 failures. We've had digital systems in our plants for
15 many years, operating out there as we speak. We have
16 never experienced a common-cause failure. I'm not
17 going to say it could never happen, but, so far, it's
18 been significantly unlikely.

19 MEMBER MARCH-LEUBA: I find that hard to
20 believe because I told you already I had that one
21 analog common-cause failure. This piece of equipment
22 crashes; the system you're running crashes two or
23 three times a day.

24 MR. ARCHAMBO: Yes, you look at that
25 system, though, and that's a system where they're

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 beaming down updates to you periodically and things
2 like that.

3 MEMBER MARCH-LEUBA: Yes.

4 MR. ARCHAMBO: That's not what we're
5 talking about.

6 MEMBER MARCH-LEUBA: What I was going to
7 say is that, even though it crashes two or three times
8 a day, I can still use it and it still works and it's
9 useful, I guess. So, it's not always the end of the
10 world.

11 CHAIRMAN BROWN: Well, I hate to tell you,
12 but my common cause -- I have no failures of this.

13 (Laughter.)

14 It works all the time. I make phone calls
15 and I can text. It's only 18 years old and I can get
16 new batteries for it. So, I continue to do that. And
17 it never crashes. And I don't have to download
18 software, and it makes phone calls. And I can hear
19 the people on the other end. They're not going
20 sporadically in and out, except if I'm talking to
21 somebody that's got one of those pieces of garbage.
22 I'm just having fun.

23 All right, go ahead.

24 MR. ARCHAMBO: Anything else?

25 CHAIRMAN BROWN: You've got another slide.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Did you want to talk to that, or is somebody else
2 going to do that?

3 MR. VAUGHN: It's a wrap-up slide.

4 MR. ARCHAMBO: I think somebody else.

5 MR. HERB: I'd like to make a point.

6 CHAIRMAN BROWN: Go ahead.

7 MR. HERB: Okay. I think that the member,
8 Mr. Bley -- "Bley," is that how you say your name?

9 MEMBER BLEY: Bley.

10 MR. HERB: Bley. Mr. Bley asked what was
11 our problem with BTP 7-19, and I don't think anybody
12 really addressed that.

13 MEMBER BLEY: I think you're right.

14 MR. HERB: First of all, we do like
15 BTP 7-19, but what we like about it was the additional
16 freedom we got to address a common-cause failure.
17 Because I think, as you can see, we always get bogged
18 down into software, the digitalness, and how that's
19 such an unknown. Nobody can eliminate all the issues
20 with software. But what we bypass is that, with the
21 new digital systems, they're highly capable systems.
22 We would like to install them. Those design
23 attributes can be programmed into them.

24 And so, the thought that you have to
25 restart your phone periodically during the day, but

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 that's a value proposition; that's a risk proposition.
2 The chances of you having to restart your phone right
3 before you have to call somebody, a 9-1-1, that's
4 probably pretty low.

5 And so, it's the same thing here. We're
6 not eliminating CCFs. We're just suggesting that
7 sometimes you can live with them and you can cope with
8 them. The system can make you aware that a failure is
9 happening in enough time that you can take correct,
10 proper manual actions without having to rely on a
11 diverse actuation system in time to either put the
12 plant in a safe condition before your design basis
13 event that's been designed, that that system's been
14 designed to address long before that happens.

15 And so, the probabilities start to get
16 minuscule that that common-cause failure is going to
17 happen at exactly the time that the demand is
18 required. Because these systems are not like the old
19 systems; they get tested on a quarterly basis or a
20 semi-annual basis. And you have to like live with
21 that possibility that they have failed. Between that
22 last time you tested and the next time you tested,
23 there may be a design basis event that happens in
24 between.

25 These systems will let you know

1 immediately when they fail. You can address that
2 immediately. And we just like to have credit for
3 that, rather than to say, you know what, the default
4 is a diverse backup system.

5 And so, in some cases we may have to have
6 a diverse backup system, but we want the option to be
7 able to take the full spectrum of response. And I
8 think that we've always felt that BTP comes with a
9 presumption that you will have a diverse backup
10 system. And it doesn't really give full credit to
11 those other aspects.

12 MEMBER BLEY: Do you feel that way now?
13 The way I read the current version, you have --

14 MR. HERB: No, I think it's much better.

15 MEMBER BLEY: -- a way out.

16 MR. HERB: But we haven't seen it since
17 August.

18 CHAIRMAN BROWN: Well, since they put in
19 the defensive.

20 MEMBER BLEY: Oh, you haven't seen it?
21 Okay.

22 MR. HERB: We've seen in general, yes.

23 MEMBER BLEY: Okay.

24 MR. HERB: We have seen it.

25 MEMBER BLEY: But you haven't actually got

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 a copy of the document we have?

2 MR. HERB: And again, we still can't look
3 into the minds of the inspector to see what weight
4 that they provide each of those.

5 MEMBER BLEY: You aren't ever going to get
6 rid of that problem.

7 (Laughter.)

8 MR. HERB: We're never going to do that.

9 CHAIRMAN BROWN: You must have been
10 listening to the conversation we had earlier in the
11 meeting about why do we worry about CCF. You were
12 echoing my comments.

13 MR. HERB: And I agree with you instead
14 of --

15 CHAIRMAN BROWN: I figured as much.

16 MR. HERB: I think that the NRC agrees
17 with --

18 CHAIRMAN BROWN: I didn't bring up the
19 point the other time that all of the systems we've
20 gotten in the design systems and even -- are you the
21 Common Q guy? That's what I thought. I thought I
22 remembered that discussion.

23 All of the systems that have been put in
24 have been built with significant self-diagnostics,
25 where they're continuously running. Every few minutes

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 they're probably running through some almost complete
2 testing of all the responses, with inputs coming in
3 and seeing that they generate the proper output each
4 time. And if they don't, then they bring something
5 in.

6 Personally, I believe that is a
7 significant benefit that we have not had in any of the
8 instrumentation control protection systems or anywhere
9 else. We used to have weekly setpoint and calibration
10 checks because we knew the analog stuff would drift,
11 and it did.

12 MEMBER BLEY: And we'd trip things
13 accidentally doing these tasks.

14 CHAIRMAN BROWN: Accidentally because of
15 that. But, once we implemented -- I had terrible
16 problems with intermediate-range and source-range
17 nuclear instrumentation always going off the
18 reservation. When we developed the microprocessor-
19 based instrumentation for the intermediate-range and
20 source-range, which we applied in probably two dozen
21 submarines before I retired, you could count the
22 number of incident reports on those systems on no
23 hands. It just tested itself continuously. If we did
24 have a problem, it was a detector problem, not a
25 processing problem.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 I'm not trying to counteract. I'm just
2 saying the self-diagnostics are a huge, huge benefit
3 relative to monitoring the safety, the health of the
4 system. And I personally think that has been
5 inadequately utilized in terms of getting through this
6 thing.

7 I believe in some diversity. It's a
8 matter of how and where it's applied, where you have
9 to have it because your other defensive measures don't
10 cover you in that area, and determining where those
11 are.

12 So, I just love these two systems, in
13 spite of the fact that I hate software and I hate
14 microprocessors, but they work awfully well and help
15 us out.

16 And these plants are really very simple
17 compared to the stuff I had to deal with when you're
18 talking about submarines and aircraft carriers. You
19 all, your brains would explode if you had seen what we
20 did with the capability of those systems. It is truly
21 phenomenal in terms of operational capability, and
22 safe because it tests every one of those features all
23 the time.

24 Sometimes it might take 5 or 10 minutes to
25 test every part because you're doing it at the end of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 every sample period, which might be 50 to 100
2 milliseconds, but every sample time has an allocated
3 time for self-test. And you run through and you just
4 pick up where you left off and keep testing until you
5 finish the whole package, and then, start over again.

6 And from what I gathered, at least the two
7 that I've seen -- I think Common Q kind of does that
8 also for the most part, and there's one other one that
9 does that also. I can't remember which one it was
10 that I looked at.

11 MEMBER BLEY: For systems that aren't
12 working, that's great. For having things running
13 operationally, it's great. For these things we worry
14 about that are extremely rare, it helps, but it's not
15 enough.

16 I'd like to direct a question to staff, if
17 I can.

18 CHAIRMAN BROWN: They're gone, except for
19 Eric. Oh, no, is Deanna here?

20 MEMBER BLEY: The discussion about
21 requirements is interesting and meshes with things
22 I've seen in the past. And the BTP doesn't really
23 draw any separation between applicant-developed
24 requirements and any of the other software involved.
25 Do you do anything special to look at those

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 requirements? And can you even see them from the
2 submittals? Do you see those requirements? Is there
3 anything in the process that shines a light there more
4 than on anything else? If you can comment on that,
5 I'd appreciate it.

6 CHAIRMAN BROWN: You're talking to Deanna?

7 MS. ZHANG: So, in general, when we do a
8 platform-level review of an I&C platform, we don't
9 typically review to address CCF because a lot of times
10 that's not addressed at the platform level, but
11 addressed at the system architecture level, which
12 would be application-specific.

13 So, when you look at the BTP, what we
14 envision is mostly this is talking about the
15 application, not the individual platforms we may see,
16 such as the Common Q or TXS or Tricon type of
17 platforms.

18 MEMBER BLEY: I'm sorry, don't leave.

19 MS. ZHANG: Unless Ross wants to talk a
20 little bit more about some of the other platforms
21 we've reviewed --

22 MEMBER BLEY: Okay. My question was
23 really aimed at the requirements.

24 MS. ZHANG: Right.

25 MEMBER BLEY: But I appreciate the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 separation between the generic platform acceptance and
2 the specific applications coming in for a particular
3 plant.

4 MS. ZHANG: Right.

5 MS. ALVARADO: This is Rossnyev Alvarado,
6 I&C Branch.

7 BTP 7-14 includes guidance for the staff
8 to review how the licensees or the applicants provide
9 the requirements specification. And it's one of the
10 IEEE standards that we have endorsed. So, it is
11 required.

12 We don't look at like details like
13 requirement by requirement, but we do spot-check and
14 track requirements to figure out how they have been
15 implemented. And we do that for both platform -- like
16 when you were asking about whether it's the software
17 that comes with the component, that's right. Well,
18 operating system is no longer used, the term. Okay.
19 And we do, too, for the application.

20 The difference is that, when it comes in
21 the platform, it's usually the vendors -- in this
22 case, Westinghouse, GE, you name it, Rolls Royce.
23 When it comes with a license amendment, it is coming
24 through the applicant or the licensee. So, a lot of
25 the responsibility shifts to the licensee to do that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 review, but we still do check.

2 And one of the requirements is that they
3 need to meet the functional requirements
4 specification. We do require that. So, we do look at
5 it. It's just not that we're going to do line-by-line
6 code check. We just need to look at it.

7 CHAIRMAN BROWN: There's no way you can do
8 a line-by-line code check.

9 MS. ALVARADO: No.

10 MEMBER BLEY: No, there isn't, but you can
11 do something with the requirements.

12 CHAIRMAN BROWN: Well, we used to do that.

13 MEMBER BLEY: We've got your statement on
14 the record. That's good. If one of you can show me
15 where in this document you refer to the requirements,
16 I would appreciate it, because you said it's in there.

17 MS. ALVARADO: This is not the document to
18 address requirements. This is a document on how --

19 MEMBER BLEY: You told me -- I'm sorry --

20 MS. ALVARADO: BTP 7-19 is a document to
21 address --

22 MEMBER BLEY: I thought earlier -- and
23 I'll check the record -- I thought you said BTP 7-19
24 included --

25 MS. ALVARADO: 7-14.

1 MEMBER BLEY: 7-14?

2 MS. ALVARADO: 7-14.

3 MEMBER BLEY: Thank you.

4 MS. ALVARADO: BTP 7-14 is the process to
5 review, that we follow to review all of the software-
6 related development process.

7 CHAIRMAN BROWN: Thank you.

8 MS. ALVARADO: Sure.

9 MEMBER MARCH-LEUBA: No, don't leave.
10 Don't leave. Don't leave.

11 CHAIRMAN BROWN: Come back.

12 MEMBER MARCH-LEUBA: Well, it's not a
13 question. It's more a statement.

14 I have a problem with the PRA all the time
15 about completeness, and it's a great methodology. The
16 problem is, how do you know you accounted for
17 everything? And when you review the functional
18 requirements, how do you account, how do you review
19 that they accounted for everything that they needed to
20 account for?

21 MS. ALVARADO: We don't.

22 MEMBER MARCH-LEUBA: Because it's very
23 easy to have requirements, implement software, and
24 test the requirements are satisfied. Almost everybody
25 knows how to do that. The problem is, oh, I forgot

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 that when this thing always happened, that one goes
2 down, you're supposed to do B.

3 MS. ALVARADO: We don't, and that's not
4 part of what we are doing. We're trying to do like a
5 spot-check, like I'm saying, like peek at certain
6 requirements to see that they follow their process.
7 And if we determine that they didn't follow the
8 process, then in that case we will ask them to address
9 that, both the vendor and the licensee.

10 MEMBER MARCH-LEUBA: You're doing the easy
11 job. I mean, it's tedious and long, but it's the
12 difficult one is thinking about what is missing. And
13 that's the problem with what you are proposing. It
14 is, how do we know?

15 MS. ALVARADO: Well, but I mean it's --

16 MR. HERB: If I could answer that question
17 for the industry, because we provide that requirements
18 to the NRC for their review and acceptance for a part
19 of a LAR.

20 Those requirements are informed by hazards
21 analyses. And so, we do a hazards analysis and we
22 look at the baseline function requirements of our
23 current licensing basis and our current systems, and
24 we look at the hazards associated with a digital
25 system, applying those. Did we get the negative

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 requirements and the missing requirements from that by
2 addressing -- there's several methods that we can use,
3 STPA methodology, HAZCADs, fault tree analysis. And
4 we look for the missing requirements.

5 And so, when we submit a license amendment
6 to install a digital protection system, it includes a
7 full set of requirements along with that that's
8 available for the NRC to review.

9 MEMBER MARCH-LEUBA: Let me give you an
10 example we just heard before. Whenever the signals
11 for that turbine control system go out of the scale,
12 you scram. Okay. The requirements you have, if it
13 goes up, it's good. So, you should have two different
14 requirements instead of only one. There was one
15 missing.

16 MR. HERB: That's right. That's
17 absolutely right. But you have to remember, turbine
18 control systems are not protection systems.
19 Protection systems are much simpler. And so, they're,
20 generally, if a signal goes high, then you trip. If
21 the signal goes low, you trip. There are some more
22 complex ones that maybe have a curve that is developed
23 based on your operating -- but they're much simpler
24 than turbine control systems.

25 MEMBER MARCH-LEUBA: That is the easy

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 part.

2 MR. HERB: Yes.

3 MEMBER MARCH-LEUBA: Again, that's the
4 easy part. That you're going to do. I'll stipulate
5 that that you do right. The problem is handling
6 exceptions. What happens if you have a division by
7 seal? What happens if your variable gets stuck at 2.7
8 volts and doesn't move anymore?

9 MS. ALVARADO: I just want to add
10 something, that maybe we're focusing a lot into
11 requirements specification. It is important, your
12 software requirements specification, but you also need
13 to keep in mind that these processes go through a
14 whole life cycle. And it's not just like I'm writing
15 the requirements, I program, and I'm done. They do go
16 through a whole set of tests at different levels, at
17 different stages of development.

18 And one example, coming back to what
19 you're saying, it actually happened with Diablo
20 Canyon. When we got the application for the Diablo
21 Canyon safety system, the reactor protection system,
22 one of the vendors -- they were using two vendors, two
23 different platforms for diversity -- did not fully
24 understand, because he was the first time working with
25 the nuclear industry, how to implement the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 requirements for the alarms that were launched. Okay?
2 And they didn't find that out until we started doing
3 design testing. That required a whole lot of like
4 rework and redesign and retests for the system.

5 But that's not something that is now my
6 responsibility as the staff to say, oh, this
7 requirement is good or not because, like Ray said,
8 they are the ones who know what they want the system
9 to do, right? So, that's why BTP 7-14 -- BTP 7-14,
10 not 19 -- has all these different steps or plans and
11 procedures and things that you have to do that are
12 endorsed by the NRC following industry standards, in
13 which they have to, you know, not just create the
14 requirements, but they have all these different steps
15 that they need to follow before they can go and plug
16 it in the plan.

17 CHAIRMAN BROWN: We've overrun, but that's
18 okay. We'll make it here.

19 Do you all have anything else to address?

20 (No response.)

21 I want to go ahead and move on to get EPRI
22 up here.

23 Okay. Thank you all very much. Thank
24 you, Ray, by the way.

25 MR. HERB: You agree with me.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: We will continue to
2 receive the slings and arrows of outrageous fortune.

3 (Laughter.)

4 You're on.

5 MR. GIBSON: Well, thanks for having me.

6 So, today I'm going to give you EPRI's
7 perspective on digital I&C --

8 CHAIRMAN BROWN: You've got to stay right
9 up there. You can't lean back.

10 MR. GIBSON: Okay. I'm going to give you
11 some EPRI perspective on digital I&C reliability and
12 software CCFs, and some of the research that we've
13 been doing really over the past 10 years. Now some of
14 this you have seen already. So, it will be a
15 refresher for you, but I'll give it maybe a little
16 different context.

17 Let's see here. There we go.

18 So, our prior research has really looked
19 pretty hard at some OE and some other reliability
20 measures over the years. Now this is a list. In the
21 interest of time, I won't read this to you.

22 CHAIRMAN BROWN: Tell people what "OE" is.

23 MR. GIBSON: Operational Experience.

24 CHAIRMAN BROWN: I know what it is. It's
25 just I would just ask you to minimize the acronyms in

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 the discussion, if you can. Okay?

2 MR. GIBSON: That will be fine.

3 MEMBER BLEY: I'll remind you when we do
4 the letter.

5 (Laughter.)

6 CHAIRMAN BROWN: I hate to remind you, but
7 I like to spell things out, and then, I got beat on to
8 put the acronyms in everywhere.

9 So, this is an internal disagreement here
10 totally unrelated to your subject.

11 MEMBER BLEY: Go ahead.

12 CHAIRMAN BROWN: So, I'll turn off my mic.

13 MR. GIBSON: So, let's look back just for
14 the folks on the phone, because I don't think I
15 actually got introduced. But I'm Matt Gibson with
16 EPRI, Technical Executive in the I&C Program. So, my
17 responsibilities are doing research on digital I&C,
18 cybersecurity, and human factors.

19 On the slide here you see a list of the
20 products that we've produced over the past 10 years
21 that are relevant to this discussion related to I&C
22 reliability. We'll just give you a history of these.

23 The one you probably have seen before,
24 because I know it's been presented here, is some OE
25 work we did on U.S. and Korean data. We were able to

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 get that data through the utilities primarily and some
2 from INPO. And we looked at those events, looking for
3 your software versus hardware, versus safety-related
4 versus non-safety related. And I'll just summarize
5 these, but you can see the software common-cause
6 failures that we detected in that data was just one
7 out of the 49 events; zero in the 19 Korean events.

8 If you look down for the non-safety,
9 because this is a good juxtaposition that we need to
10 think about, you'll see that your common-cause
11 failures rose a little bit. Of course, we had a lot
12 more events to work with; Korea less events of 3
13 percent.

14 What's probably useful to see here is the
15 non-software common-cause failures were significantly
16 higher than the software common-cause failures in both
17 the Korean data and U.S. data, and both for safety and
18 non-safety. And that really lines up with what you
19 guys have been talking about all day: why are we
20 talking about software CCFs and what's the context?

21 So, the conclusions that we made from this
22 was that your software CCF is something you have to
23 think about, that's true; something you have to deal
24 with; that's true. But is it any more problematic
25 than other CCFS?

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 The methods used by the folks during this
2 time period, which really goes back a pretty long
3 ways, were -- especially for 1E -- were effective in
4 limiting those CCFs. And when we looked at these, we
5 didn't see platform-level CCFs, either, software CCFs.
6 The one mentioned here, of course, people can argue
7 what the definition of a platform is, and we can do
8 that in a few minutes when we get onto questions, but
9 more at the application level.

10 MEMBER REMPE: I was waiting for you to
11 ask your question again. Are you going to?

12 MR. HECHT: It might be better if you ask
13 it, Joy.

14 (Laughter.)

15 MEMBER REMPE: Oh, okay.

16 So, you heard earlier he was asking, is
17 EPRI willing to share the underlying data with the
18 NRC, with this new research project, the two new
19 research projects that are started?

20 And then, I have a question for the staff
21 that I'm curious about.

22 MR. GIBSON: That's a pretty long
23 question. The short answer is no. All right. The
24 long answer is that getting meaningful reliability
25 data for stuff is a closely-guarded IP secret of these

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 folks, especially accurate information, because they
2 share that information with the folks they have
3 business relationships with or they have other
4 relationships with. But we were able to get this data
5 through a series of NDAs, and that sort of thing, that
6 preclude us from actually giving raw data out.

7 MEMBER REMPE: That's a good enough
8 answer.

9 Then, I would like to ask the staff
10 person, weren't you the person who said you would come
11 up and talk a little bit more about the two new
12 projects that you're starting? Because I was looking
13 up the -- we had a discussion with the staff in the
14 beginning of November, and they didn't really discuss
15 any new projects that are coming up on CCF. In fact,
16 the user need was like 2015. So, could you talk a
17 little bit about what it is you're doing with those
18 two new projects more? And could you let us know, are
19 they feasibility studies, or what are they?

20 MR. JENKINS: This is Ronaldo Jenkins.
21 I'm the Chief of the Instrumentation, Controls, and
22 Electrical Engineering Branch.

23 Paul Rebstock, who spoke earlier, he's not
24 directly involved with the projects you're referring
25 to.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 The two risk-informed projects that we
2 just started in the Office of Research, one is on how
3 to enable the staff to use risk-informed
4 methodologies. So, that's one. One of the projects
5 is focused on that.

6 The other project, which is much more
7 longer term, is to look at software reliability. And,
8 of course, there's been a lot of questions about
9 software reliability and what exactly does it mean.
10 One of the problems is it's a moving target. As you
11 know, the life cycle for software in terms of it being
12 a product changes fairly quickly over time. So, if
13 you're studying the reliability of a given product in
14 the sixties, you're dealing with a different product
15 than you are currently now.

16 So, our focus is on the nuclear power
17 plant technology that, presumably, would be put into
18 service with the digital upgrades. So, we're trying
19 to estimate with that second project a reliability
20 number. And it is going to be difficult; there's no
21 question about it.

22 We also took action to look at the EPRI
23 data, the operating experience data. We had a group
24 of folks to look at that, and Matt Gibson was kind
25 enough to help us to look at that data.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 One of the problems you have is, when
2 you're looking at a given report, it's summary-level
3 information, and it doesn't get to the root cause
4 associated with that failure. And that's really what
5 you need. In order to compare apples to apples, you
6 need to know you're dealing with the same apple or a
7 version of it, not a totally different root cause
8 associated with it.

9 Does that help?

10 MEMBER REMPE: That helps a bit.

11 MR. JENKINS: Okay.

12 MEMBER REMPE: We may have some follow-on
13 questions.

14 MR. JENKINS: Okay.

15 MEMBER REMPE: But I'm glad this topic
16 came up today. So, thank you.

17 MR. HECHT: I just would urge that, before
18 precious resources be spent in investigating that
19 issue, that you look at past related studies. I
20 mentioned ORNL. There's been others done by
21 Brookhaven.

22 MR. JENKINS: Right.

23 MR. HECHT: I'm sure that there are
24 probably others in the archives. If you don't have
25 data, if you don't have enough data, and if you don't

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 have sufficient quality data --

2 MR. JENKINS: Right.

3 MR. HECHT: -- you probably will end up in
4 the same place as those other forgotten reports, and
5 that would be a shame.

6 MR. JENKINS: Right. You're exactly
7 right. The problem is getting data that will allow
8 you to draw some statistical inferences associated
9 with how is the reliability that you are trying to
10 estimate, whether or not that data is sufficient or
11 not. And so, that is always a problem in any type of
12 research that you're going to do.

13 MEMBER REMPE: Is this a user need that's
14 going forward or is this a feasibility study? What is
15 this now?

16 MR. JENKINS: This is a user need. The
17 technical lead for this project is in the Division of
18 Risk Analysis. So, it's the same folks who are doing
19 PRA. They're taking the lead on the project, but
20 we're working with them from a digital I&C
21 perspective.

22 MEMBER REMPE: Okay. So, it's an existing
23 one with a new twist, is what it is? It's not a new
24 one?

25 MR. JENKINS: No, it's a new project.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MEMBER REMPE: It is a new one? Okay.

2 MR. JENKINS: Yes.

3 MEMBER REMPE: Thank you.

4 MR. WATERS: This is Mike Waters.

5 I just want to clarify for Ronaldo that
6 the goal is to look at existing methods, because we
7 recognize industry are making reliability claims.
8 They're going to continue to do so. We recognize one
9 day they may want to start assigning numbers in their
10 PRAs when we now modify to digital.

11 So, this research is to look at the state-
12 of-the-art methodologies, what are limitations, what
13 makes sense for us to independently evaluate
14 reliability claims that are being made to us. So, I
15 just want to clarify we're not developing a new
16 reliability method or a new way to assess or quantify
17 reliability.

18 MR. JENKINS: Yes, that's correct. It's
19 not to develop a new methodology.

20 MEMBER REMPE: Thank you.

21 MR. HECHT: The methodology is not the
22 issue. The parameters are.

23 MEMBER BLEY: Hey, Matt, just a little
24 favor?

25 MR. GIBSON: Yes.

1 MEMBER BLEY: We got you to pull the mic
2 up real close, but it's so close that it makes noise
3 when you breathe. So, if you could push it off just
4 a little bit? There you go.

5 (Laughter.)

6 MR. GIBSON: Well, we'll calibrate. How
7 about that?

8 MEMBER BLEY: Thank you.

9 MR. GIBSON: Okay. So, I can use my
10 outside voice, too, if I need to.

11 MEMBER BLEY: No, it's got to go on the
12 record, so we need it through the system.

13 Christina, Matt's second slide had a list
14 of EPRI reports. I know we've seen some of them. Can
15 you see which ones we can actually get and take a look
16 at? I don't want to do this now. Don't address it
17 now. Just talk with them and see what we can get.

18 MS. ANTONESCU: Okay. Sure.

19 MEMBER BLEY: I just took a look. They're
20 not publicly available, or at least the first couple
21 I looked at were not.

22 MR. GIBSON: You have all of these.

23 MEMBER BLEY: The staff does?

24 MR. GIBSON: Yes.

25 MEMBER BLEY: You've given them all to the

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 staff?

2 MR. GIBSON: Yes.

3 MEMBER BLEY: So, we can get them from the
4 staff. Okay. Thank you.

5 MR. GIBSON: You're welcome.

6 So, let's pick up with some research we
7 did on the actual sensitivity of I&C reliability. So,
8 in this particular research, we did really plug in
9 digitalizing into the PRAs, looked at 18 initiating
10 events, and experimented with sensitivity analysis.
11 You know, having the system fail, always failing, and
12 also never failing.

13 And what you see from that is the actual
14 sensitivity that even protection systems have to
15 overall plant safety. Because there's enough
16 functional reliability in a plant that, when you do
17 the probabilities and such like that, that I&C becomes
18 less of an actual risk.

19 So, if an initiating event has a high
20 frequency, if you just do the math, it will end up,
21 you know, the reliability of the digital system will
22 have more of an impact on the total risk frequencies
23 or the consequence frequencies. If the initiating
24 events have very long periods or low frequencies, then
25 the reliability the digital system will have much less

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 of an impact.

2 Now, when Warren and such were up here,
3 you guys were talking about failure of 10 to the minus
4 4 for reliability and such, and somebody used the
5 probability failure on demand. Well, actually, in
6 61508 and ISA 84, probability of failure on demand
7 takes the reliability of the system and mixes it with
8 normal reliability math with the frequency of the
9 event. Because, remember, it's probability of failure
10 on demand, not probability of failure. The system
11 may, in fact, fail once in a while, but if it doesn't
12 fail on demand, which is when the initiating event is
13 occurring -- so, those numbers are actually pretty
14 high. I noticed you had an event initiation 10 to the
15 minus 4 that 10 to the minus 8 would be the
16 probability on demand. So, you would actually result
17 in a consequence because that has to have coincident
18 failure of the system along with the initiating event.

19 Anyway, these sensitivity studies also
20 tell us a little bit about the impact of adding
21 diverse systems, because there's probably been a
22 little bit of too much of a focus on a specific
23 failure mode. And I think some of the industry folks
24 earlier talked about that.

25 If you truly are risk-informed and you use

1 risk tools to figure out what this is, you can insert
2 an actual brand-new system that can itself trip the
3 plant. Potentially, depending on how it's done, your
4 total core damage frequency can go up. And you might
5 have been attempting to address a specific failure
6 mode, but if you don't evaluate that change you made
7 to the system against the total risk, you don't really
8 know if you're making the risk more or less. And I
9 think that really brings the question of, you know,
10 exactly how much are we going to use risk-informed and
11 other tools to inform this process. I think that's a
12 question on the table from measuring total system
13 reliability.

14 CHAIRMAN BROWN: Go back to your previous
15 slide. You said a lot of other things, but you didn't
16 -- I was looking at your chart, and it says, "Event
17 and sensitivity analysis concluded that a diverse
18 platform was not more effective in mitigating
19 postulated SCCF than functional diversity or manual
20 operator action." And yet, I had no way to conclude
21 that from looking at your little chart. I presume --

22 MR. GIBSON: No, this is an all-day
23 discussion actually because we have to go at it
24 through the data. But here's --

25 CHAIRMAN BROWN: No, no. No, no, no. I'm

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 not going to track through the data. Does this table
2 somehow communicate -- I mean, I see all these
3 accidents, events with CDFs, but how do they --

4 MR. GIBSON: If you look, it's --

5 CHAIRMAN BROWN: Let me finish.

6 MR. GIBSON: Okay.

7 CHAIRMAN BROWN: How do these relate to
8 conclude that a diverse platform was not more
9 effective in mitigating a postulated SCCF?

10 MR. GIBSON: So, if you look in the -- I
11 printed these rather small -- but if you look at the
12 righthand column, there's going to be a discussion
13 about doing these probabilities by the insertion of
14 diversity, which were just added onto the fault trees,
15 right? You added a diverse system which would --

16 CHAIRMAN BROWN: Is that the little box at
17 the lower righthand corner?

18 MR. GIBSON: Yes, the little box at the
19 right that takes all of the -- you see how the lines
20 go vertically?

21 CHAIRMAN BROWN: Yes.

22 MR. GIBSON: Those are the top and the
23 bottom, and you'll see some of them are the six
24 sensitivities that were done with and without
25 diversity.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: So, what does that say?

2 MR. GIBSON: It says that your diversity,
3 when you add it, controls for a specific failure mode,
4 but doesn't necessarily reduce the risk because it
5 itself adds risk. You can't add a diverse system
6 without adding risk. So, the risk you add has to be
7 less than the risk you mitigate.

8 MEMBER MARCH-LEUBA: What risk are you
9 adding?

10 MR. GIBSON: The risk you're trying to
11 mitigate is a software common-cause failure.

12 MEMBER MARCH-LEUBA: And now, I have a
13 second system, a diverse system, and what risk am I
14 adding?

15 MR. GIBSON: Your risk is you're adding a
16 whole other system which in itself has reliability --

17 MEMBER DIMITRIJEVIC: But it's a backup
18 for the first system.

19 MR. GIBSON: Yes, it can itself initiate
20 a plant event, initiate itself, because it can trigger
21 the plant, right? If it's a backup reactor protection
22 system, it itself can fail and trip the plant,
23 initiating an event.

24 MEMBER MARCH-LEUBA: I find that hard to
25 believe.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MEMBER DIMITRIJEVIC: It doesn't make
2 sense.

3 MR. GIBSON: Why?

4 MEMBER DIMITRIJEVIC: You're adding a
5 redundant system. So, you're making the system more
6 reliable. Now how important does --

7 MR. GIBSON: You're not making it more
8 reliable. You're not making it more. You're
9 controlling for one failure mode.

10 MEMBER DIMITRIJEVIC: What do you mean by
11 "failure mode"?

12 MR. GIBSON: See, the reliability of --

13 MEMBER DIMITRIJEVIC: It's a software
14 failure.

15 MR. GIBSON: We'll get to this in a
16 second.

17 If you plug systems into a fault tree, and
18 you assign probabilities to them, okay, the most
19 reliable thing is where you have a system and it never
20 fails. But what really happens is now you have these
21 different components and systems coming up through
22 your fault tree with different probabilities. Now if
23 you assume a CCF, right, if you assume a CCF, and you
24 say the redundancies will appear on the fault tree --
25 if you say, okay, instead of giving that equipment

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 reliability figures like 10 to the minus something,
2 but I'll say that I'm going to accept a software
3 common-cause failure and force it to fail on the fault
4 tree. You will get a probability and you say, okay,
5 that's bad because it will always go to an event. I
6 need to add something in line with that on the fault
7 tree that, if I assume that CCF, then it will prevent
8 me from taking a consequence. Well, that new thing
9 you put on there in itself can fail, and it has a
10 reliability metric all by itself. So, while you've
11 controlled for one fault, you've actually added the
12 potential of other faults in the fault tree.

13 MEMBER DIMITRIJEVIC: Okay, but we added
14 to mitigate these faults. So, it may only add
15 spurious operation or initiating event, but that's
16 usually very low risk. So, therefore, by preventing
17 your common-cause failure, it actually helps you.
18 It's an "and" gate, not an "or" gate. You're
19 discussing it like it's an "or" gate, but it's
20 actually an "and" gate with your software failure.
21 And therefore, it helps you with that. You need to
22 fail them both in order to fail.

23 MR. GIBSON: You need to fail them both to
24 reach the event that you're protecting against --

25 MEMBER DIMITRIJEVIC: Yes.

1 MR. GIBSON: -- for the CCF. But that
2 thing you added, all right, has to be able to, well --

3 MEMBER BLEY: Independently actuate a trip
4 as well.

5 MR. GIBSON: Yes, it's independent, right?
6 So, it's not an "or" (sic) with the thing, "and" --
7 this is "or". So, you'll have to be able to trip the
8 plant if the conditions, if the primary system doesn't
9 trip the plant.

10 MEMBER MARCH-LEUBA: Yes, but you're
11 telling me that adding a protection system to the
12 reactor is really, really bad.

13 MR. GIBSON: Really what?

14 MEMBER MARCH-LEUBA: Really bad.

15 MR. GIBSON: It's not really bad, but it
16 might not be doing what you think it's doing. That's
17 all we're saying.

18 CHAIRMAN BROWN: He's just simply saying
19 the backup system could initiate a trip independent of
20 whether the other system --

21 MEMBER DIMITRIJEVIC: But that's --

22 CHAIRMAN BROWN: -- independent of an
23 event occurring. It can trip the plant regardless --

24 MEMBER MARCH-LEUBA: Everybody keeps
25 talking risk-informed and they forget about the risk.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 I mean, you always keep talking
2 probabilities/frequencies instead of talking
3 consequence. The consequence of a scam is nothing --

4 MR. GIBSON: Consequence is not risk.
5 Risk is consequence and probability.

6 MEMBER MARCH-LEUBA: Right.

7 MR. GIBSON: So, when you change the
8 probability that you could potentially have a bad
9 outcome broadly, then --

10 MEMBER MARCH-LEUBA: It's late; I'm not
11 buying.

12 MR. GIBSON: That's okay.

13 CHAIRMAN BROWN: I can't believe this; I
14 think I'm even agreeing with Vesna and Jose, in that
15 the backup was added. You've got a system to take
16 care of a particular event. That's what it's designed
17 to do, and it's a software -- because we're going to
18 terminate this discussion after I finish.

19 (Laughter.)

20 Because we've got to get on with it.

21 You've got a system that's in there that's
22 supposed to respond to a thing, but it may have a
23 common-cause failure --

24 MR. GIBSON: That's right.

25 CHAIRMAN BROWN: -- of some type that

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 prevents it. So, you add another system, diverse,
2 that will also perform the same function. Okay.
3 There's two things that can happen. One, in the
4 absence of an event, the other system can cause the
5 plant to trip on its own.

6 MR. GIBSON: That's true.

7 CHAIRMAN BROWN: It can fail and it can
8 cause a problem. Okay? Now you don't have an event
9 occurring. All you've done is put the plant in a safe
10 condition when you do that, theoretically.

11 MR. GIBSON: Theoretically.

12 CHAIRMAN BROWN: So, that's a reliability
13 issue. What you're preventing is the failure of
14 either one of those two systems to not operate when
15 you actually have an event that could damage the
16 plant. And so, I think that's the way I view it. So,
17 the argument that you're increasing the probability of
18 something, to me, doesn't --

19 MEMBER MARCH-LEUBA: Would you allow 20
20 seconds?

21 CHAIRMAN BROWN: No, but go ahead. You're
22 going to take it anyway.

23 MEMBER MARCH-LEUBA: I'm going to talk
24 anyway.

25 (Laughter.)

1 By adding a second scram system, at most
2 you double the probability of a full spurious
3 actuation. Factor of two. Factor of two, as my
4 colleagues tell me, is nothing. I mean, you need 10
5 to the minus 4. Two is non-existent. So, I mean, you
6 just doubled the probability of having a spurious
7 actuation.

8 But, on the common cause, you went from 10
9 to the minus 4 to 10 to the minus 8. I'm not buying.

10 CHAIRMAN BROWN: Yes, I'm agreeing with
11 you. If you didn't get that out of my comments --

12 MEMBER DIMITRIJEVIC: Basically, the risk
13 associated with spurious trip, whereas, the risk
14 associated not to trip on demand, it's totally
15 different.

16 MR. GIBSON: Okay. So, I see where your
17 failure mode is here.

18 (Laughter.)

19 So, if you are viewing this strictly as
20 I'm going to take a CCF, and therefore, my diverse
21 thing helps me, that's one way you can look at it.
22 But, reality, your CCF does not have a zero, I mean,
23 a one probability. So, let's say the probability of
24 that CCF is really -- I'm just making this up -- 10 to
25 the minus 3. When you add that other device in there,

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 and you plug in those other reliability numbers,
2 that's where you see the impact of your diverse
3 system. Because it's only theoretical that a CCF will
4 always happen.

5 CHAIRMAN BROWN: All it's doing is
6 increasing the possibility that you may have a
7 response that is not unsafe; it's just it's
8 unreliable. It takes you offline. Whereas, the other
9 system, if it didn't have the backup, if it had the
10 failure when you had a demand, then you damage
11 something, the plant. You melt something or you have
12 whatever the circumstance is.

13 MEMBER MARCH-LEUBA: But in my car, I have
14 a car that only has brakes and two front tires. And
15 now, I've got a second system; the brakes are also on
16 the back tires. Tell me what's wrong with that. I
17 mean, what is this problem with having two --

18 MR. GIBSON: Well, we could probably move
19 on.

20 CHAIRMAN BROWN: We're going to move on.

21 MR. GIBSON: The data to support that is
22 in that report.

23 CHAIRMAN BROWN: Okay, we're terminating
24 all this. Go on to the next slide, Matt.

25 MR. GIBSON: All right.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 CHAIRMAN BROWN: Okay?

2 MR. GIBSON: I'll do the best I can.

3 The dependability, we did some research on
4 dependability, and we call it "methods for assuring
5 safety and dependability when applying visual
6 instrumentation and control system". We pursued
7 developing specific preventive and limiting measures
8 that could be used to reduce the likelihood that you
9 would have a CCF. And we brought those out in this
10 report.

11 We also furthered the research we did in
12 the previous one and looked at dealing with those
13 CCFs, software CCFs, and other CCFs, would have a
14 nexus to your safety analysis in your PRA. And that's
15 all in this report, and I think some of this was
16 advanced on NEI 16-16. But, you know, for whatever
17 reasons, I'm not familiar with all the reasons why
18 that didn't go forward.

19 We'll move on to the next research we did,
20 our most recent research, where we went and got
21 reliability data from the industry for equipment that
22 had been SIL-certified, Safety Integrity Level
23 certified, using the requirements in IEC 61508. So,
24 the previous OE data that we had was good, but it was
25 small as far as the amount of data we had, amount of

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 operation that we had. There was also a broad
2 diversity of systematic controls applied to that
3 equipment.

4 So, you know, software is not just
5 software. I mean, you have to understand how it was
6 made, under what circumstances it was made, and what
7 requirements were applied to it, because the software
8 reliability in your home router is different than it's
9 going to be in the one in your protection system in
10 your plant. It is.

11 And so, we figured out that we would have
12 to move on from nuclear information. There's just not
13 enough. There's enough digital in nuclear, and
14 nuclear is not that big of an industry comparative to
15 petrochemical and others.

16 So, through a series of NDAs, we were able
17 to get a fairly large amount of data, about 2 billion
18 hours or so of operating data off of 12 logic solvers.
19 And we analyzed those things.

20 What we were able to do with this research
21 is control for reliability. So, if you're doing a
22 research project and you want some highly reliable
23 software, you can only compare software that's been
24 created using the same process, even though it's
25 different software. Because if it's created with

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 different systematic processes, the information you
2 get might not be accurate.

3 So, by comparing software -- well, this
4 was software and hardware, but the software that had
5 been certified or created through the requirements of
6 IEC 61508, which had detailed specific implementation
7 requirements for software and hardware to drive
8 reliability. Then, we can compare, well, how did that
9 turn out? Did that process actually result in
10 reliable systems? And I think it did, because we
11 didn't find any platform-level issues that were
12 correlated to the software itself having a latent
13 failure out of those 2 billion hours.

14 So, that gives some statistical idea about
15 the platform software. I think Neil was talking about
16 what's a platform. In the case of this, it's your
17 hardware. It's your system software; that is, the
18 infrastructure software that's running that particular
19 program logic controller. It's also the library that
20 you subsequently use to make your software with. It's
21 the tools that you use to make those risks. So, it's
22 all those are included in the certification.

23 And that's also reflected in these hours,
24 too. Because the way this data is reported back
25 through the processes and the various pathways we use

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 to get the data, had there been a failure in, say, the
2 library, a function block, it would have been reported
3 back through this. Application failure, though, would
4 not be reported this way.

5 Let's see if there's anything more that we
6 can tell you.

7 MR. HECHT: Can I ask a question
8 about that data?

9 MR. GIBSON: Sure.

10 MR. HECHT: You said that some of it was
11 from SIL 3-certified platforms, some of it?

12 MR. GIBSON: It's all from SIL 3, in
13 SIL 3.

14 MR. HECHT: So, all those 2 billion
15 operating hours come --

16 MR. GIBSON: All from that, yes.

17 MR. HECHT: I see. But that would be a
18 pretty large sample, and it's pretty homogeneous
19 within that.

20 MR. GIBSON: Of course, that was the point
21 of it. See, we were actually testing -- you have
22 systematic controls on software resulting in high
23 reliability statistically. And that's what we were
24 able, we think, to demonstrate.

25 The only way you can do that is have a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 consistent process for producing the software. It's
2 just like a mechanical thing. If you have some steel
3 and you produce it one way, and you have some more
4 steel and you produce it a different way, you can't
5 compare the structural reliability of steel without
6 knowing how it was made and its metallurgy, and all
7 that sort of thing. And we did that here.

8 We controlled, basically, in sort of a
9 scientific method for how the software was made. And
10 so, what this tells you is that the systematic
11 controls required by IEC 61508 do result in a highly
12 reliable platform. I mean, that's the gist of what
13 our data showed.

14 MR. HECHT: Two billion hours is a lot of
15 data and should result in a fairly low or fairly
16 narrow confidence interval. Do you have the numerical
17 value for the platform?

18 MR. GIBSON: You know what? I don't. I
19 don't have it. We did not calculate a 10 to the minus
20 frequency. And I'll tell you why. We'll talk about
21 it because I have a little more time.

22 CHAIRMAN BROWN: Why don't you move on?

23 MR. GIBSON: Well, this is an important
24 tie-in to something else I'm going to say.

25 The researchers, the team researching

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 this, we did not want to claim a 10-to-the-minus or a
2 frequency-type conclusion for this because the
3 academic community and the practitioner community,
4 when you do this, do not support ever doing that.

5 So, really -- and this is something maybe
6 you guys can think about -- what we really did with
7 this is prove the effectiveness of the systematic
8 control, not necessarily reliability of the software
9 in general. So, this data that we have only mattered
10 or has relevance if you're talking about an IEC 61508-
11 certified device. It doesn't really mean anything
12 otherwise, right, because that's what we controlled
13 for.

14 So, in the future, if you want to do
15 integration of risk reliability for software, you're
16 really going to have to control for how it was made,
17 because that's really the reliability metric you're
18 measuring, is the reliability of that process, not the
19 intrinsic reliability of software, because it's all
20 over the place.

21 Any more?

22 MR. HECHT: I think we're limited by time.

23 MR. GIBSON: All right. Well, there we
24 go.

25 You've seen this before. I'll just

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 concentrate on a little bit about the insight we got
2 from doing that was that your platforms and your
3 integration activities and your applications are
4 really three distinct layers of the composition. And
5 in the broader world, they're really done by different
6 people usually. Platforms are currently bought. Most
7 people, even in our current nuclear industry, buy
8 their platforms from somebody and they add integration
9 applications to it.

10 So, we think that even potentially for any
11 retroactivity you're doing that, if you separate these
12 out a little bit and potentially have maybe different
13 criteria for the different platforms, integrations,
14 and applications, it will make it more straightforward
15 to analyze something you get to read. So, that's
16 something to think about.

17 When you actually build one of these, when
18 you build a system, this is how you build it. This is
19 how you really put it together and make it and test it
20 and do stuff. You start with the platform, you
21 integrate, you add applications to the top of it.

22 We'll move on to HAZCADs. You know, folks
23 mentioned that a little bit. We've published HAZCADs
24 and you have a copy of it in-house. Revision 1 is
25 coming out in the summer next year. We published it

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 in the version you see, so we could get started doing
2 blind studies. So, we have done blind studies with
3 this product with utility and some vendor
4 participants.

5 So, if you can see this, okay, if you look
6 closely at this -- on your handout it's gray, so
7 that's good -- but if you look on your handout, you'll
8 see the gray squares that are on the fault tree. So,
9 what we're able to do with this process is to use a
10 process called System Theoretic Process Analysis,
11 which is a hazard analysis developed by MIT. It's
12 being proven to be very favored in other industries.
13 And it gives you a structured way to find the problems
14 with your system at whatever level of decomposition
15 you need.

16 So, what we do with this process is we
17 look for those hazards through this process. Again,
18 that's something we can talk about in some detail
19 later. But, if we find what's called an unsafe
20 control latch, which is a result of this analysis, we
21 can then insert it into the fault tree. See where
22 these gray slots are.

23 This is a qualitative idea. So, what we
24 do is we put the qualitative node into the fault tree
25 and, then we do sensitivity analysis on it, again, by

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 setting it to always true and always false. And that
2 gives an idea of what kind of impact that particular
3 piece of equipment would have on your top event
4 frequency. So now, we know what the hazards are,
5 which is one big thing, and the next thing we know is
6 how sensitive that that digital hazard will be to the
7 final consequence.

8 Now, in our estimation, in our research,
9 this provides a risk-informed infrastructure for
10 digital I&C because it combines qualitative and
11 quantitative analysis, gives you a sensitivity for
12 your qualitative ideas, and from that, then, you can
13 decide on the degree of qualitative or systematic
14 controls you want to apply to achieve a high degree of
15 reliability for a software-based system.

16 And we talk about a little in the bottom,
17 the next thing you press on after this is look at your
18 causal factors, which gives you your initiating causes
19 for each one of these function blocks. That's sort of
20 below this block in the fault tree. So now, we know
21 why this particular node in the fault tree -- what
22 things are driving it. And we include all manner of
23 reliability issues, including cybersecurity, in that.

24 We just finished blind studies doing this,
25 as I mentioned. We got a darn good insight with that.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 We found out that STPA worked really well in finding
2 the faults or the hazards -- let's put it that way --
3 all kinds of hazards. Design hazards mainly is what
4 we're looking at here.

5 We did that by crafting a scenario where
6 we knew there was a problem with the system and asking
7 the participants to find that problem using this
8 process, and they did. They were 100 percent
9 successful finding the unknown problem that they were
10 faced with.

11 What we did find out is engineering and
12 risk analysis -- and I'll say, you know, that's the
13 challenge we face all around -- engineering, a lot of
14 folks, the engineers aren't that familiar with how to
15 do risk and fault trees, and the fault tree people
16 aren't really comfortable with saying, well, if it's
17 10 to the minus X, then we're done, the actual
18 analysts themselves.

19 So, we think this process is going to have
20 to be a team process where your engineering folks do
21 the hazard analysis and the causal factors, and then,
22 the risk analysts will, then, apply that and do
23 sensitivity analyses to give you the risk insights you
24 need.

25 And depending on the level at which you do

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 it, your risk insights can come from simply knowing
2 the hazards and the likelihood and the causal factors.
3 So, there's a little triangle here that you can see on
4 your thing. It's kind of like the risk triangle. If
5 you break any one of these sides, you've prevented the
6 consequence. You've eliminated a hazard. You've
7 eliminated the causal factors. Or you reduced the
8 likelihood to a very low level.

9 MR. HECHT: Can I ask a question about the
10 HAZCADS methodology?

11 MR. GIBSON: You sure can.

12 MR. HECHT: You say it provides a basis
13 for risk-informed I&C infrastructure. Are you
14 advocating that the NRC consider using HAZCADS, and if
15 so, I guess I would have a lot of questions about how
16 STPA is being applied. And specifically, you have --

17 MR. GIBSON: EPRI doesn't do policy
18 advocacy. So, we do this and we provide it to our
19 community of interest, which is you guys and our
20 utility members. So, I think if you want to do risk-
21 informed, you ought to look at it.

22 MR. HECHT: Okay. Thank you.

23 MR. GIBSON: Any other questions you might
24 have in the future, feel free to reach out.

25 DRAM is part of this process. It's a

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 modular process. This is where we look for the causal
2 factors. These are the things that would contribute
3 to the reliability issues that you have in any digital
4 system. This will be a replacement for our 300, 200-
5 5326 process, and it will give it structure, a three-
6 step structure; and also, leverage the terminology and
7 requirements of 61508. So now, you'll be working
8 towards the industry standards that have been proved
9 very effective in achieving high reliability in like
10 PLCs and other types of safety devices.

11 I'll just flash this. We can move on to
12 the next one.

13 This is something we're working on, is to
14 more clearly define software common-cause failure.
15 Common-cause failures really have a context. I think
16 Steve Vaughn talked about it. They're really part of
17 the decomposition of your system and they exist in
18 various levels of your system composition and
19 decomposition.

20 And we think it's important to have a
21 good, crisp definition, at least in our research. So,
22 we're trying to do some research on what that would
23 actually mean. What is a software common-cause
24 failure? Certainly, we have to have some redundancy
25 expectation to achieve a common cause because it has

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 to have that, but we also want to separate and help
2 people identify the difference between a software
3 common-cause failure and a single point vulnerability,
4 because that gets conflated a little bit sometimes.

5 This is how it's put together. The
6 HAZCADS you just were looking at, which has the STPA
7 and FDA. The reliability is integrated into a systems
8 engineering process. This is the process that I think
9 Neil Archambo mentioned that U.S. industry has
10 adopted. The CNOs have created a recommendation that
11 every utility adopt these. So, the industry is in the
12 process of adopting this process using the Digital
13 Engineering Guide to improve the execution or do the
14 modification. And they will be using these components
15 when they do it.

16 I think maybe the last thing to see -- and
17 you can study these, I guess -- this is a reliability
18 model. And also, it's risk-informed. Your HAZCADS
19 and your DRAM come together. You get your hazards
20 inventory and sensitivity results, and you can take
21 actions on those. You can make design changes and
22 other compensatory measures to ensure that the
23 consequence is not actualized.

24 (Announcement of alarm condition in
25 building.)

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MR. GIBSON: All right. I'll try to speak
2 over our AI that's speaking to us.

3 (Laughter.)

4 Our overall insights -- we probably just
5 should have started with this slide -- are that your
6 software reliability is really proportional to
7 systematic controls and design and implementation
8 constraints. You've got to constrain the design, too.
9 You can't do things that are inherently unreliable to
10 do. It's just one of those things.

11 CCF is a subset of total software design
12 and implementation errors. You can't have a software
13 CCF unless you have a software failure in the first
14 place. Your software CCF really needs to be more
15 narrowly defined. I mean, just as a practitioner, it
16 helps to have it narrowly defined because then you can
17 work on the actual failure mechanisms that caused that
18 particular thing to happen, not a more broad idea of
19 software common-cause failure. And you need to be
20 really aware of where in the decomposition of the
21 system the software common-cause failure occurred,
22 whether it's in the application or in the platform.

23 (Announcement of alarm condition in
24 building continues.)

25 MR. GIBSON: Why don't you all guys read

1 this? Because I can't do it with this guy talking in
2 my head.

3 (Laughter.)

4 So, questions, anybody?

5 MEMBER BLEY: That's all right. Your
6 voice cuts right through it.

7 MR. GIBSON: Oh, does it now.

8 (Laughter.)

9 I guess the last one, the last thing,
10 maybe the last two, is we get a lot of value -- this
11 is a good point to make. If you look at the IEC
12 stuff, if you look at NUREG-0800, and you look at
13 Chapter 7, all of the standard references in there are
14 about 30 years old. I mean, they are. We froze them
15 in time. The rest of the industry worldwide, the
16 safety industry, has moved along, because more and
17 more things are done with software.

18 So, what we find when we look out in the
19 other industries, the non-nuclear safety industries
20 which primarily use the IEC standard, they potentially
21 -- I mean this is for your consideration -- have
22 eclipsed us in their ability to ensure reliability of
23 a system or a component that's software-based. They
24 have good processes. They have an active community of
25 academics, vendors, and experts working on these

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 standards all the time, integrating their operational
2 experience into it. Our research indicates that
3 they're achieving a pretty good degree of reliability.
4 IEC is the primary standard body that's working with
5 folks for autonomous cars, autonomous cranes, and
6 they're integrating all that OE. They're getting
7 software reliability back into those standards. So,
8 they're pretty good.

9 It's also where, if we need data, if you
10 need data to support adopting any of these things,
11 you're really going to have to go after non-nuclear
12 databases because they're big. Maybe you can get at
13 them. But I think that would be something to
14 consider.

15 CHAIRMAN BROWN: Okay. The next round, we
16 need to get public comment. So, why don't you get the
17 phone, and I'll ask, is there anybody in the room that
18 would like to provide comments?

19 (No response.)

20 Hearing none, we will wait for the line.
21 Is the line open? Or are you going to open it?

22 Thank you, Matt.

23 MR. GIBSON: You're welcome.

24 CHAIRMAN BROWN: We're going through the
25 rest of the dog-and-pony show right now.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 MR. GIBSON: I understand.

2 CHAIRMAN BROWN: Is there anyone on the
3 public line who would like to make a comment for this
4 meeting? If so, say something.

5 (No response.)

6 Hearing none, we will close the public
7 line.

8 Are there any other comments from members?
9 Anybody? I'll start with Dennis, on your side.

10 MEMBER BLEY: Nothing to add. It was a
11 good day. I learned a lot and look forward to seeing
12 the next round.

13 CHAIRMAN BROWN: Okay. Jose?

14 MEMBER MARCH-LEUBA: Nothing to add.

15 CHAIRMAN BROWN: Joy?

16 MEMBER REMPE: I just wanted to thank the
17 presenters for their patience today. This was an
18 unusually different day for our abilities to have a
19 meeting.

20 CHAIRMAN BROWN: I guess we lost Ron.

21 Does our consultant have any additional
22 comments?

23 MR. HECHT: Just to reiterate the fact
24 that I think Matt said that we should be using non-
25 nuclear data sources. ORNL tried; it didn't work.

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 Perhaps it would work better.

2 CHAIRMAN BROWN: Oh, okay.

3 MR. HECHT: Perhaps we could get some help
4 from EPRI or others, I guess primarily EPRI. I think
5 that, irrespective of whether EPRI is able to get
6 their NDA data to us, perhaps some guidance for how
7 the NRC might be able to acquire it on its own might
8 be valuable.

9 With respect to the HAZCADS methodology
10 and the integration with FDA for probabilistic risk
11 assessments, Nancy Leveson probably would not approve
12 of that, saying that anytime she has a box with a
13 software probability failure, she would say, "Just
14 make it one."

15 But STPA certainly can be valuable in
16 terms of defining requirements for failure mitigation
17 and for hazard mitigation, what they call
18 "constraints," and should be considered.

19 And finally, with respect to the comments
20 about, whether it's 61508 or BTP 7-19, the underlying
21 principles I think haven't changed in 30 or 40 years,
22 which is, basically, define good requirements; create
23 a design traceable to those requirements; implement
24 code traceable to the design, and test at all levels.
25 I would say that it might be instructive to look at

NEAL R. GROSS

COURT REPORTERS AND TRANSCRIBERS
1323 RHODE ISLAND AVE., N.W.
WASHINGTON, D.C. 20005-3701

1 the differences between 7-19 and 61508 to see if there
2 are any really significant differences from those
3 principles.

4 MR. GIBSON: So, I did want to mention
5 that we are bringing HAZCADs to the STPA conference
6 this coming year. And so, we think Ms. Leveson will
7 allow us to present.

8 MR. HECHT: I'm sure she will.

9 CHAIRMAN BROWN: Okay. Thank you very
10 much, Myron.

11 With that, I don't have any additional
12 comments to make, either.

13 So, with that, we are adjourned.

14 (Whereupon, at 4:49 p.m., the Subcommittee
15 was adjourned.)

16

17

18

19

20

21

22

23

24

25

Branch Technical Position 7-19 Draft Revision 8

Advisory Committee on Reactor Safeguards
Subcommittee Meeting
NRC Staff Presentation
November 21, 2019

Agenda

- Background on Commission's Common Cause Failure (CCF) Policy
- Objective of Branch Technical Position (BTP) 7-19 Modifications
- Key Changes:
 - Categorization Scheme and Graded Approach
 - Defense-in-Depth and Diversity (D3) Assessment
 - Means to Eliminate CCF from Further Consideration
 - Qualitative Assessment
 - Spurious Operation Assessment
 - Re-structuring of BTP

Objective

- Present the modifications proposed for the next draft of BTP 7-19 regarding the review of license applications and amendments addressing CCFs due to latent software defects
- Obtain ACRS Subcommittee feedback for draft BTP-19, Revision 8

Background: Commission's Policy on CCF

- SRM-SECY-93-087 presents the Commission's policy on how potential CCFs should be addressed in DI&C systems
- Provides four positions for addressing potential CCFs
 - Perform D3 assessment to demonstrate that vulnerabilities to CCF have been adequately addressed
 - Analyze each postulated CCF for each event evaluated in the SAR accident analysis using best estimate methods
 - If the assessment shows a CCF could disable a safety function, provide a diverse means with a documented basis that the diverse means is unlikely to be subject to the same CCF
 - Provide a set of diverse displays and controls located in the main control room for manual, system-level actuation of critical safety functions and monitoring of critical plant parameters to support the performance of these safety functions

Background: SECY-18-0090

- SECY-18-0090 clarifies the application of the Commission's direction in the four positions within SRM-SECY-93-087
 - Recognizes significant effort has been applied to the development of highly reliable DI&C systems but residual faults within digital systems may lead to CCFs
 - Provides five guiding principles for updating the staff's guidance for addressing CCF

Summary of Draft BTP 7-19 Changes

- Incorporates the guiding principles from SECY 18-0090 Alignment
- Clarifies the applicability of the D3 assessment to safety-related systems with high safety significance
- Incorporates qualitative assessment criteria from Supplement 1 to RIS 2002-22 for non-RPS/ESFAS
- Clarifies staff positions on means to address CCF
- Provides additional guidance on spurious operation assessment
- Improves the structure of the BTP to enhance ease of use

Key Changes: Categorization Scheme and Graded Approach

	Safety-Related	NSR
Safety Significant— Significant contributor to plant safety	A1 Perform D3 Assessment	B1 Perform Qualitative Assessment
Not Safety Significant— Not a significant contributor to plant safety	A2 Perform Qualitative Assessment	B2

Deterministic Criteria for Categorization of DI&C Systems (1)

- A1: safety-related DI&C system that:
 - Is relied upon to initiate and complete control actions essential to maintain plant parameters within acceptable limits established for a DBE, or
 - Whose failure could directly lead to accident conditions that may cause unacceptable consequences if not mitigated by other A1 systems
- A2: safety-related DI&C system that:
 - Provides an auxiliary or indirect function in the achievement or maintenance of plant safety, or
 - Maintains the plant in a safe shutdown state after the plant has reached initial safe shutdown state

Deterministic Criteria for Categorization of DI&C Systems (2)

- B1: NSR DI&C that:
 - Directly controls the reactivity or power level of the reactor, or
 - Whose failure may result in unacceptable consequences to plant safety due to integration of multiple control functions into a single system
- B2: NSR DI&C system that:
 - Does not have direct affect on reactivity or power level of the reactor, or
 - Whose failure does not have consequences to plant safety or whose failure can be detected and mitigated with significant safety margin

Use of Risk Insights to Support Categorization

- Risk insights can be used to support the safety-significance determination in categorizing the DI&C system in terms of safety consequences from site-specific PRAs
- Use of risk insights should be an input to an integrated decision-making process for categorizing the proposed DI&C system

Key Changes: D3 Assessment

- D3 assessment should be performed for A1 systems
- D3 assessment includes determination of whether:
 - CCF vulnerability is eliminated from further consideration by use of design attributes, testing, or defensive measures;
 - A diverse means can be used to perform the same or different function than the safety function disabled by the postulated CCF; or
 - Consequence of a DBE concurrent with a CCF of the A1 system is acceptable
- For systems that are not A1 but are integrated with A1 systems, the D3 assessment should be performed on the integrated system unless it can be shown that the non-A1 system will not adversely impact the A1 system upon a postulated CCF

Key Changes: Means to Eliminate CCF from Further Consideration (1)

- Use of design attribute: diversity within the DI&C system or component
 - Provides guidance to use diversity within each safety division or among redundant divisions to address CCF
 - Calls for an analysis to demonstrate sufficient diversity exists in the design, so it is not subject to the same CCF
 - Provides acceptance criteria for use of this attribute

Key Changes: Means to Eliminate CCF from Further Consideration (2)

- Use of testing to demonstrate latent defects are not present
 - Clarifies criteria and terminology associated with use of testing to eliminate CCF from further consideration
 - Emphasizes the limitations on use of testing
 - Provides guidance to establish test methods
 - Provides acceptance criteria

Key Changes: Means to Eliminate CCF from Further Consideration (3)

- Use of defensive measures
 - Provides guidance to use defensive measures to prevent, limit, or mitigate the effects of a potential CCF to eliminate CCF from consideration
 - Provides criteria to use defensive measures based on an NRC-approved methodology
 - Provides criteria for use of other methodologies with the provision of a technical basis and acceptance criteria

Key Changes: Diverse Means (1)

- Clarifies guidance on the use of diverse means to perform the same or different function as the safety function disabled by the postulated CCF
- Clarifies the types of diverse means that can be credited
 - Existing systems
 - Manual operator actions
 - Diverse system
- Identifies acceptance criteria

Key Changes: Diverse Means (2)

- Provides guidance on the use of equipment outside the main control room for the performance of manual operator actions
 - Applies only for use of diverse means to address Position 3 in the SRM-SECY-93-087
- Clarifies guidance to address Position 4 in SRM-SECY-93-087, which calls for manual controls and indications located in the MCR to perform manual system level actuation of critical safety functions

Key Changes: Qualitative Assessment

- Provides guidance for performing a qualitative assessment to evaluate potential CCFs and their effects in A2 and B1 systems
- Identifies three factors can be used to show that the likelihood of CCF is sufficiently low, including:
 - Design attributes
 - Design quality
 - Operating experience
- Provides guidance on the performance of a qualitative assessment on a B2 system that could place the plant in an unanalyzed condition
 - Basis for not performing an assessment should be documented

Key Changes: Spurious Operation Assessment

- Provides bifurcated criteria for addressing spurious operation of SSCs due to a CCF in a DI&C system
- Provides guidance for operating reactors for performing an assessment to demonstrate that the safety analysis of spurious operations is not invalidated by the proposed digital modification
- Provides guidance for new and advanced reactors for performing an assessment to demonstrate that potential spurious operation of SSCs is bounded by events analyzed in the safety analysis
- Clarifies scope and methods for performing the assessment, including use of design attributes, testing, and defensive measures to eliminate CCF from further consideration

Key Changes: Re-Structuring of BTP 7-19

- Simplifies background and incorporates new guidance on CCF
 - SECY-18-0090
 - NUREG/CR 7007
 - RIS 2002-22, Supplement 1
- Maps criteria to four positions in the SRM-SECY-93-087
- Consolidates CCF guidance and corresponding acceptance criteria

Next Steps

- Public comment period ends in February 2020
- Potential public meeting during public comment period to facilitate comments
- Potential second ACRS Subcommittee meeting in Spring 2020 if changes resulting from public comment period are significant
- ACRS Full Committee meeting in Spring 2020
- OMB review and publication of final BTP 7-19, Revision 8 anticipated in 3rd Quarter 2020

Questions

Questions



Acronyms

BTP	Branch Technical Position	NSR	Not safety related
CCF	Common Cause Failure	PRA	Probabilistic Risk Assessment
CFR	Code of Federal Regulations	RIS	Regulatory Issue Summary
D3	Defense-in-Depth and Diversity	RPS	Reactor Protection System
DI&C	Digital Instrumentation and Control	SAR	Safety Analysis Report
ESFAS	Engineered Safety Feature Actuation System	SRM	Staff Requirements Memorandum
MCR	Main Control Room	SSC	Structure, System and component
MP	Modernization Project		

Background Information

Modernization Plans (MPs)

- Developed in accordance with Staff Requirements Memorandum (SRM) to SECY-16-0070
- MP#1 – Common Cause Failure
 - MP#1A: Supplement 1 to RIS 2002-22
 - MP#1D: Update to BTP 7-19
- MP#2 – 10 CFR 50.59 Guidance
- MP#3 – Commercial Grade Dedication
- MP#4A – ISG-06 Revision
- MP#4B – Broader Modernization Activities

SECY-18-0090 – Five Guiding Principles

1. Applicants and licensees for Production and Utilization Facilities under 10 CFR Part 50, “Domestic Licensing of Productions and Utilization Facilities” or under 10 CFR Part 52, “Licensees, Certifications and Approvals for Nuclear Power Plants” should continue to assess and address CCFs due to software for DI&C systems and components.
2. A defense-in-depth and diversity analysis for reactor trip systems and engineered safety features should continue to be performed to demonstrate that vulnerabilities to a CCF have been identified and adequately addressed. In performing this analysis, the vendor, applicant, or licensee should analyze each postulated CCF for each event evaluated in the accident analysis section of the safety analysis report. This defense-in-depth and diversity analysis can be either a best estimate analysis or a design-basis analysis.
3. This analyses should also be commensurate with the safety significance of the system. An analysis may not be necessary for some low-significance I&C systems whose failure would not adversely affect a safety function or place a plant in a condition that cannot be reasonably mitigated.

Five Guiding Principles continued

4. If a postulated CCF could disable a safety function, then a diverse means, with a documented basis that the diverse means is unlikely to be subject to the same CCF, should perform either the same function or a different function. The diverse or different function may be performed by either a safety or a non-safety system if the system is of sufficient quality to perform the necessary function under the associated event conditions in a reliable manner. Use of either automatic or manual actuation within an acceptable time frame is an acceptable means of diverse actuation. If the defense-in-depth and diversity analysis demonstrates that a CCF, when evaluated in the accident analysis section of the safety analysis report, can be reasonably mitigated through other means (such as with current systems), a diverse means that performs the same or a different function may not be needed.
5. The level of technical justification needed to demonstrate that defensive measures (i.e., prevention and mitigation measures) are adequate to address potential CCFs should be commensurate with the safety significance of the DI&C system. For the systems of higher safety significance, any defensive measures credited need technical justification that demonstrates that an effective alternative to internal diversity and testability has been implemented.

SRM to SECY-93-087

1. The applicant shall assess the defense-in-depth and diversity of the proposed instrumentation and control system to demonstrate that vulnerabilities to common-mode failures have adequately been addressed.
2. In performing the assessment, the vendor or applicant shall analyze each postulated common-mode failure for each event that is evaluated in the accident analysis section of the safety analysis report (SAR) using best-estimate methods. The vendor or applicant shall demonstrate adequate diversity within the design for each of these events.
3. If a postulated common-mode failure could disable a safety function, then a diverse means with a documented basis that the diverse means is unlikely to be subject to the same common-mode failure, shall be required to perform either the same function or a different function. The diverse or different function may be performed by a nonsafety system if the system is of sufficient quality to perform the necessary function under the associated event conditions.
4. A set of displays and controls located in the main control room shall be provided for manual, system-level actuation of critical safety functions and monitoring of parameters that support the safety functions. The displays and controls shall be independent and diverse from the safety computer system identified in Items 1 and 3 above.

Graded Approach for Systems Categorization Concept

	Safety-Related	Non-Safety Related
Safety Significant	A1 (e.g. Protection System, Safety Control Systems*, Load Sequencers*)	B1 (e.g. Rod Control System, Feedwater Control system, Certain BOP Control Systems)
Not Safety Significant	A2 (e.g. Safety Chillers, Safety Control Systems*, Load Sequencers*)	B2 (e.g. Plant Computer, Service Water System Controls)

*The staff recognizes actual categorization may be driven by specific plant system configurations, the exact nature in which systems may be interconnected by digital equipment, and the plant's licensing basis. Systems that depend on the overall plant design may be safety significant or non-safety significant.

Common Cause Failure (CCF) and DI&C Systems

ACRS Subcommittee – DI&C

November 21, 2019



Background and Context

- Common Cause Failure (CCF) in digital systems:
 - The determination of reasonable assurance with respect to digital and analog systems should be congruent
 - Challenges with using probabilistic terminology in a deterministic context
 - Focus has been on ‘eliminating the consideration of CCF’ as opposed to ‘appropriately addressing CCF’
 - Software vs Hardware reliability

Path Forward

- Align on 1st principles
 - Software quality depends on complete and correct requirements, design, and implementation
 - Concurrent triggering conditions are required to activate a latent software defect
 - The effects and the likelihood of a software CCF can be minimized by design
 - Operating history can support software quality

Path Forward

- Align on Safe Design Objectives
 - Design Requirements Development
 - Design Attributes
 - Quality of the Software Design Process
 - ◆ Graded approach to safety
 - Division of Responsibility

Closing Remarks

- If CCF is ‘appropriately addressed’, then a diverse backup is not warranted
- CCF can be ‘appropriately addressed’ by adhering to:
 - ◆ 1st principles
 - ◆ Safe design objectives
 - ◆ Use industry best practices

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

ACRS Digital I&C Subcommittee Meeting on Draft Branch Technical Position (BTP) 7-19, Revision 8

Matt Gibson
Technical Executive
Digital Instrumentation & Control
mgibson@epri.com

November 21st, Washington DC



Introduction

- Over the past 10 yrs. EPRI has conducted various R&D projects to investigate digital I&C reliability and the nexus to plant safety.
- Today we will review the key R&D products developed over that period, the cumulative conclusions reached, and the methodologies developed to address digital technology.
 - 1016731- US 1E and Non-1E OE on digital systems
 - 1022986- KHNP 1E and Non-1E OE on digital systems
 - 1019183- Sensitivity of digital in D3,PRA, and Safety Analysis
 - 3002005326/DRAM- Safety and dependability Methods for digital systems
 - 3002011817- Safety Integrity Level(SIL) Certification efficacy for nuclear
 - 3002012755 – HAZCADS- Hazards analysis for digital systems
 - 3002011816 – Digital Engineering Guide (DEG)- systems engineering

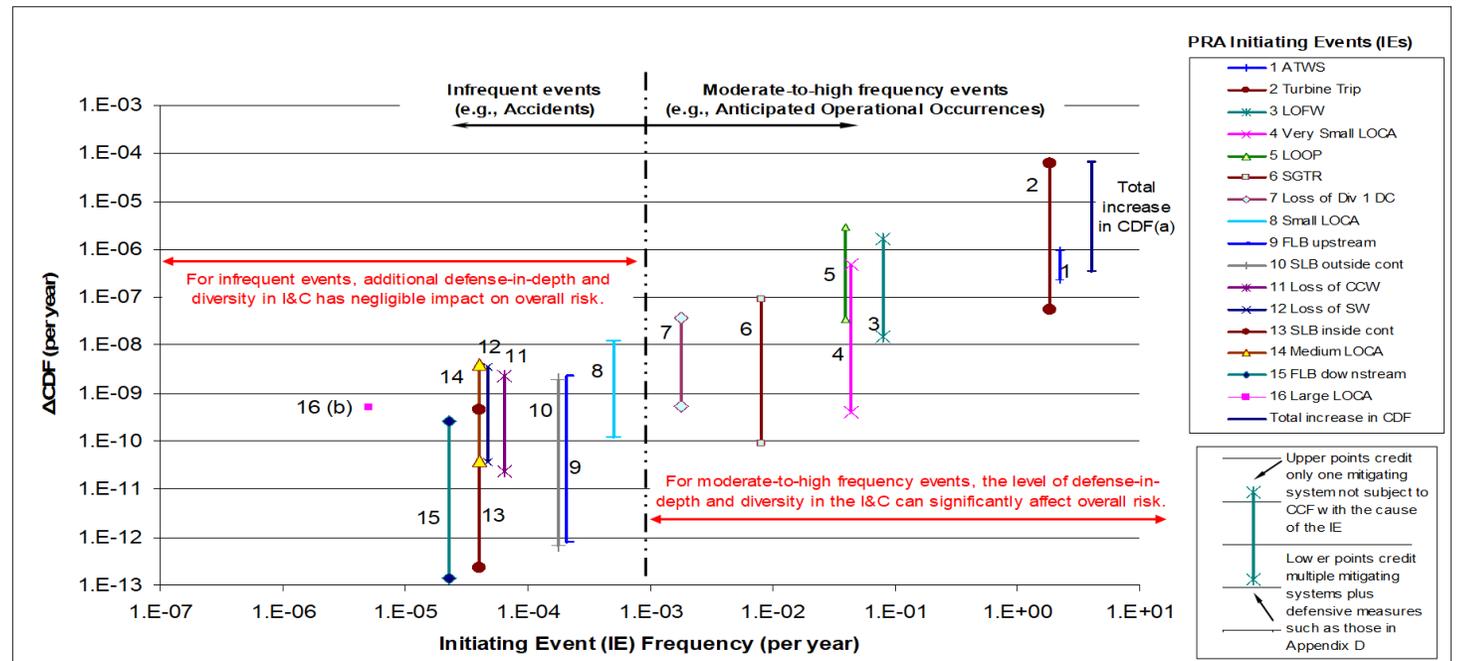
Past Operating Experience Reviews- US and Korea

- EPRI research has looked for software common cause failures in the OE data of 1E and non-1E systems
- CCF not very prevalent in safety-related systems
- Conclusions from 1016731 (US) and 1022986 (KHNP) Data:
 - Software has been no more problematic than other CCF contributors
 - Past methods have been effective in keeping software a minor contributor to potential 1E CCFs
 - EPRI Research has not identified any 1E events where diverse platforms would have been effective in protecting against SCCF. SCCF occurs predominately at the application level.
 - Several identified events confirmed the effectiveness of signal and functional diversity in protecting against CCF

Categories	U.S. 1987 – 2007 (EPRI 1016731)	KHNP 1984 – 2010 (EPRI 1022986)
Safety-related digital events reviewed	49	19
Single failures	38 (78%)	19 (100%)
Non-software common cause failures	10 (20%)	0 (0%)
Software common cause failures	1 (2%)	0 (0%)
Non-safety related digital events reviewed	273	78
Single failures	217 (79%)	61 (78%)
Non-software common cause failures	42 (19%)	14 (18%)
Software common cause failures	14 (2%)	3 (4%)

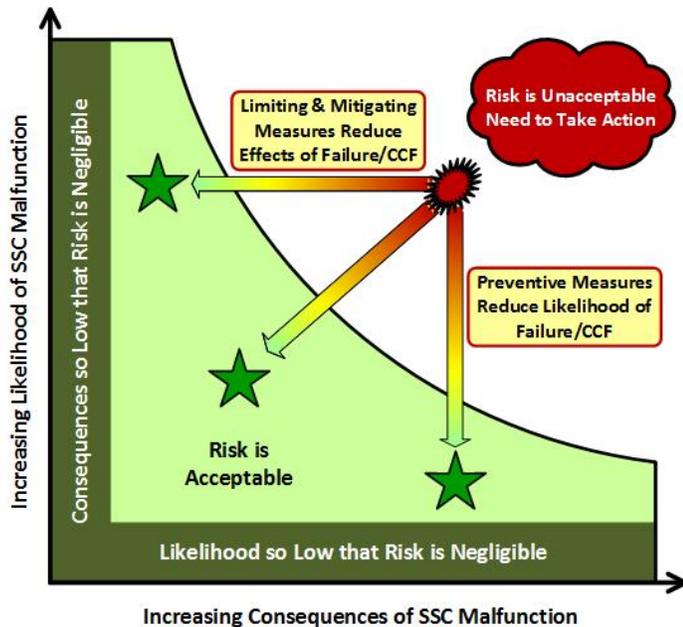
Effects of Digital Instrumentation and Control Defense-in-Depth and Diversity on Risk in Nuclear Power Plants - 1019183

- Eighteen initiating events were analyzed.
- Six sensitivity studies conducted: including addition of diverse platforms.



- Event and sensitivity analysis concluded that a diverse platform was not more effective in mitigating postulated SCCF than functional diversity or manual operator action.
- For low frequency events I&C diversity had even less risk impact.

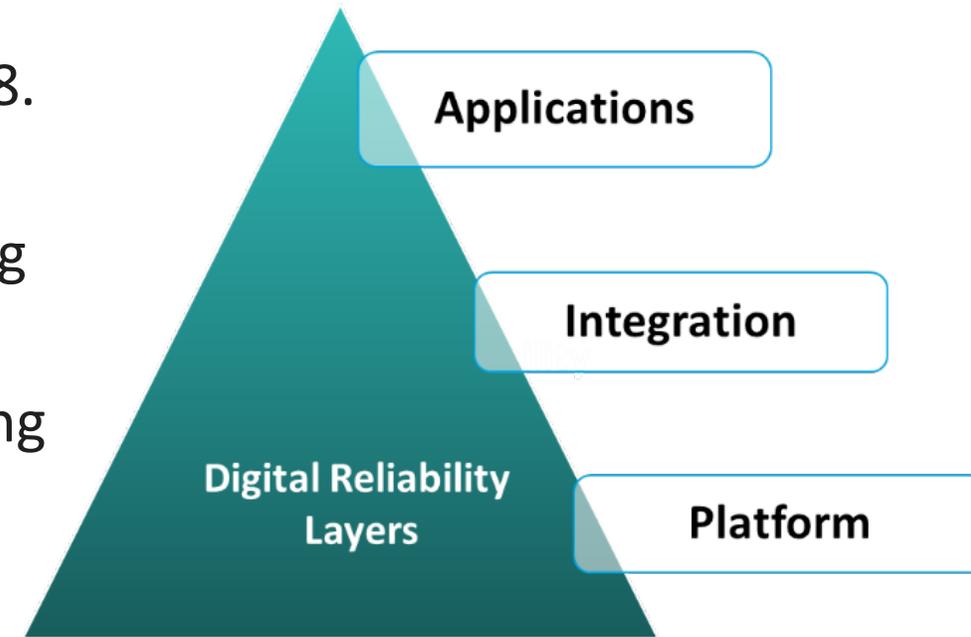
Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems- 3002005326



- Developed Preventive and Limiting (P&L) measures based on I&C failure/error modes.
- Developed Safety Analysis and PRA evaluation methods to integrate P&L and risk insights.
- Developed a Safety Significance based graded approach.
- Highlighted the need for more effective hazards analysis.
- Highlighted the need for more effective risk analysis integration.
- Results pointed to a more structured dependability analysis and implementation based on international standards.

Safety Integrity Level (SIL) Certification Efficacy for Nuclear Power- 3002011817

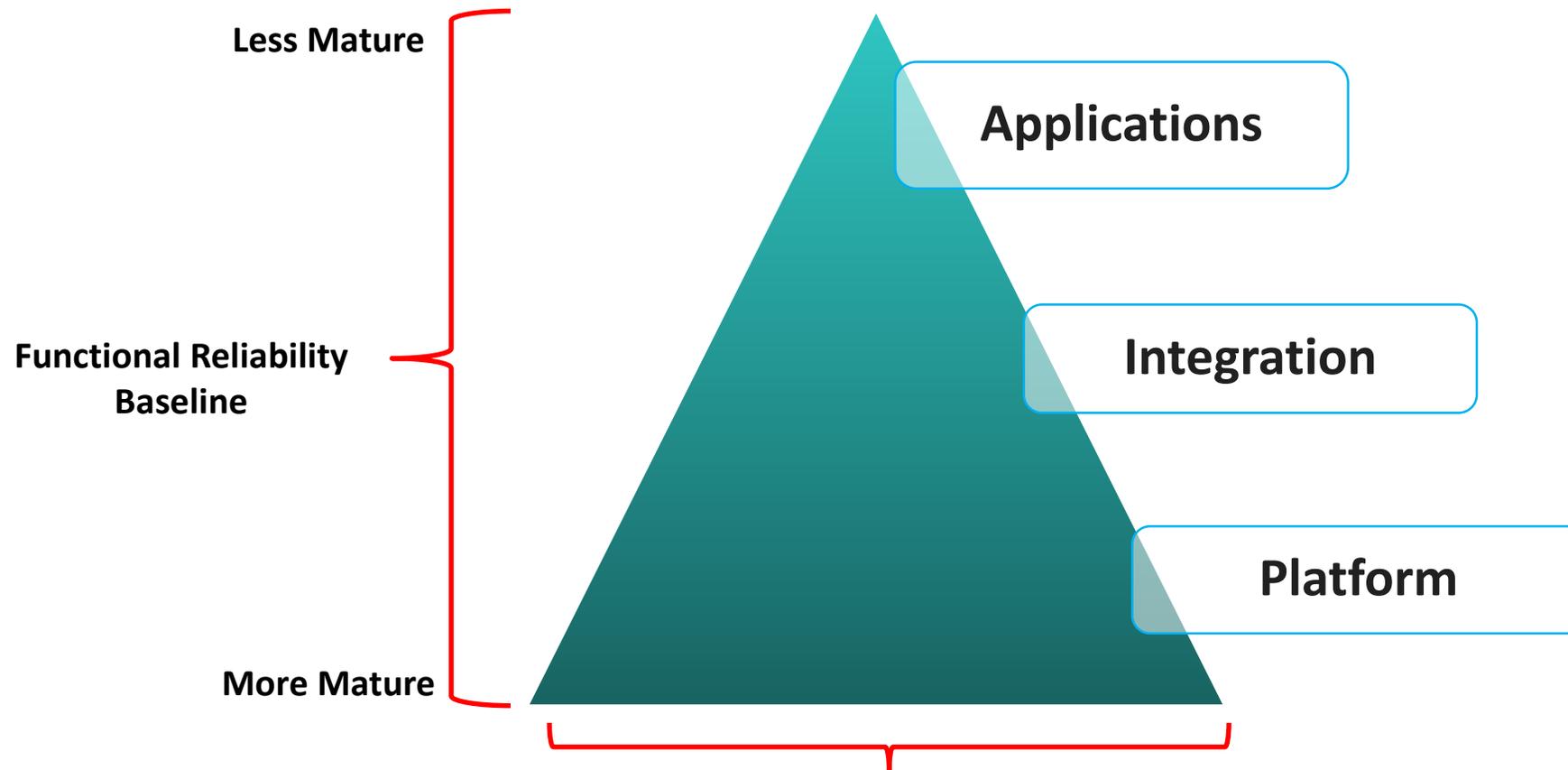
- Studied reliability of platforms certified to IEC-61508.
- Achieved a large data set across 12 safety logic solvers(e.g. PLC's), nearly 2 billion hours of operating data.
- More effective data than traditional OE by controlling for quality.
- Non-nuclear safety platforms proved very reliable, hardware and software, at the ***platform level***.



- **Since SCCF is a subset of all software failures, a high software reliability correlates with a low likelihood of SCCF.**
- **SIL certification has a high efficacy for replacing some existing design and review processes.**
- **Being Leveraged by NEI for MP#3 via NEI 17-06 in US.**

Reliability Layers

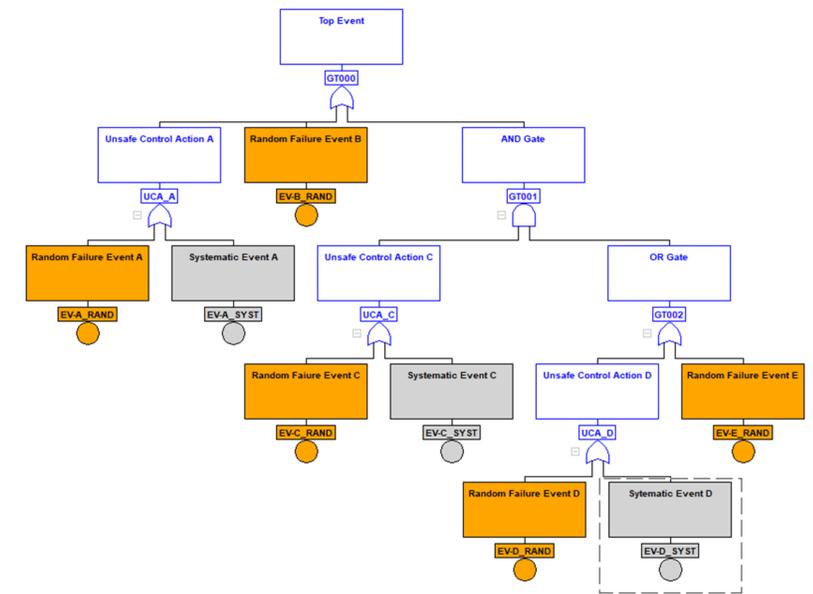
Reliability, especially software reliability, including CCF, should be segmented by *platform, integration, and application*.
Then Considered Separately



Production Data and OE Quantity and Quality Drive Maturity and Reliability using IEC-61508/SIL

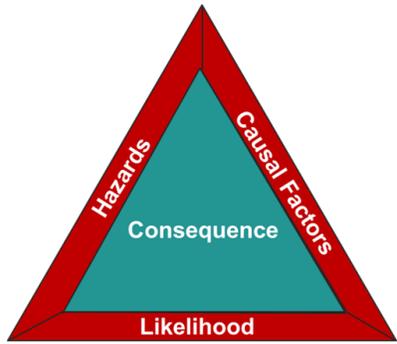
HAZCADS: Hazards and Consequences Analysis for Digital Systems-3002012755

- Advances the use of hazards analysis to identify system and plant level digital I&C design and implementation issues, including CCF and SPV.
- Executed throughout the design and implementation lifecycle.
- Uses System Theoretic Process Analysis(STPA) and FTA.
- Integrates qualitative hazards with random failures with Fault Tree Analysis based sensitivity analysis.



- **Achieves a credible risk informed I&C infrastructure compatible with existing processes.**
- **Dramatically improves hazard detection, resolution, and overall system reliability.**
- **Validated through blind studies and usability workshops.**
- **Used with causal factor analysis methods for a complete reliability assessment and resolution methodology.**

Risk- Informed Process Insights From Blind Studies



Risk Triangle

Engineering

Risk Analyst

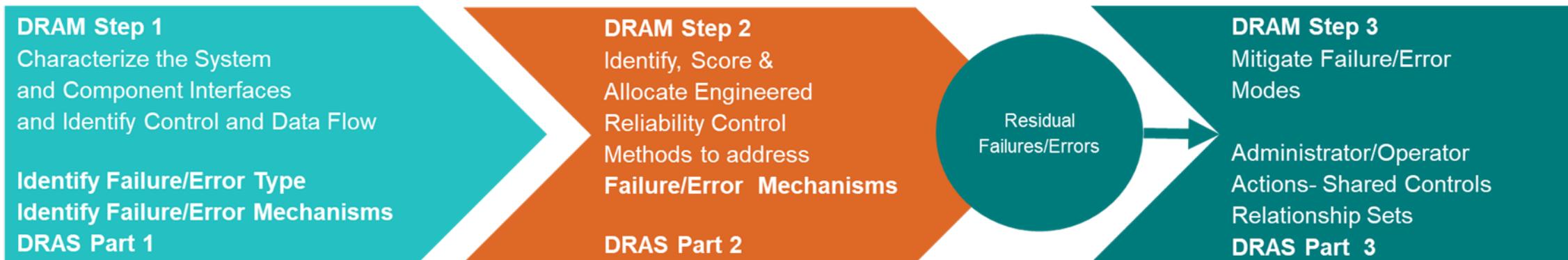
- Engineers are Uncomfortable with Probabilities.
- Risk Analysts are Uncomfortable with Engineering Decisions.
- The blind studies indicate the optimum process:
 - Identify Hazards/Consequences/Losses
 - Identify Causal Factors (DRAM/TAM)
 - Identify Control Measures (DRAM/TAM)
 - Probabilities/likelihood/sensitivity analysis done only if it would provide an ROI with further refinement based on the cost of preliminary control measures

Risk insights can be gleaned from any combination of Hazards, Consequences, or Likelihood.

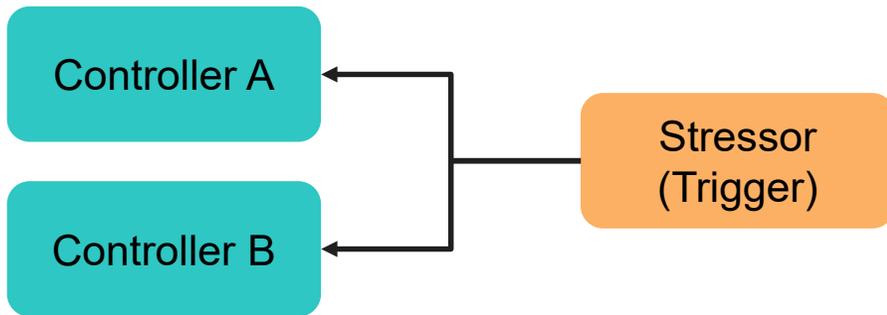
Digital Reliability Assessment Methodology (DRAM) Revision 0

- **Replacement for EPRI 3002005326 - *Methods for Assuring Safety and Dependability when Applying Digital Instrumentation and Control Systems* (June 2016)**
 - Development in progress for 2019/2020:
 - Identify, analyze, and resolve digital reliability items.
 - Shift to a hazard analysis based method.
 - P&L measures will become prototypes.
 - Update terminology to match IEC 61508.
 - Integrated into Digital Engineering Guide(DEG).

- **Integration of Hazard/Risk methods**
- **Developed into a field usable methodology**
- **Blind Studies in 2020**

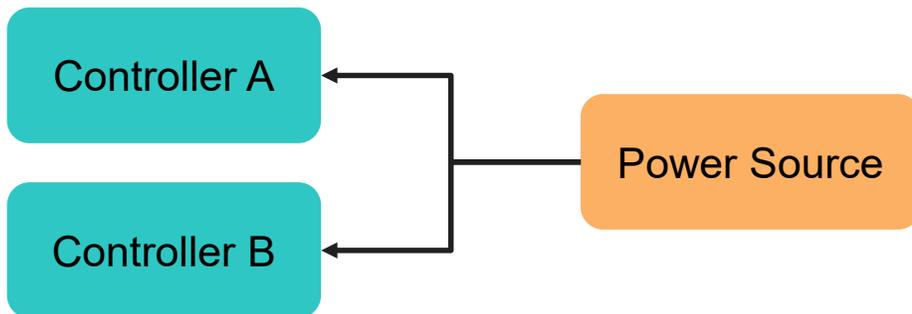


DRAM Software CCF and SPV Type Examples



Software Common Cause Failure

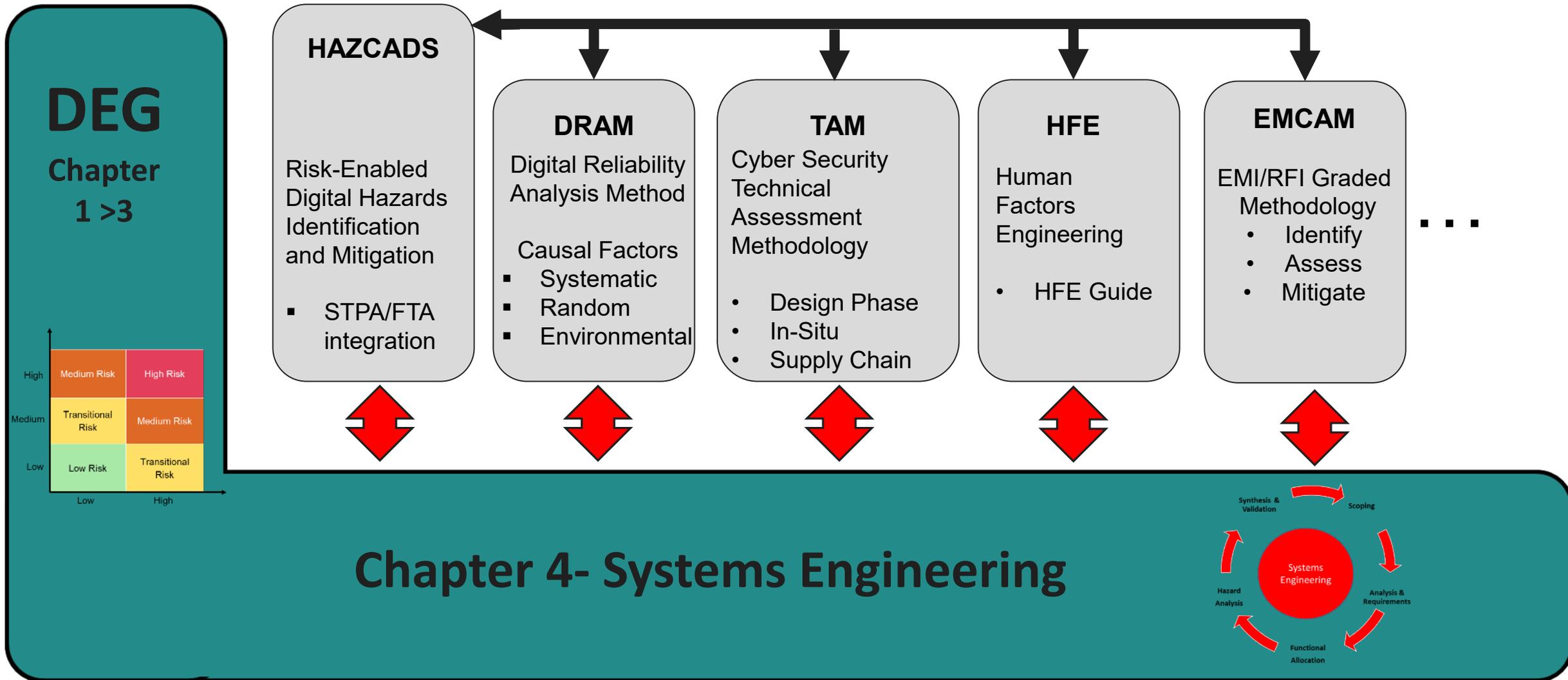
Both Controller A and B must exhibit internal behaviors that negate their design functions. Two failure/errors have occurred, one in each controller. The stressor or trigger must not itself be a failure or error. Likely caused by implicit design or implementation errors. Is systematic.



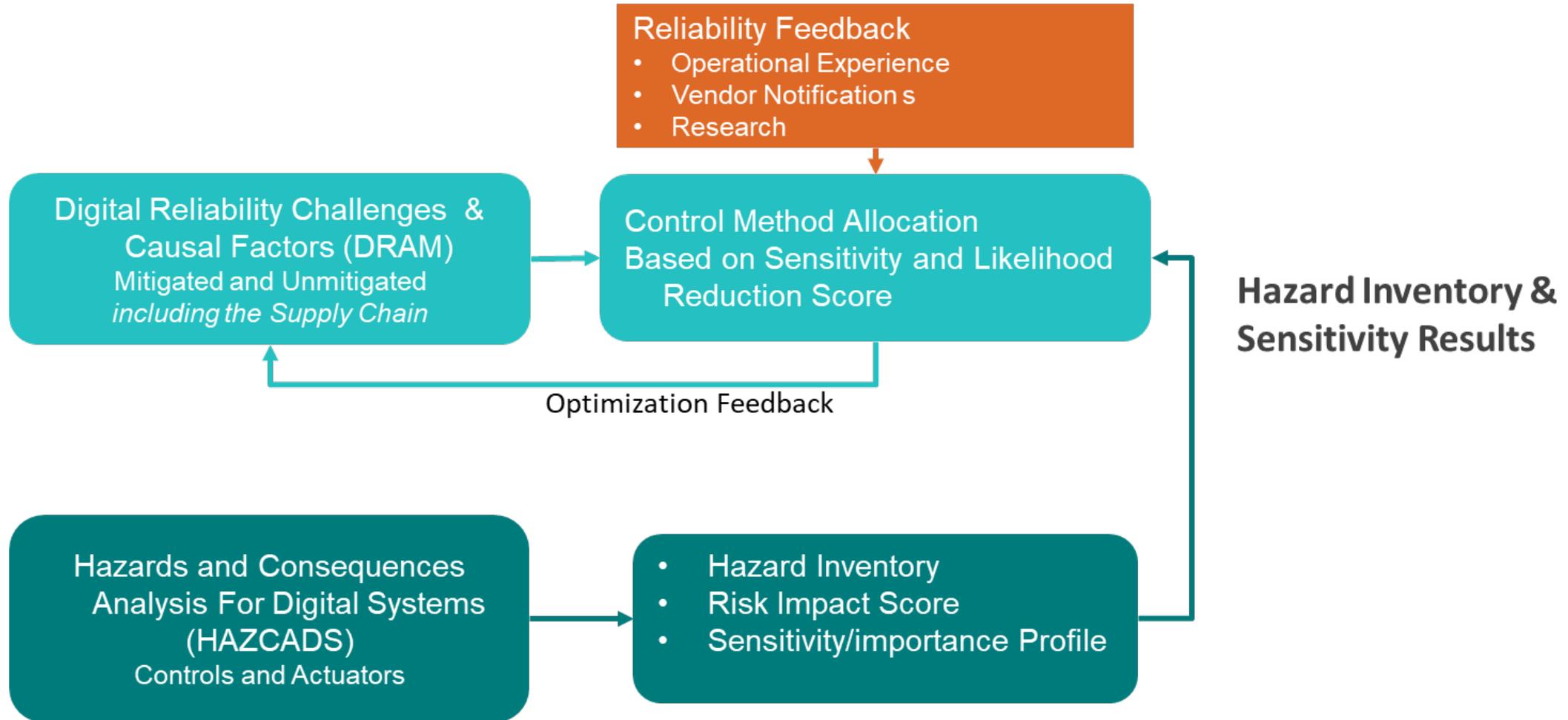
Single Point Vulnerability

Both Controller A and B must exhibit functional failures in their design functions. The Controllers have functioned as designed and are properly implemented. One failure has occurred, loss of a common power source. The stressor or trigger must not itself be a failure or error. May be normal and intended operation. Not a digital problem. Can be systematic or probabilistic.

The EPRI Digital Engineering Guide-3002011816



EPRI Risk-Informed Digital Reliability Process Model



➤ Target Reliability based on analyzed hazards, informed by Feedback sources, can dramatically **REDUCE THE SENSITIVITY** of a nuclear facility to the introduction of digital technologies.

EPRI R&D Overall Insights

- *Software reliability is directly proportional to the systematic controls and design and implementation constraints.*
- *Software CCF is a subset of total software design and implementation errors.*
- *Software CCF should be more narrowly defined to improve focus on the actual failure mechanisms of interest.*
- *An effective Systems Engineering process can ensure digital reliability is considered and resolved at each layer of the design and implementation process.*
- *Hazards analysis coupled with sensitivity analysis can ensure vulnerabilities are identified, analyzed, and efficiently resolved in the context of overall plant impact.*
- *Existing non-nuclear safety standards have evolved to a level of completeness, efficacy, and common use that they can enhance I&C reliability beyond that achievable with current nuclear industry methods.*
- *Existing non-nuclear safety standards can enhance nuclear safety by providing a basis for objective, risk informed criteria for I&C design and implementation.*

Together...Shaping the Future of Electricity

Antonescu, Christina

From: Ken Scarola <KenScarola@NuclearAutomation.com>
Sent: Thursday, November 21, 2019 3:10 PM
To: Antonescu, Christina
Subject: [External_Sender] Comments for ACRS meeting

Follow Up Flag: Follow up
Flag Status: Flagged

Christina,

The phone quality is terrible and it keeps cutting out. Below are the comments I would have offered during the public part of the meeting. Please pass them along to the committee members and to the Staff.

1. BTP 7-19 has been limited (and is still limited) to addressing CCF due to software defects. But SECY 93-087 was written to address all new sources of CCF that apply to digital systems that did not apply to analog systems. SECY 93-087 does not limit the new sources of CCF to a software defect. Modern integrated digital systems share numerous resources that are all new sources of CCF – these include digital processors that encompass multiple control or protection functions, and communication networks and soft controls that interface to numerous digital processors. These are all new sources of CCF that did not apply to analog systems, but do apply to modern digital systems. These CCFs can occur due to a single random hardware failure that is much more likely to occur than the triggering of a software defect due to an obscure combination of unanticipated events. Keep in mind that shared hardware resources are identified in the very first paragraph of SECY 93-087 as potential sources of CCF. To revise BTP 7-19 again, without addressing these additional new sources of CCF to the same extent as software defects fails to address the fundamental intent of SECY 93-087, which is to address new sources of CCF in digital systems.
2. This revision to BTP 7-19 differentiates a “D3 Assessment” for A1 systems from a “Qualitative Assessment” for A2 and B1 systems. But the difference is ambiguous. Here are some examples:
 1. For a D3 Assessment, CCF can be eliminated from further consideration through sufficient diversity, testing or defensive measures. “Sufficient” without clear deterministic definitions and acceptance criteria is in fact qualitative.
 2. The D3 Assessment, refers to defensive measures, the Qualitative Assessment refers to design attributes – defensive measures are design attributes. BTP 7-19 does not explain the difference.
 3. The D3 Assessment uses the words “CCF can be eliminated from further consideration”, the Qualitative Assessment uses the words “likelihood of CCF is sufficiently low”, which also means a CCF can be eliminated from further consideration. BTP 7-19 does not explain the difference. This sounds like legaleze embedded in what is supposed to be technical guidance.

BTP 7-19 is on revision 8, because it lacked clarity from the first day it was issued. If this ambiguity is not eliminated, revision 9 is certainly inevitable in the short term.

3. For CCFs that cannot be eliminated, SECY 93-087 and BTP 7-19 require an analysis of each event evaluated in the SAR. But the SAR considers all events with a concurrent loss of offsite power (LOOP). For valid technical reasons concurrent LOOP has not been considered in the D3 assessments previously approved by the Staff. On the 8th revision of BTP 7-19, it would seem that we could finally document this valid technical position.
4. Examples of A1 and A2 systems should be provided. If there is any dispute as to whether a diesel load sequencer is an A1 system, then examples should be given to explain when a sequencer would be considered an A1 system and when it is not.

Thank you.

Ken

Ken Scarola
Nuclear Automation Engineering, LLC
3672 Pine Tree Ln.
Murrysville, PA 15668
412-612-1192